Guía de soluciones de Arcserve® Unified Data Protection

Versión 8.x

arcserve®

Ayuda en línea de las soluciones de Arcserve® Unified Data Protection

Versión 8.x

La lista de contenido aparece en el panel izquierdo. Para ver todos los temas, haga clic en el icono  **que aparece en la parte superior.**

arcserve®

Aviso legal

Esta documentación, que incluye sistemas incrustados de ayuda y materiales distribuidos por medios electrónicos (en adelante, referidos como la "Documentación") se proporciona con el único propósito de informar al usuario final, pudiendo Arcserve proceder a su modificación o retirada en cualquier momento. Esta Documentación es información propiedad de Arcserve. Queda prohibida la copia, transferencia, reproducción, divulgación, modificación o duplicación de la totalidad o parte de esta Documentación sin el consentimiento previo y por escrito de Arcserve.

Si dispone de licencias de los productos informáticos a los que se hace referencia en la Documentación, Vd. puede imprimir, o procurar de alguna otra forma, un número razonable de copias de la Documentación, que serán exclusivamente para uso interno de Vd. y de sus empleados, y cuyo uso deberá guardar relación con dichos productos. En cualquier caso, en dichas copias deberán figurar los avisos e inscripciones relativas a los derechos de autor de Arcserve.

Este derecho a realizar copias de la Documentación sólo tendrá validez durante el período en que la licencia aplicable para el software en cuestión esté en vigor. En caso de terminarse la licencia por cualquier razón, Vd. es el responsable de certificar por escrito a Arcserve que todas las copias, totales o parciales, de la Documentación, han sido devueltas a Arcserve o, en su caso, destruidas.

EN LA MEDIDA EN QUE LA LEY APLICABLE LO PERMITA, ARCSERVE PROPORCIONA ESTA DOCUMENTACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO INCLUIDAS, ENTRE OTRAS PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN CONCRETO Y NO INCUMPLIMIENTO. ARCSERVE NO RESPONDERÁ EN NINGÚN CASO, ANTE VD. NI ANTE TERCEROS, EN LOS SUPUESTOS DE DEMANDAS POR PÉRDIDAS O DAÑOS, DIRECTOS O INDIRECTOS, QUE SE DERIVEN DEL USO DE ESTA DOCUMENTACIÓN INCLUYENDO A TÍTULO ENUNCIATIVO PERO SIN LIMITARSE A ELLO, LA PÉRDIDA DE BENEFICIOS Y DE INVERSIONES, LA INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL, LA PÉRDIDA DEL FONDO DE COMERCIO O LA PÉRDIDA DE DATOS, INCLUSO CUANDO ARCSERVE HUBIERA PODIDO SER ADVERTIDA CON ANTELACIÓN Y EXPRESAMENTE DE LA POSIBILIDAD DE DICHAS PÉRDIDAS O DAÑOS.

El uso de cualquier producto informático al que se haga referencia en la Documentación se regirá por el acuerdo de licencia aplicable. Los términos de este aviso no modifican, en modo alguno, dicho acuerdo de licencia.

Arcserve es el fabricante de esta Documentación.

Esta Documentación presenta Derechos restringidos. El uso, la duplicación o la divulgación por parte del gobierno de los Estados Unidos está sujeta a las restricciones establecidas en las secciones 12.212, 52.227-14 y 52.227-19(c)(1) - (2) de FAR y en la sección 252.227-7014(b)(3) de DFARS, según corresponda, o en posteriores.

© 2014-2021 Arcserve y sus empresas subsidiarias o afiliadas. Todos los derechos reservados. Las marcas registradas o de copyright de terceros son propiedad de sus respectivos propietarios.

Referencias de productos de Arcserve

En este documento se hace referencia a los siguientes productos de Arcserve:

- Arcserve® Unified Data Protection
- Agente de Arcserve® Unified Data Protection para Windows
- Agente de Arcserve® Unified Data Protection para Linux
- Arcserve® Backup
- Arcserve® Continuous Availability

Ponerse en contacto con Soporte de Arcserve

El equipo de Soporte de Arcserve ofrece un conjunto importante de recursos para resolver las incidencias técnicas y proporciona un fácil acceso a la información relevante del producto.

Contacto con Soporte técnico

Con Soporte de Arcserve:

- Se puede estar en contacto directo con la misma biblioteca de información que se comparte internamente por nuestros expertos de Soporte de Arcserve. Este sitio le proporciona el acceso a los documentos de nuestra base de conocimiento (KB). Desde aquí se pueden buscar fácilmente los artículos de la base de conocimiento relacionados con el producto que contienen soluciones probadas para muchas de las principales incidencias y problemas comunes.
- Se puede utilizar nuestro vínculo Conversación en vivo para iniciar instantáneamente una conversación en tiempo real con el equipo de Soporte de Arcserve. Con la Conversación en vivo, se pueden obtener respuestas inmediatas a sus asuntos y preguntas, mientras todavía se mantiene acceso al producto.
- Se puede participar en la Comunidad global de usuarios de Arcserve para preguntar y responder a preguntas, compartir sugerencias y trucos, discutir prácticas recomendadas y participar en conversaciones con sus pares.
- Se puede abrir un ticket de soporte. Al abrir un ticket de soporte en línea se puede esperar una devolución de llamada de uno de nuestros expertos en el área del producto por el que está preguntando.
- Se puede acceder a otros recursos útiles adecuados para su producto de Arcserve.

Contenido

Ayuda en línea de las soluciones de Arcserve® Unified Data Protection 2

Capítulo 1: Funciones y mejoras 31

Nuevas funciones 32

Mejoras de funcionalidades 34

Mejoras del Agente de Linux 35

Compatibilidad con la plataforma y la base de datos 36

Mejoras de seguridad y aplicaciones de terceros 37

Mejoras del Dispositivo de Arcserve 38

Funciones eliminadas 39

Capítulo 2: Funcionamiento de Arcserve UDP 41

Introducción 42

Cómo funciona Arcserve UDP 44

Máquina virtual instantánea (IVM) frente a la máquina de Virtual Standby (VSB) 46

Seguridad del usuario 49

Roles para los servicios de Arcserve UDP 50

Privilegios de usuario para las funciones de Arcserve UDP 52

Capítulo 3: Instalación de Arcserve UDP 63

Cómo instalar Arcserve UDP 64

Revisión de las consideraciones y requisitos previos 65

Selección del tipo de instalación 66

Instalación de Arcserve Unified Data Protection mediante el Asistente de instalación 67

Instalación de Arcserve Unified Data Protection mediante la línea de comandos 72

Instalación de Arcserve UDP mediante el instalador unificado 77

Verificación de la instalación 79

Puertos de comunicación usados por Arcserve UDP 80

Cómo afecta el proceso de instalación a los sistemas operativos 101

Cómo instalar actualizaciones de Arcserve UDP 107

Revisión de las consideraciones para instalar las actualizaciones 108

Especificación de las preferencias de actualización 109

Compruebe e instale las actualizaciones 115

Actualización de agentes en nodos remotos mediante la puerta de enlace 117

Actualización del servidor de puntos de recuperación en el servidor remoto mediante la puerta de enlace 118

(Opcional) Instalación de las actualizaciones de Arcserve UDP en modo silencioso 119

Verificación de la instalación correcta de las actualizaciones 120
Cómo desinstalar Arcserve UDP 121
Desinstalación estándar 122
Desinstalación silenciosa 123
Eliminación de los componentes que ha dejado el desinstalador 125
Capítulo 4: Actualización a Arcserve UDP versión 8.0 127
Versiones compatibles con la actualización 128
Secuencia de actualización en el dispositivo de Arcserve 129
Actualización del dispositivo de Arcserve que funciona como Consola de Arcserve UDP y como servidor de puntos de recuperación 130
Actualización del Dispositivo de Arcserve que solo funciona como servidor de puntos de recuperación de Arcserve UDP 131
Pasos de actualización cuando se utilizan dos o más Dispositivos de Arcserve en el entorno 132
Actualización del Agente de Linux de Arcserve Backup en el dispositivo de Arcserve 133
Actualización de Arcserve Backup en el dispositivo de Arcserve 134
Política de compatibilidad con versiones anteriores 135
Política de compatibilidad con versiones anteriores para Arcserve UDP versión 8.0 135
Política de compatibilidad con versiones anteriores para Arcserve UDP versión 7.x 139
Política de compatibilidad con versiones anteriores para Arcserve UDP versión 6.5 Actualización 4 142
Compatibilidad con versiones anteriores para el servidor de copia de seguridad de Linux 145
Secuencia de actualización para la Consola de UDP, el Servidor de puntos de recuperación y el Agente 146
Cómo actualizar a Arcserve UDP 8.0 desde una versión anterior 147
Cómo actualizar a Arcserve UDP 8.0 con el instalador único 150
Cómo actualizar a Arcserve UDP 8.0 o Arcserve Backup 18.0 para activar la copia en cinta 154
Cómo migrar la Consola de Arcserve UDP de un servidor a otro 157
Cómo actualizar la puerta de enlace a la misma versión de su Consola registrada 158
Cómo realizar la migración de la Consola de Arcserve UDP 158
Capítulo 5: Exploración y configuración de Arcserve UDP 161
Inicio de sesión en la Consola de Arcserve UDP utilizando la autenticación multifactor 161
Revisión de los requisitos previos 161
Cómo iniciar sesión en la Consola de Arcserve UDP utilizando MFA 162
Arcserve Unified Data Protection Interfaz de usuario 167
Navegación en Arcserve UDP 168
Fichas 170

Cuadro de diálogo Controlador de tareas ... 188
Cómo configurar Arcserve UDP ... 189
Configuración del protocolo de comunicaciones del servidor ... 190
Configuración de bases de datos ... 192
Configuración de la sincronización de datos de copia de seguridad de Arcserve ... 196
Configuración de SRM ... 198
Configuración de la detección de nodos ... 200
Configuración del correo electrónico y alertas ... 202
Configuración del proxy ... 204
Actualización de la configuración ... 206
Configuración de la cuenta del administrador ... 208
Configuración de la implementación remota ... 209
Asignación del plan a la cuenta de usuario ... 210
Gestión de usuarios ... 212
Configuración de la duración del tiempo de espera de la Consola ... 213
Cómo migrar los puntos de recuperación de Arcserve r16.5 a Arcserve UDP ... 214
Creación de un almacén de datos para replicar los datos de un punto de recuperación de Arcserve r16.5 ... 215
Replicación de los datos de Arcserve r16.5 al almacén de datos de UDP ... 216
Configuración del asistente de configuración ... 217
Capítulo 6: Funcionamiento de las funciones clave de Arcserve UDP ... 219
Funcionamiento de la función Nutanix en Arcserve UDP ... 220
Funcionamiento de la función OneDrive en Arcserve UDP ... 221
Funcionamiento de la función Exchange Online en Arcserve UDP ... 222
Funcionamiento de la función de instantánea de hardware en UDP ... 223
Funcionamiento de la función de la nube en UDP ... 225
Funcionamiento de la función de la ruta UNC/NFS en UDP ... 227
Funcionamiento de la función SharePoint Online en UDP ... 228
Requisitos previos ... 228
Capítulo 7: Uso de la administración basada en roles de Arcserve UDP ... 229
Acceso a la Consola de gestión de usuarios ... 230
Inicio de la Consola de gestión de usuarios de Arcserve UDP ... 230
Configuración de la autenticación multifactor ... 231
Adición de usuarios, eliminación de usuarios y cambios de contraseña ... 238
Configuración de la gestión de usuarios ... 239
Roles predefinidos ... 240

Asignación de roles predefinidos ... 244
Visualización y cancelación de un rol ... 245
Adición de un nuevo rol ... 246
Búsqueda de usuarios y roles ... 248
Integración de Arcserve UDP con Active Directory ... 249
Cómo integrar Arcserve UDP 8.0 con Active Directory utilizando grupos de Windows ... 250
Cómo integrar Arcserve UDP 8.0 con Active Directory utilizando grupos de Active Directory ... 254
Acceso a Arcserve UDP utilizando la autenticación integrada de Windows ... 260
Solución de problemas para la autenticación integrada de Windows (IWA) ... 261
La Consola de Arcserve UDP no es compatible con IWA si la conexión de la base de datos de la Consola utiliza el modo de autenticación de Windows ... 263
Solución de problemas ... 265
Capítulo 8: Adición y gestión de nodos de origen ... 267
Cómo agregar nodos a la consola ... 268
Revisión de los requisitos previos ... 269
Adición de nodos ... 270
Detección de nodos ... 275
Importación de nodos ... 278
Cómo gestionar nodos ... 285
Revisión de los requisitos previos ... 286
Actualización de la información del hipervisor ... 287
Especificación del hipervisor ... 288
Actualización de la información de la máquina virtual ... 290
Actualización de nodos ... 291
Exportación de nodos ... 295
Pausa de nodos ... 296
Reanudación de un nodo ... 297
Sincronizar datos ... 298
Supresión de nodos desde la consola ... 299
Implementación del Agente en los nodos ... 300
Realización de comprobaciones previas a las tareas de copia de seguridad ... 301
Cómo agregar y gestionar una ruta UNC/NFS ... 320
Adición de una ruta UNC/NFS ... 321
Actualización de una ruta UNC/NFS ... 324
Supresión de una ruta UNC/NFS ... 325
Cómo agregar y gestionar grupos de nodos ... 326

Revisión de los requisitos previos ... 328
Agregación de grupos de nodos ... 329
Modificación de grupos de nodos ... 330
Supresión de grupos de nodos ... 331
Cómo gestionar nodos para la nube ... 332
Descarga de un punto de recuperación de la nube ... 333
Carga de un punto de recuperación a la nube ... 337
Copia de puntos de recuperación en el disco local o en un recurso compartido de red ... 340
Adición de una matriz de almacenamiento de ... 343
Adición de una matriz de almacenamiento para NetApp ... 345
Agregación de los detalles de HPE RMC que gestiona la matriz de almacenamiento HPE 3PAR Storeserv ... 352
Adición de una matriz de almacenamiento de Nimble ... 354
Cómo agregar y gestionar un sitio ... 356
Especificación del nombre del sitio ... 358
Compartir instrucción de registro ... 359
Comprobar y agregar el sitio ... 360
Modificación de la dirección URL de la consola ... 361
Modificación del sitio ... 362
Eliminación de un sitio ... 363
Configuración de un servidor proxy para la puerta de enlace ... 364
Cómo gestionar los nodos de Exchange Online ... 367
Adición de un nodo de Exchange Online ... 368
Actualización de un nodo de Exchange Online ... 370
Supresión de un nodo de Exchange Online ... 371
Compatibilidad con el buzón de correo de la carpeta pública para la protección de Exchange Online ... 372
Cómo gestionar los nodos de SharePoint Online ... 373
Adición de un nodo de SharePoint Online ... 374
Actualización de un nodo de SharePoint Online ... 375
Supresión de un nodo de SharePoint Online ... 376
Cómo gestionar el nodo de OneDrive ... 376
Adición de un nodo de OneDrive ... 377
Supresión de un nodo de OneDrive ... 377
Cómo gestionar los nodos del grupo de la base de datos de Oracle ... 377
Actualización del nodo de la base de datos de Oracle ... 377
Exportación de nodos ... 378

Copia de seguridad del nodo de la base de datos de Oracle 379
Cancelación de la tarea de copia de seguridad de los nodos de la base de datos de Oracle 380
Supresión de los nodos de la base de datos de Oracle 381
Capítulo 9: Adición y gestión de destinos 383
Cómo agregar un destino 384
Cómo agregar un destino 385
Agregar servidores de Arcserve Backup 399
Adición de una consola remota 401
Adición de una cuenta de la nube 403
Adición de una cuenta de la nube de Arcserve 438
Cómo gestionar un almacén de datos 440
Revisión de los requisitos previos 441
Modificación de un almacén de datos 442
Inicio de un almacén de datos 452
Detención de un almacén de datos 453
Supresión de un almacén de datos de la consola 455
Supresión de los datos del nodo de un almacén de datos 456
Control de la capacidad de espacio del almacén de datos 458
Examen de puntos de recuperación en un almacén de datos 465
Compatibilidad de FQDN con un almacén de datos 467
Ejecutar una tarea de combinación manual o a petición 468
Modificación del límite de nodos activos simultáneos para la copia de seguridad manual 470
Solución de problemas: Cómo utilizar un almacén de datos cuando una o varias de las carpetas estén completas. 471
Cómo gestionar un servidor de punto de recuperación 474
Revisión de los requisitos previos 475
Actualización de un servidor de punto de recuperación 476
Supresión de un servidor de punto de recuperación desde la consola 477
Importación de un almacén de datos 478
Instalación/actualización del servidor de punto de recuperación 480
Cómo gestionar servidores de Arcserve Backup 481
Actualización del servidor de Arcserve Backup 482
Eliminación de un servidor de Arcserve Backup 483
Cómo gestionar una carpeta compartida 484
Modificación de una carpeta compartida 485
Supresión de una carpeta compartida 486

Cómo gestionar una consola remota 487
Modificación de una consola remota 488
Supresión de una consola remota 489
Prueba de la conexión de la consola remota 490
Capítulo 10: Creación de planes para proteger datos 493
Funcionamiento del plan y de las tareas 494
Cómo crear un plan de copia de seguridad en Windows 498
Revisión de las consideraciones y requisitos previos 499
Creación de un plan de copia de seguridad con una tarea de copia de seguridad 505
(Opcional) Realización de una copia de seguridad manual 529
Verificación de la copia de seguridad. 532
Cómo crear un plan de copia de seguridad de Nutanix 533
Cómo crear un plan de Virtual Standby a Nutanix AHV 534
Cómo crear una máquina virtual instantánea en Nutanix AHV 534
Cómo crear un plan de recuperación asegurada para proteger Nutanix AHV para el nodo de Linux 534
Cómo realizar la copia de seguridad del volumen compartido de clúster 534
Modificación de la configuración del equipo del agente para realizar la copia de seguridad del volumen CSV 536
Cómo realizar la copia de seguridad de volúmenes sin la letra de unidad 537
Revisión de los requisitos previos 538
Montaje del volumen sin letra de unidad en la carpeta NTFS 538
Especificación del volumen sin letra de unidad en el registro 539
Cómo realizar la copia de seguridad del volumen seleccionado 540
Cómo crear un plan de copia de seguridad en Linux 542
Revisión de las consideraciones y requisitos previos 543
Creación de un plan de copia de seguridad 544
(Opcional) Realización de una copia de seguridad manual 567
Verificación de la copia de seguridad. 570
Solución de problemas 571
Cómo crear un plan de copia de seguridad de máquina virtual basada en el host 574
Revisión de las consideraciones y requisitos previos 576
Creación de un plan de copia de seguridad basado en el host 582
(Opcional) Realización de una copia de seguridad manual 623
Verificación del plan 626
Cómo crear un plan de Virtual Standby a AWS EC2 627
Revisión de las consideraciones y requisitos previos 628

Creación de un plan con una tarea de copia de seguridad 636
Adición al plan de una tarea de Virtual Standby a EC2 655
(Opcional) Ejecución manual de la tarea de Virtual Standby a EC2 662
Pausa y reanudación de la tarea de Virtual Standby 663
Verificación del plan 665
Finalización de recursos de EC2 665
Cómo crear un plan de Virtual Standby a Microsoft Azure 667
Revisión de las consideraciones y requisitos previos 668
Creación de un plan con una tarea de copia de seguridad 669
Adición de una tarea de Virtual Standby al plan 670
(Opcional) Ejecución de la tarea de Virtual Standby manualmente 678
Pausa y reanudación de latidos 679
Pausa y reanudación de la tarea de Virtual Standby 680
Verificación del plan 682
Cómo crear un plan de Virtual Standby 683
Revisión de las consideraciones y requisitos previos 684
Creación de un plan con una tarea de copia de seguridad 686
Cómo agregar una tarea de Virtual Standby al plan 705
(Opcional) Ejecución de la tarea de Virtual Standby manualmente 719
Pausa y reanudación de latidos 720
Pausa y reanudación de la tarea de Virtual Standby 721
Verificación del plan 723
Cómo crear un plan de recuperación asegurada 724
Revisión de las consideraciones y requisitos previos 725
Adición de una tarea de recuperación asegurada al plan 727
(Opcional) Ejecución manual de la tarea de prueba de recuperación asegurada 742
Cómo crear un plan de copia de seguridad de la ruta UNC/NFS 745
Revisión de las consideraciones y requisitos previos 746
Creación de un recurso compartido de archivos 746
Creación de un plan de copia de seguridad con una tarea de la ruta UNC/NFS 751
(Opcional) Realización de una copia de seguridad manual 774
Otras tareas en el plan UNC/NFS 777
Verificación de la copia de seguridad. 778
Cómo proteger equipos de Virtual Standby 779
Revisión de las consideraciones y requisitos previos 780
Encendido de las máquinas de Virtual Standby 781

Protección de las máquinas de Virtual Standby después de encenderlas 788
Verificación de que la máquina de Virtual Standby está protegida 790
Cómo proteger máquinas virtuales instantáneas 791
Revisión de las consideraciones y requisitos previos 792
Encendido de máquinas virtuales instantáneas a partir de un punto de recuperación 793
Protección de una máquina virtual instantánea al encenderse 794
Verificación de que la máquina virtual instantánea está protegida 795
Cómo replicar datos entre almacenes de datos gestionados desde una Consola de UDP 796
Revisión de las consideraciones y requisitos previos 797
Creación de una tarea de copia de seguridad 798
Cómo agregar una tarea de replicación al plan 799
(Opcional) Realización de una replicación manual 802
Verificación del plan 803
Cómo replicar datos entre almacenes de datos gestionados desde consolas de UDP diferentes 804
Revisión de los requisitos previos 807
Creación de una cuenta de usuario para la consola de origen 808
Creación de un plan para definir el almacén de datos de destino 809
Asignación del plan a la cuenta de usuario 812
Envío de los detalles de la cuenta de usuario y el plan al administrador de origen 814
Recepción de los detalles de la cuenta de usuario y el plan del administrador de destino 815
Creación de un plan de replicación para enviar datos a la consola de destino 816
Verificación de los datos replicados 820
Cómo realizar una replicación de datos sin conexión mediante el servidor de puntos de recuperación Jumpstart 821
Revisión de los requisitos previos 824
Creación de un almacén de datos temporal en un dispositivo externo 825
Replicación de datos de origen en un almacén de datos temporal 826
Supresión del almacén de datos temporal desde la consola de origen 827
Envío del dispositivo externo a la ubicación de destino 828
Recepción del dispositivo externo 829
Importación del almacén de datos temporal desde el dispositivo externo 830
Creación de un almacén de datos de destino 831
Replicación de datos desde el almacén de datos temporal en el de destino 832
Verificación de la replicación de los datos 833
(Opcional) Establecimiento del número de nodos simultáneos para el servidor de puntos de recuperación JumpStart 834

Cómo realizar la replicación inversa 834
Revisión de los requisitos previos 835
Realización de la replicación ad hoc 835
Realización de la replicación inversa desde la Consola remota al servidor del servidor de puntos de recuperación local 843
Cómo crear un plan de copia de puntos de recuperación 851
Revisión de las consideraciones y requisitos previos 852
Creación de un plan con una tarea de copia de seguridad 853
Adición de una tarea de copia de puntos de recuperación al plan 870
Verificación del plan 879
Cómo crear un plan de copia de archivo 880
Revisión de las consideraciones y requisitos previos 881
Creación de un plan con una tarea de copia de seguridad 882
Adición de una tarea de copia de archivo al plan 901
(Opcional) Realización de una copia de archivos manual 912
Verificación del plan 913
Cómo crear un plan de archivado de archivos 914
Revisión de las consideraciones y requisitos previos 915
Creación de un plan con una tarea de copia de seguridad 916
Adición de una tarea de archivado de archivos al plan 935
(Opcional) Realización de un archivado de archivos manual 947
Verificación del plan 948
Cómo crear un plan de copia en cinta 949
Revisión de las consideraciones y requisitos previos 950
Creación de un plan con una tarea de copia de seguridad 951
Adición de una tarea de copia en cinta al plan 952
Cómo crear y gestionar una máquina virtual instantánea en Microsoft Azure 961
Revisión de los requisitos previos para una máquina virtual instantánea en Microsoft Azure 962
Creación de una máquina virtual instantánea en Microsoft Azure 963
Gestión de una máquina virtual instantánea 972
Cómo crear y gestionar una máquina virtual instantánea en servidores Hyper-V y servidores ESX VMware 975
Revisión de los requisitos previos para una máquina virtual instantánea 977
Creación de una máquina virtual instantánea 980
Gestionar máquina virtual instantánea 996
Cómo crear y gestionar una máquina virtual instantánea en Amazon EC2 1002

Revisión de los requisitos previos para una máquina virtual instantánea en Amazon EC2 ... 1003
Creación de un de la máquina virtual instantánea en Amazon EC2 ... 1004
Gestión de una máquina virtual instantánea ... 1013
Cómo crear un plan para la replicación entre sitios ... 1019
Creación de un plan para la replicación entre sitios ... 1021
Cómo proteger los datos de Microsoft Office 365 ... 1023
Autenticación moderna ... 1023
Cómo crear un plan de copia de seguridad de Exchange Online ... 1030
Cómo crear un plan de copia de seguridad de SharePoint Online ... 1062
Cómo crear un plan de copia de seguridad de Microsoft Office 365 OneDrive ... 1083
Gestión de la copia de seguridad y la restauración de Microsoft Teams ... 1102
Revisión de las consideraciones y requisitos previos ... 1105
Adición del rol y del grupo necesarios a la cuenta de copia de seguridad de Exchange Online para realizar la copia de seguridad y la restauración ... 1108
Creación de un plan de copia de seguridad de Exchange Online 1110
Especificación del origen ... 1112
Especificación del destino ... 1121
Especificación de la programación ... 1122
Funcionamiento de la programación avanzada y de la retención ... 1126
Especificación de la configuración avanzada ... 1129
Revisión de los requisitos previos ... 1152
Creación de un plan de copia de seguridad de SharePoint Online ... 1153
Especificación del origen ... 1155
Especificación del destino ... 1160
Especificación de la programación ... 1161
Especificación de la configuración avanzada ... 1165
Cómo crear y configurar máquinas virtuales instantáneas simultáneas en varios hipervisores ... 1183
Selección de un servidor de puntos de recuperación de origen ... 1185
Selección de la ubicación de las máquinas virtuales ... 1187
Selección de servidores de recuperación ... 1191
Configuración de las máquinas virtuales ... 1193
Verificación del resumen ... 1198
Cómo configurar máquinas de Virtual Standby simultáneas ... 1201

Capítulo 12: Uso de la instantánea de hardware para la copia de seguridad 1205

Cómo utilizar la instantánea de hardware para copias de seguridad 1206

Utilización de la instantánea de hardware para la copia de seguridad sin agente de VMware 1208

Consideraciones para la compatibilidad de NetApp iSCSI/FC con VMware 1210

Consideraciones para la compatibilidad de NFS con VMware 1214

Consideraciones sobre el almacenamiento de Nimble cuando la autenticación CHAP está activada 1217

Utilización de la instantánea de hardware para la copia de seguridad sin agente de Hyper-V 1219

Utilización de la instantánea de hardware para la copia de seguridad basada en el agente 1221

Verificación del uso de la instantánea de hardware por parte de la copia de seguridad 1222

Capítulo 13: Restauración de datos protegidos 1223

Cómo restaurar desde un punto de recuperación 1224

Revisión de las consideraciones y requisitos previos de la restauración 1226

Especificación de la información del punto de recuperación que se debe restaurar 1233

Restauración del contenido del punto de recuperación 1247

Verificación de que se ha restaurado el contenido 1248

Cómo restaurar desde una copia de archivo 1249

Revisión de las consideraciones y requisitos previos de la restauración 1251

Especificación de la información de la copia de archivo que se debe restaurar 1254

Restauración del contenido de la copia de archivo 1266

Verificación de que se ha restaurado el contenido 1268

Cómo restaurar desde un archivado de archivos 1269

Revisión de las consideraciones y requisitos previos de la restauración 1270

Especificación de la información de la copia de archivo que se debe restaurar 1272

Restauración del contenido del punto de recuperación 1284

Verificación de que se ha restaurado el contenido 1286

Cómo restaurar archivos y carpetas 1287

Revisión de las consideraciones y requisitos previos de la restauración 1290

Especificación de la información del archivo y/o carpeta que se debe restaurar 1297

Restauración del archivo y/o carpeta 1317

Verificación de que el archivo y/o carpeta se ha restaurado 1319

Cómo realizar una reconstrucción completa utilizando una máquina virtual de Virtual Standby o instantánea 1320

Revisión de las consideraciones y requisitos previos de la reconstrucción completa 1322

Definición de las opciones de la reconstrucción completa 1324
Verificación de que la reconstrucción completa ha sido correcta 1347
Información de referencia de la reconstrucción completa 1348
Solución de problemas relacionados con la recuperación completa 1356
Cómo restaurar una máquina virtual 1363
Revisión de las consideraciones y requisitos previos de la restauración 1365
Especificación de la información de la máquina virtual que se va a restaurar 1366
Restauración de la máquina virtual 1385
Verificación de que la máquina virtual se ha restaurado 1386
Cómo restaurar SQL Filestream 1386
Cómo aplicar el parche T00002266 1387
Restauración de la base de datos SQL a la ubicación original 1388
Restauración de la base de datos SQL a una instancia alternativa en el mismo servidor 1391
Restauración de la base de datos SQL a una instancia alternativa en un servidor diferente 1396
Restauración de la base de datos SQL a una ubicación alternativa en la misma instancia 1403
Modo de restauración a través de la clave de registro 1406
Cómo usar la utilidad Exchange Granular Restore (GRT) 1413
Introducción 1414
Revisión de las consideraciones y requisitos previos 1415
Cómo restaurar datos de Microsoft Exchange Data con la utilidad Exchange Granular Restore (GRT) 1416
Cómo restaurar una aplicación de Microsoft Exchange 1422
Revisión de las consideraciones y requisitos previos de la restauración 1424
Especificación de la información de Microsoft Exchange para restaurar 1426
Restauración de la aplicación de Microsoft Exchange 1432
Verificación de que la aplicación de Microsoft Exchange se ha restaurado 1434
Cómo restaurar datos de Exchange en una máquina virtual de VMware 1435
Cómo descargar archivos o carpetas sin restaurar 1436
Cómo descargar archivos o carpetas sin restaurar para nodos de Linux 1438
Cómo restaurar una aplicación de Microsoft SQL Server 1440
Revisión de las consideraciones y requisitos previos de la restauración 1442
Especificación de la información de Microsoft SQL Server para restaurar 1445
Restauración de la aplicación de Microsoft SQL Server 1451
Verificación de que la aplicación de Microsoft SQL Server se ha restaurado 1453
Cómo restaurar desde una ruta UNC/NFS 1454
Revisión de las consideraciones y requisitos previos de la restauración 1455

Especificación de la información de la ruta UNC/NFS que se debe restaurar 1456
Restauración de los archivos o carpetas y el contenido que se encuentra en la ruta UNC/NFS 1467
Verificación de que se ha restaurado el contenido 1469
Cómo restaurar una base de datos de Oracle 1470
Revisión de las consideraciones y requisitos previos 1472
Restauración del archivo de parámetros del servidor 1473
Restauración del archivo de parámetros 1474
Restauración de los registros de rehacer archivados 1475
Restauración de los espacios de tablas o archivos de datos 1476
Restauración del sistema o acción de deshacer espacios de tablas o archivos de datos 1478
Restauración de todos los espacios de tablas y archivos de datos 1480
Restauración de archivos de control 1482
Restauración de la base de datos entera (espacios de tablas y archivos de control) 1484
Recuperación de la base de datos de Oracle mediante la reconstrucción completa 1486
Cómo realizar una recuperación a nivel de archivo en nodos de Linux 1487
Revisión de los requisitos previos 1489
(Opcional) Recuperación de los datos a partir del volumen de iSCSI del equipo de destino 1490
Especificación del punto de recuperación para la copia de seguridad basada en agentes 1492
Especificación de los detalles del equipo de destino 1499
Especificación de la configuración avanzada 1503
Creación y ejecución de la tarea de restauración 1508
Verificación de la restauración de archivos 1510
Cómo realizar una recuperación de archivos desde copias de seguridad sin agente basadas en el host para nodos de Linux 1511
Revisión de los requisitos previos 1512
Especificación del punto de recuperación 1513
Especificación de los detalles de la máquina de destino 1518
Especificación de la configuración avanzada 1522
Creación y ejecución de la tarea de restauración 1527
Verificación de la restauración de archivos 1528
Cómo realizar la migración de la máquina virtual instantánea (del punto de recuperación de Linux) desde la nube al recurso local 1529
Revisión de los requisitos previos y consideraciones para la migración de la máquina virtual instantánea 1530
Realización de la migración de la máquina virtual instantánea desde la nube al recurso local 1531
Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux 1532

Revisión de los requisitos previos de BMR ... 1535
Obtención de la dirección IP del equipo de destino mediante Live CD ... 1536
(Opcional) Recuperación de los datos en el volumen de iSCSI del equipo de destino ... 1538
(Opcional) Recuperación de los datos a partir del volumen de iSCSI del equipo de destino ... 1540
Revisión del servidor de copia de seguridad ... 1542
Especificación de los puntos de recuperación ... 1544
Especificación de los detalles del equipo de destino ... 1546
Especificación de la configuración avanzada ... 1548
Creación y ejecución de la tarea de restauración ... 1554
Verificación de que el nodo de destino se ha restaurado ... 1562
Cómo realizar una reconstrucción completa (BMR) de la migración para los equipos de Linux ... 1563
Revisión de los requisitos previos para la reconstrucción completa de migración ... 1564
Realización de una reconstrucción completa en el equipo temporal ... 1565
Realización de una reconstrucción completa de la migración ... 1567
Verificación de que el nodo de destino se ha restaurado ... 1569
Cómo realizar una reconstrucción completa mediante una copia de seguridad ... 1570
Revisión de las consideraciones y requisitos previos de la reconstrucción completa ... 1573
Definición de las opciones de la reconstrucción completa ... 1575
Verificación de que la reconstrucción completa ha sido correcta ... 1594
Información de referencia de la reconstrucción completa ... 1595
Solución de problemas relacionados con la recuperación completa ... 1603
Cómo restaurar los nodos agrupados en clúster y los discos compartidos de Microsoft ... 1611
Revisión de los requisitos previos ... 1613
Restauración de archivos de un disco compartido agrupado en clúster ... 1614
Restauración de un nodo específico de un clúster ... 1615
Restauración de un disco dañado compartido del clúster ... 1616
Restauración de todos los nodos agrupados en clúster y del disco compartido ... 1617
Cómo restaurar un Active Directory ... 1619
Revisión de las consideraciones y requisitos previos de la restauración ... 1621
Restauración de Active Directory ... 1622
Verificación de que Active Directory se ha restaurado ... 1626
Cómo restaurar datos de Active Directory utilizando la utilidad Restauración de nivel de objeto de Active Directory de Arcserve UDP ... 1626
Cómo restaurar los datos de Microsoft Office 365 ... 1634
Cómo restaurar los datos del buzón de correo de Exchange Online ... 1635

Cómo restaurar los datos de recopilación de sitios de SharePoint Online 1652
Cómo restaurar los datos de OneDrive 1663
Exploración del punto de recuperación de copia en cinta para la restauración 1674
Cómo realizar la restauración a un momento determinado 1674
Requisitos previos 1675
Consideraciones 1675
Realización de la restauración a un momento determinado 1676
Cómo restaurar el volumen compartido de clúster 1680
Revisión de las consideraciones y requisitos previos 1681
Especificación de la información de CSV para la restauración 1687
Restauración del contenido de CSV 1697
Capítulo 2: Gestión de restauración y copia de seguridad de cintas 1699
Cómo realizar la copia de seguridad de un almacén de datos de deduplicación en una cinta 1700
Cómo restaurar un almacén de datos de deduplicación desde una cinta 1701
Revisión de los requisitos previos 1703
Restaurar desde un medio de cinta a una ubicación alternativa 1704
Importación del almacén de datos restaurado al servidor de puntos de recuperación 1706
Capítulo 3: mediante la interfaz de PowerShell 1709
Cómo utilizar la interfaz de PowerShell 1710
Revisión de los requisitos previos 1711
Uso de la interfaz de PowerShell para Arcserve UDP 1712
Sintaxis y parámetros de PowerShell 1713
Ejemplos de PowerShell 1726
Archivo de configuración y propiedades de PowerCLI 1730
Capítulo 4: Protección del sistema Oracle utilizando Recovery Manager (RMAN) 1733
Revisión de los requisitos previos para la base de datos de Oracle con RMAN (Windows y Linux) 1734
Cómo crear un plan de copia de seguridad para la base de datos de Oracle (Windows y Linux) 1743
Creación de un plan de copia de seguridad con una tarea de copia de seguridad 1744
Adición de una tarea de recuperación asegurada al plan 1768
(Opcional) Realización de una copia de seguridad manual 1778
Cómo restaurar una base de datos de Oracle utilizando RMAN 1780
Selección de los elementos de la base de datos de Oracle para restaurar 1781
Definición de las opciones de restauración 1789

Limitaciones ... 1803

Capítulo 5: Protección del entorno de Microsoft SharePoint ... 1805

Consideraciones sobre la instalación para el entorno de Microsoft SharePoint ... 1806

Cómo realizar copias de seguridad de servidores de Microsoft SharePoint ... 1807

Revisión de las consideraciones ... 1808

Creación de una copia de seguridad del servidor de SharePoint ... 1809

Cómo restaurar un entorno de SharePoint ... 1812

Restauración mediante máquina virtual instantánea ... 1813

Restauración mediante la interfaz de usuario del Agente de Arcserve UDP ... 1823

Restauración mediante el montaje de la base de datos desde el punto de recuperación 1829

Creación de una red aislada para la recuperación de SharePoint ... 1853

Cómo crear una red aislada para la recuperación de SharePoint en máquinas virtuales de VMware ... 1854

Cómo crear una red aislada para la recuperación de SharePoint en máquinas virtuales de Hyper-V ... 1860

Capítulo 6: Generación de informes de Arcserve UDP ... 1863

Funcionamiento de los informes de Arcserve UDP ... 1864

Informes de Arcserve UDP ... 1865

Utilización de filtros y acciones ... 1883

Cómo trabajar con los informes de Arcserve UDP ... 1885

Creación de un perfil de acuerdo de nivel de servicio ... 1886

Programación de correos electrónicos ... 1889

Enviar informe mediante correo electrónico ... 1894

Generación de un informe ... 1896

Personalización de los días de retención para un informe de estado de una tarea ... 1897

Tamaño de los datos sin formato en el informe de la capacidad gestionada para la copia de seguridad de la máquina virtual sin agente basada en el host ... 1898

Visualización de los valores reales en el origen y en el destino para los tipos de tareas ... 1902

Capítulo 7: Gestión de High Availability ... 1905

Cómo funciona High Availability ... 1906

Gestión de los servicios de control de High Availability ... 1907

Gestión de licencias de High Availability ... 1908

Gestión de escenarios ... 1909

Instalación remota ... 1923

Informes de alta disponibilidad ... 1926

Capítulo 8: Uso de la utilidad VSphereConfig ... 1927

Activación o desactivación de la etiqueta VSPhereBackupNFC mediante el símbolo del sistema ... 1927

Capítulo 9: Uso de la utilidad de diagnóstico 1935

Recopilación de la información de diagnóstico 1936

Recopilación de información de diagnóstico de un agente independiente 1938

Carga de información de diagnóstico al sitio web de Arcserve usando el FTP 1939

Descompresión de registros del Agente 1941

Descompresión de los registros de la consola 1942

Omisión del contenido de la carpeta histórica del registro utilizando el registro 1943

Recopilación de registros del equipo de la puerta de enlace utilizando la línea de comandos 1943

Recopilación de registros del servidor de puntos de recuperación utilizando la línea de comandos 1944

Recopilación de registros de código auxiliar de la instancia de Hyper-V con el agente instalado 1945

Recopilación de mensajes del visor de eventos de Hyper-V 1946

Recopilación de la carpeta CA_LIC y de los archivos OLF 1946

Recopilación de la lista de directorios de los directorios del almacén de datos o del destino de la copia de seguridad 1947

Capítulo 10: Instalación manual de Sophos Intercept X Advanced for Server en Arcserve UDP 1949

Capítulo 11: Aplicación de prácticas recomendables 1955

Prácticas recomendadas para proteger el servidor de Arcserve UDP 1956

Exclusión de archivos desde la exploración de antivirus 1957

Configuración de los parámetros de multitransmisión 1958

Relacionados con Exchange Online 1959

Configuración para obtener un rendimiento óptimo 1960

Prácticas recomendadas para las copias de seguridad 1961

Prácticas recomendadas para la restauración 1963

Preguntas más frecuentes sobre Exchange Online 1964

Relacionados con Microsoft Azure 1965

Prácticas recomendadas para una máquina virtual instantánea en Microsoft Azure 1965

Implementación de Arcserve UDP en Microsoft Azure 1965

Capítulo 12: Solución de problemas 1967

Información relacionada con un error de comunicación de Arcserve UDP 1968

Arcserve UDP no se puede comunicar con nodos de Windows 1969

No se pueden recibir alertas de correo electrónico desde la cuenta de Gmail 1970

Arcserve UDP no se puede comunicar con el servidor de copia de seguridad de Linux de Arcserve UDP en nodos remotos 1971

Arcserve UDP no se puede comunicar con el servidor de puntos de recuperación de Arcserve UDP en nodos remotos 1972

Arcserve UDP no se puede comunicar con el servidor de Arcserve Backup en nodos remotos 1974

Arcserve UDP no se puede comunicar con el sitio remoto 1975

Relacionados con planes, tareas y configuración 1976

Error en la tarea de copia de seguridad tras cambiar la dirección IP o el nombre de host de la Consola 1977

Cómo agregar la contraseña de cifrado para un destino cifrado existente 1978

No se pueden aplicar valores de configuración de la copia de seguridad al nodo 1979

Error en la implementación del plan tras cambiar la contraseña del equipo proxy de copia de seguridad sin agente 1980

Valores de configuración desactivados al abrir la interfaz de usuario del Agente 1981

Error al pausar y reanudar cuando el Agente no está conectado a la red 1982

El servicio del Agente de Arcserve UDP se ejecuta lentamente 1983

Configuración del registro para volver a ejecutar una tarea de copia en cinta 1985

Configuración del registro para copiar varios puntos de recuperación del mismo tipo a la cinta en la misma tarea 1986

Falta un archivo o carpeta de la copia de seguridad de la carpeta compartida de NFS o el nombre de archivo o carpeta está dañado 1987

Error de la copia de seguridad de la carpeta compartida de NFS 1987

Restablecimiento de la Consola de UDP activada para MFA cuando TOTP no está disponible 1987

Relacionados con la máquina virtual instantánea 1994

Error al crear una máquina virtual instantánea en VMware debido a un nombre de almacén de datos de NFS duplicado 1995

Error al crear una máquina virtual instantánea con Windows 2008 R2 como el servidor de recuperación para VMware o el servidor Windows 2008 R2 Hyper-V 1996

Se ha producido un error al iniciar una máquina virtual instantánea si el equipo de origen es un servidor de Active Directory de Windows 2008/2012/2016 1997

Se ha producido un error al encender la máquina virtual después de restaurar Hyper-V 1999

Error en la tarea de máquina virtual instantánea debido a un fallo del servicio NFS de Windows 2000

No se puede acceder o suprimir la carpeta de archivos de la máquina virtual instantánea incluso con privilegios de administrador. 2001

Fallo de inicio de la máquina virtual instantánea en Hyper-V después de reiniciar el servidor de recuperación 2002

Error al crear un almacén de datos de NFS de VMware y aparición del error No se puede determinar el nombre de host 2003

Se ha producido un error al implementar el servicio de integración en la máquina virtual invitada en Hyper-V 2005

Error en la máquina virtual instantánea de Linux en un servidor de Hyper-V en un idioma distinto al inglés 2006

Consumo de una licencia adicional para rutas UNC que se encuentran en una máquina virtual de Hyper-V con licencia 2007

Se produce un error de licencia al cambiar la edición o el tipo de licencia y al crear una máquina virtual instantánea 2007

Relacionados con el Agente de Linux 2009

Configuración del destino de la copia de seguridad desactivada al abrir la interfaz de usuario del Agente de Linux 2010

El estado de la tarea, el historial de tareas y el registro de actividades no son visibles 2011

Se ha producido un error al restaurar el volumen del sistema de SUSE15 con el sistema de archivos XFS 2013

Relacionados con la restauración 2014

No se pueden restaurar los archivos 2015

Adición de la base de datos de contenido restaurado a la aplicación web original 2016

No se puede montar la base de datos mientras se restaura la base de datos de Microsoft Exchange 2019

El campo De no se muestra correctamente en los correos electrónicos enviados por aquellos usuarios que tengan permisos “en nombre de” en un buzón compartido 2021

Se produce un error en las tareas de restauración después las copias de seguridad de la integración sencilla 2022

La restauración a la carpeta compartida de NFS daña el nombre de archivo 2022

Relacionados con las puertas de enlace, los servidores de puntos de recuperación, los almacenes de datos, las consolas y las bases de datos 2024

El nombre del almacén de datos ya está en uso 2025

Error de conexión al almacén de datos debido a un problema de DNS 2026

El almacén de datos se cambia al modo de solo restauración 2027

Error cuando la versión del servidor de puntos de recuperación es inferior a la versión de la Consola 2029

No es posible agregar el mismo recurso en distintos sitios 2031

Cómo activar truncamientos del registro cuando la base de datos SQL está en modo de recuperación completa 2032

En la exploración de puntos de recuperación no se muestran los puntos de recuperación disponibles cuando el RPS está configurado con FQDN 2034

Acceso denegado al agregar el servidor de puntos de recuperación 2035

Asignación de roles y privilegios de administrador a un usuario del dominio 2036

Error de cambio de la vista de UDP para el punto de recuperación 2040

Acceso denegado al agregar o actualizar nodos 2041

Error de apertura de la Consola de UDP tras el cambio de la contraseña del administrador de SQL 2043

Error al montar los puntos de recuperación debido al tiempo de espera 2044

Cómo actualizar las credenciales del servidor de la puerta de enlace 2045

Cómo actualizar la puerta de enlace cuando se cambian las credenciales del proxy de la puerta de enlace 2047

En la Consola se muestra el mensaje: Identity service is starting (El servicio de identidades se está iniciando) 2049

Relacionados con la restauración y la copia de seguridad de la máquina virtual ... 2050

Adición de permisos para VDDK en el nivel del servidor de vCenter ... 2053

La tarea de copia de seguridad para la plantilla de máquina virtual siempre se convierte en copia de seguridad completa y el tamaño de los datos de la copia de seguridad es el tamaño de aprovisionamiento del disco virtual ... 2060

La tarea de copia de seguridad de la plantilla de máquina virtual omite los discos independientes ... 2062

Se produce un error en la tarea de copia de seguridad de la máquina virtual en el recurso compartido de SMB 3.0 con un mensaje de error ... 2064

Se produce un error en la tarea de recuperación de la máquina virtual al restaurar la máquina virtual en un recurso compartido predeterminado de archivos de Windows ... 2065

La información del volumen no está disponible para el punto de recuperación ... 2066

Convierta las copias de seguridad incrementales en copias de seguridad de verificación porque las instantáneas de la máquina virtual se han modificado desde la última tarea de copia de seguridad o requieren una consolidación ... 2067

Se produce un error en la copia de seguridad sin agente para la máquina virtual de VMware si el dispositivo de CD/DVD de la máquina virtual está conectado a una imagen ISO que se encuentra en un almacén de datos de NFS desconectado ... 2068

Se produce un error en la copia de seguridad basada en el host sin agente de la máquina virtual de Hyper-V después de actualizar Arcserve UDP ... 2069

Error en la copia de seguridad sin agente basada en host en VMware ESXi 6.0 ... 2070

La copia de seguridad basada en el host sin agente se bloquea cuando se utiliza Windows 2003 R2 de 64 bits como servidor proxy de la copia de seguridad ... 2072

La copia de seguridad sin agente basada en host no utiliza el modo de transporte HotAdd ... 2073

La tarea de copia de seguridad o restauración sin agente basada en host utiliza el modo de transporte NBD o NBDSSL incluso cuando se puede usar el modo SAN ... 2074

Se ha producido un error al crear una instantánea para las máquinas virtuales de Hyper-V cuando se están ejecutando varias tareas ... 2076

Se ha producido un error en Hyper-V al crear la instantánea VSS ... 2078

Se ha producido un error al realizar la copia de seguridad de un disco virtual debido al error del sistema [El dispositivo no está preparado (21)] ... 2079

Error en la tarea de copia de seguridad ... 2080

Se produce un error al importar máquinas virtuales de VMware desde vCenter ... 2082

Se produce un error en las copias de seguridad debido a la licencia de ESXi ... 2083

El modo de transporte HotAdd no funciona cuando se intenta realizar la copia de seguridad de una máquina virtual de VMware ... 2084

Control más detallado de VSS sobre las desactivaciones del sistema operativo invitado de Windows ... 2086

No se puede configurar la máquina virtual para activar el parámetro Disk.EnableUUID ... 2088

Las operaciones de recuperación producen un error al recuperar datos mediante el modo de transporte HotAdd o SAN ... 2090

Error de recuperación de la máquina virtual al especificar un puerto no predeterminado ... 2092

Error en la tarea de copia de seguridad incremental programada o completa para la máquina virtual de Hyper-V ... 2093

Error en el editor VSS de NTDS de Hyper-V al tomar la instantánea VSS en la máquina virtual ... 2095

No se conservarán los cambios de la dirección de MAC después de la recuperación de máquinas virtuales ... 2096

Se produce un error en la recuperación de la máquina virtual con el error No se pueden abrir archivos VMDK. ... 2097

Problemas causados por UUID de la máquina virtual duplicados ... 2099

Error en la tarea de catálogo del sistema de archivos o error en la comprobación del punto de recuperación para la copia de seguridad sin agente basada en host ... 2101

Conversión de la copia de seguridad incremental en copia de seguridad de verificación o incremento del tamaño de copia de seguridad en Hyper-V ... 2103

Se produce un error en la copia de seguridad basada en el host para la máquina virtual de Hyper-V que tiene una configuración especial de discos diferentes. ... 2105

Error en la tarea de copia de seguridad para una máquina virtual de VMware ... 2106

Desactivación de una nueva exploración de adaptadores HBA durante la copia de seguridad incremental ... 2108

Desactivación de la creación de instantáneas consecutivas en máquinas virtuales de VMware para una copia de seguridad ... 2109

Cuando se restaura desde una versión superior del host de ESXi a una versión inferior del host de ESXi, la máquina virtual se bloquea en la fase de inicio ... 2111

La utilización de la memoria RAM alcanza el 99 % cuando las tareas de copia de seguridad se envían a la máquina virtual ... 2112

Se produce un error en la tarea de restauración de Hyper-V, no se puede conectar a la utilidad del host ... 2113

Se produce un error en la protección automática al detectar y proteger la máquina virtual ... 2115

Establecimiento del tamaño de bloque de lectura cuando se realiza la copia de seguridad de un archivo VMDK ... 2118

Reserva de espacio de LUN heredada mientras se realiza el clon de LUN ... 2118

Relacionados con Virtual Standby ... 2120

Sistema operativo no encontrado ... 2121

Las tareas de Virtual Standby no se pueden realizar debido a errores internos ... 2122

Error en las tareas de Virtual Standby al utilizar el modo de transporte hotadd ... 2125

Las tareas de Virtual Standby realizadas sobre sistemas Hyper-V producen errores ... 2127

Problema relacionado con el UUID de agente duplicado ... 2128

Las modificaciones realizadas en la nube privada virtual en la tarea de Virtual Standby no se reflejan en Amazon EC2 ... 2128

No se muestra la opción Finalizar recursos de EC2 ... 2129

Relacionados con la copia de puntos de recuperación ... 2130

Configuración del registro para la tarea de copia del punto de recuperación ... 2131

Congestión del ancho de banda con las tareas de copia del punto de recuperación a la nube ... 2132

Tarea de combinación omitida ... 2134

Información sobre informes de Arcserve UDP 2136
Cómo mostrar los gráficos para ver informes de Arcserve UDP 2137
Relacionados con Microsoft Office 365 Exchange Online 2140
No se puede ver la lista de buzones en el cuadro de diálogo Seleccionar el destino 2140
Acceso o permiso denegado para el grupo de Exchange Online 2141
Capítulo 13: Apéndice 2143
Herramienta de línea de comandos para el almacén de datos de deduplicación 2144
Cómo mostrar la opción Comprobación del punto de recuperación 2148
Cómo aplicar una versión diferente de VDDK distinta a la incorporada en Arcserve UDP 2151
Modificación del VDDK manualmente para la copia de seguridad de Virtual Standby (VSB) 2151
Modificación del VDDK manualmente para la copia de seguridad basada en el host (HBBU) 2153
Cómo migrar datos de copia de seguridad de Arcserve D2D r16.5 de dos servidores con el mismo nombre de host a un almacén de datos del servidor de puntos de recuperación 2154
Cómo implementar Arcserve UDP en Microsoft Azure 2155
Funcionamiento del flujo del proceso 2155
Consideraciones 2156
Planificación de la implementación de Arcserve UDP en Microsoft Azure 2157
Implementación de Arcserve UDP en Microsoft Azure 2169
Términos y definiciones de Arcserve UDP 2182
Copia de seguridad basada en el agente 2182
Compresión 2182
configuración 2183
cuadro de mandos 2183
Almacén de datos 2183
Destino 2183
Nodos detectados 2183
Cifrado 2184
Deduplicación global 2186
Copia de seguridad sin agente basada en host 2186
Modo de transporte HOTADD 2186
Tarea 2186
tareas 2186
Modo de transporte NBD 2187
Modo de transporte NBDSSL 2187

Nodos 2187
Plan 2187
Nodos protegidos 2187
Evento reciente 2187
Punto de recuperación 2187
Servidor de puntos de recuperación 2188
Replicación 2188
Recursos 2188
Modo de transporte SAN 2188
Sistemas 2188
Tareas 2188
Nodos desprotegidos 2189
Deduplicación de datos 2191
Tipos de deduplicación de datos 2192
Cómo funciona la deduplicación de datos 2193
Cuándo se debe utilizar la deduplicación 2195
Configuración de almacenes de datos de deduplicación en Arcserve UDP 2196
Deduplicación, cifrado y compresión 2198
Limitaciones de la deduplicación 2199

Capítulo 1: Funciones y mejoras

Esta sección explica las funciones o mejoras proporcionadas en cada versión de Arcserve UDP. Arcserve UDP proporciona una solución que incluye todo lo necesario para solucionar los problemas relacionados con el almacenamiento de nueva generación de las organizaciones que tienen, como finalidad, proteger los datos en un mundo que cambia rápidamente y que es virtual, está en la nube y es de servicios. La solución hace esto proporcionando una interfaz de usuario única para una amplia gama de funcionalidades que abarcan la continuidad del negocio de varios sitios y los problemas de preparación ante desastres.

Esta sección proporciona información sobre las nuevas funciones, las mejoras y el soporte.

Esta sección incluye los siguientes temas:

Nuevas funciones

Importante: Para obtener información sobre las funciones más recientes, consulte UDP 8.1.

A continuación, se muestra una lista de las nuevas funciones disponibles en Arcserve UDP 8.0.

- **Copias de seguridad y restaurar desde volúmenes ocultos:** Se permite realizar copias de seguridad y restaurar datos desde volúmenes ocultos. El volumen oculto es un volumen que se monta sin una letra de unidad o una ruta de carpeta en el sistema operativo. Se puede acceder a los volúmenes ocultos mediante el GUID del volumen correspondiente.
- **Configuración de exportación e importación:** Se permite la configuración de exportación e importación mediante el archivo JSON en el Agente de Windows.
- **Compatibilidad con OneDrive:** Opciones de restauración permitidas a las ubicaciones originales o alternativas.
- **Compatibilidad con SharePoint Online:** Las funciones siguientes están disponibles para la compatibilidad con SharePoint Online:
  - Se permite realizar copias de seguridad de listas y bibliotecas de sitios personales.
  - Se permite agregar varias recopilaciones de sitios a la vez.
  - Se permite agregar automáticamente las recopilaciones de sitios recién agregadas dentro del plan.
- **Compatibilidad con Oracle RMAN:** Arcserve UDP ahora proporciona una forma de proteger el sistema Oracle mediante Recovery Manager (RMAN). RMAN es una utilidad de Oracle que realiza tareas de copia de seguridad, restauración y recuperación en bases de datos y automatiza la administración de estrategias de copia de seguridad. Para obtener más información, consulte Protección del sistema Oracle mediante Recovery Manager (RMAN).
- **Compatibilidad de grupo de Office 365:** Se ha activado la compatibilidad de grupo para los usuarios de Office 365.
- **Replicación inversa:** Se ha activado la replicación de datos (punto de recuperación) desde la nube, MSP o el servidor de puntos de recuperación gestionado de forma remota a un servidor de puntos de recuperación local o de UDP. Para obtener más información, consulte Cómo realizar la replicación inversa.

- **Nutanix Files:** Arcserve UDP ahora proporciona una forma de proteger Nutanix Files mediante la opción UNC/NFS de Arcserve UDP. Nutanix Files es una solución de almacenamiento de archivos escalable y definida por software que proporciona un repositorio para datos no estructurados como, por ejemplo, directorios principales, perfiles de usuario, recursos compartidos de departamentos, registros de aplicaciones, copias de seguridad y archivos de archivado. Para obtener más información, consulte Protección de la ruta UNC/NFS.
- **Compatibilidad con Teams:** La compatibilidad con la copia de seguridad y restauración de datos está activada para MS Teams, que es una plataforma de conversación para la comunicación empresarial. Para obtener más información, consulte Gestión de la copia de seguridad y restauración de Microsoft Teams.
- **Compatibilidad con el almacenamiento inmutable para la copia del punto de recuperación:** Se permite crear almacenamiento inmutable en Amazon S3 utilizando la función Bloqueo de objetos.
- **Reemplazo de Adobe Flash:** Adobe Flash ya no es necesario y la instalación de .NET Framework permite ver gráficos.

Mejoras de funcionalidades

Importante: Para obtener información sobre las últimas mejoras de funciones, consulte UDP 8.1.

- **Cambios en PowerCLI:** Se activan las siguientes opciones para los archivos de registro UDPPowerCLI.log:
  - Se permite cambiar la ubicación de los archivos de registro de PowerCLI de UDP.
  - Se permite controlar el tamaño máximo de los archivos de registro mediante la circulación de registros.
  - La marca de tiempo en los archivos de registro se cambia al formato de 24 horas.
  - Se permite la política de retención basada en el período de retención para los archivos de registro de PowerCLI de UDP.
  - Se permite la política de retención basada en el número de retención de archivos para los archivos de registro de PowerCLI de UDP.
- **Mejora en la instantánea:** Se ha activado el plan de copia de seguridad del Agente de Arcserve UDP (Windows/Linux) y el plan de copia de seguridad sin agente basada en el host (Nutanix/ESXI/Hyper-V) para ejecutar el script posterior a la instantánea incluso cuando se produce un error en la instantánea.
- **Autenticación moderna:** Se ha activado la autenticación moderna para la copia de seguridad y la restauración de Office 365.
- **Especificación de la red para la restauración y replicación:** Se ha activado la restauración y la replicación mediante una red para establecer la comunicación entre el Agente de Windows y el servidor de puntos de recuperación.
- **Especificación de la red para Linux:** Se ha activado la copia de seguridad y la restauración mediante una red para establecer la comunicación entre el Agente de Linux y el servidor de puntos de recuperación.
- **Máquina virtual instantánea simultánea:** Se permite crear y configurar máquinas virtuales instantáneas simultáneas en varios hipervisores mediante la Consola de Arcserve UDP.
- **Virtual Standby simultánea:** Se permite configurar máquinas de Virtual Standby simultáneas mediante la Consola de Arcserve UDP.

Mejoras del Agente de Linux

Importante: Para obtener información sobre las últimas mejoras del Agente de Linux, consulte UDP 8.1.

- Nuevas plataformas compatibles:
  - Red Hat Enterprise Linux 8.3
  - CentOS 7.9, 8.3
  - Oracle Linux 8.3
  - Debian Linux 9.12, 9.13, 10.6, 10.7
- **Especificación de la red para Linux:** Se ha activado la copia de seguridad y la restauración mediante una red para establecer la comunicación entre el Agente de Linux y el servidor de puntos de recuperación.
- **Máquina virtual instantánea simultánea:** Se permite crear y configurar máquinas virtuales instantáneas simultáneas en varios hipervisores mediante la Consola de Arcserve UDP.
- **Mejora en la instantánea:** Se ha activado el plan de copia de seguridad del Agente de Linux de Arcserve UDP para ejecutar el script posterior a la instantánea incluso cuando se produce un error en la instantánea.
- **Reemplazo de Adobe Flash:** Adobe Flash ya no es necesario para ver gráficos en el Agente de Linux.

Compatibilidad con la plataforma y la base de datos

Importante: Para obtener información sobre la compatibilidad más reciente con la plataforma y la base de datos, consulte UDP 8.1.

- Nutanix AOS 5.19
- Red Hat Enterprise Linux 8.3
- CentOS 7.9, 8.3
- Oracle Linux 8.3
- Debian Linux 9.12, 9.13, 10.6, 10.7
- VMware vSphere 7.0 Update 1
- Oracle Database 19c
- Nutanix Files 3.8.z, 3.7.z, 3.6.z

Mejoras de seguridad y aplicaciones de terceros

Importante: Para obtener información sobre las últimas mejoras de seguridad y de terceros, consulte UDP 8.1.

- **Compatibilidad con Open JDK:** La versión de Open JDK se ha actualizado a 1.8.0.265.b01
- **Compatibilidad con VMware Virtual Disk Development Kit:** La versión de VDDK se ha actualizado a 7.0. 1.40833
- **Compatibilidad con el SDK de los servicios web de VMware vSphere:** La versión del SDK se ha actualizado a 6.7.1
- **Compatibilidad con WSO2:** La versión de WSO2 se ha actualizado a v5.7.0
- **Compatibilidad con Apache:** La versión de Apache se ha actualizado a 2.4.46
- **Compatibilidad con OpenSSL:** La versión de OpenSSL se ha actualizado a la versión 1.1.1i
- **Compatibilidad con Tomcat:** La versión de Tomcat se ha actualizado a la versión 9.0.37
- **Compatibilidad con SQLite:** La versión de SQLite se ha actualizado a 3.26
- **AWS SDK para Java:** La versión de AWS SDK para Java se ha actualizado a 1.11.852
- **AWS SDK para C ++:** La versión de AWS SDK para C ++ se ha actualizado a 1.6.53

Mejoras del Dispositivo de Arcserve

Importante: Para obtener información sobre las últimas mejoras del Dispositivo, consulte UDP 8.1.

Los clientes del Dispositivo existente pueden actualizar a Arcserve UDP 8.0. Para obtener más información, consulte Instalación.

Funciones eliminadas

Importante: Para obtener información sobre los elementos con compatibilidad eliminada, consulte UDP 8.1.

- Compatibilidad con vSphere 5.5. Se recomienda encarecidamente actualizar el entorno (vCenter/ESXi) a la última versión compatible de VMware. Para obtener más información sobre el fin de la compatibilidad general para vSphere 5.5, consulte el artículo de la base de conocimiento.
- Nutanix AHV 5.5.3.1.

Capítulo 2: Funcionamiento de Arcserve UDP

Esta sección incluye los siguientes temas:

Introducción

Arcserve Unified Data Protection es una solución completa para proteger entornos de TI complejos. La solución protege los datos que están residiendo en diversos tipos de nodos como, por ejemplo, Windows, Linux y máquinas virtuales en servidores ESX de VMware, en servidores Microsoft Hyper-V y en servidores Nutanix AHV. Se puede realizar la copia de seguridad de datos en un equipo local o en un servidor de puntos de recuperación. Un servidor de puntos de recuperación es un servidor central donde se almacenan copias de seguridad de varios orígenes.

Arcserve UDP proporciona las capacidades siguientes:

- Protege diversos tipos de nodos de origen, incluyendo el nodo basado en el agente, el nodo sin agentes, CIFS, Exchange Online, SharePoint Online, OneDrive, etc.
- Realiza la copia de seguridad de datos en servidores de punto de recuperación.
- Replica datos de copia de seguridad en servidores de puntos de recuperación remotos y locales.
- Controla Arcserve High Availability
- Archiva datos.
- Copia:
  - Archivos de origen seleccionados a una ubicación de la copia de seguridad secundaria.
  - Puntos de recuperación a ubicaciones de la nube y locales como la carpeta de recursos compartidos y EC2 AWS.
  - Puntos de recuperación a cinta.
- Crea
  - Máquinas de Virtual Standby a partir de datos de copia de seguridad en el hipervisor local (Hyper-V, ESX, Nutanix), AWS EC2 o Microsoft Azure
  - Máquina virtual instantánea en el hipervisor local (Hyper-V, ESX, Nutanix) para Windows
  - Máquina virtual instantánea en el hipervisor local (Hyper-V, ESX, Nutanix), AWS EC2 o Microsoft Azure para Linux

- Restaura
  - Datos de copia de seguridad y realiza una reconstrucción completa.
  - Objetos de correo electrónico y objetos que no lo son de Microsoft Exchange mediante la utilidad Exchange Granular Restore de Arcserve UDP.

    Nota: Para obtener más detalles sobre las especificaciones compatibles, las funciones y otras características, consulte la Guía del usuario de Exchange Granular Restore (esr.pdf).
- Es compatible con
  - La administración basada en roles
  - La instantánea de hardware
  - Prueba de recuperación asegurada para los puntos de recuperación.
  - Informe de acuerdo de nivel de servicio para RTO y RPO

Arcserve UDP replica los datos de copias de seguridad que se guardan como puntos de recuperación desde un servidor en otro servidor de puntos de recuperación. Se pueden crear también máquinas virtuales a partir de los datos de copia de seguridad que pueden actuar como equipos en espera cuando se produce un error en el nodo de origen. La máquina virtual en espera se crea convirtiendo puntos de recuperación al formato de máquina virtual de VMware ESX, Microsoft Hyper-V o Nutanix AHV.

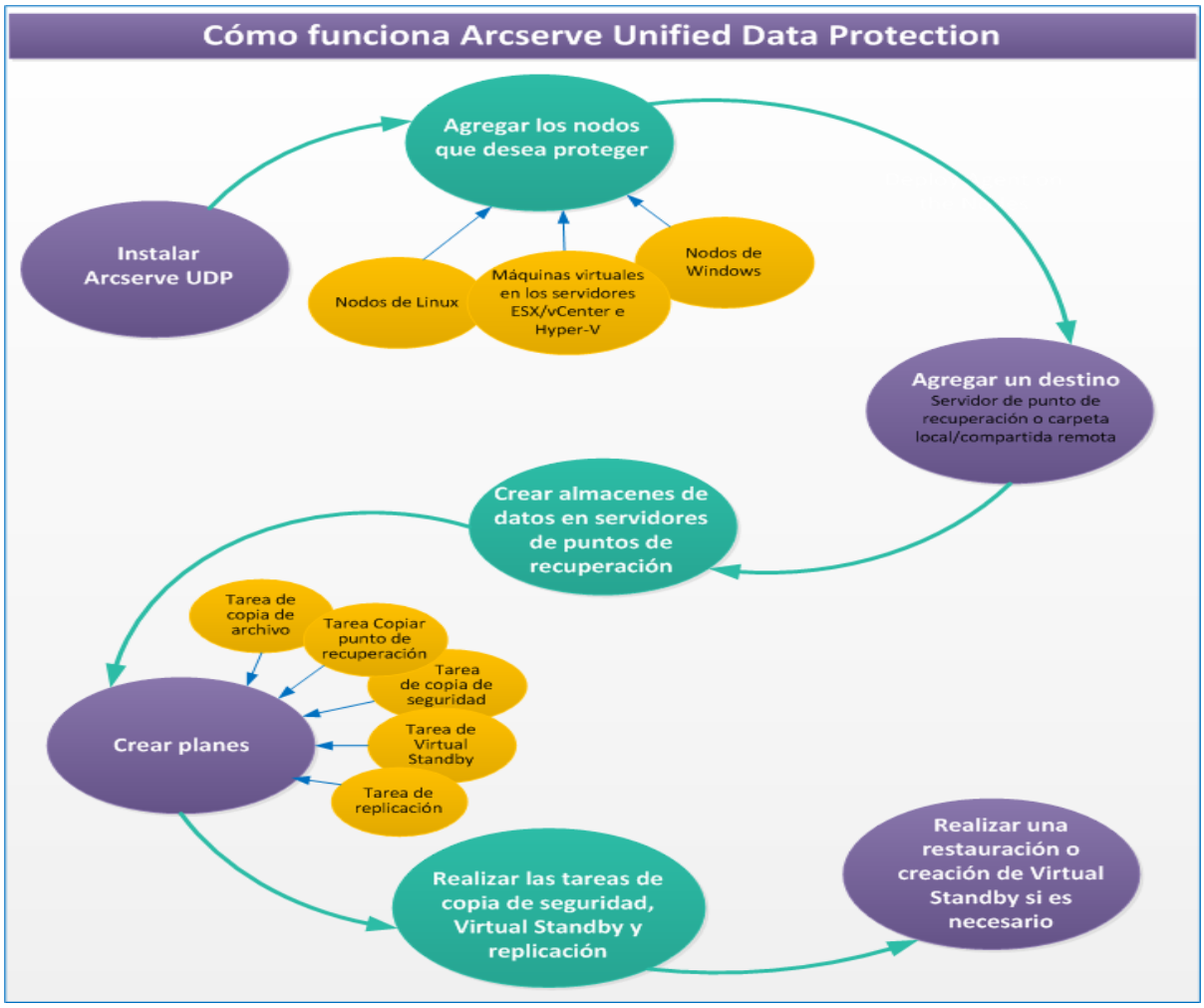
La solución Arcserve UDP proporciona integración con Arcserve High Availability. Después de crear escenarios en Arcserve High Availability, se pueden gestionar y controlar los escenarios y realizar operaciones como agregar o suprimir equipos de destino.

Cómo funciona Arcserve UDP

Arcserve UDP es una solución de protección de datos unificada que le permite proteger sus sistemas informáticos. Utilice los siguientes pasos de nivel alto para proteger los sistemas utilizando Arcserve UDP.

1. Instalación de Arcserve Unified Data Protection.
2. Agregar nodos que se desean proteger. Se pueden agregar máquinas virtuales y nodos de Windows o Linux en servidores ESX/vCenter, servidores Hyper-V y servidores Nutanix AHV.
3. Agregar un destino. Un destino puede ser un servidor de punto de recuperación, carpeta local o carpeta compartida remota.
4. Crear almacenes de datos en servidores de puntos de recuperación. Un almacén de datos es una zona física de un disco. Se pueden crear almacenes de datos de deduplicación y de no deduplicación.
5. Crear un plan. Un plan es un grupo de tareas para gestionar la copia de seguridad, la replicación, la copia de punto de recuperación, la copia en cinta, la creación de máquinas de Virtual Standby o la prueba de recuperación asegurada. También se puede agregar la Ruta UNC, el nodo de Office 365 Exchange Online, el nodo de SharePoint Online o el nodo de OneDrive y crear tareas relacionadas.
6. Realizar tareas como copia de seguridad, crear Virtual Standby y replicación.
7. Realizar una restauración simple o una reconstrucción completa.

   El diagrama siguiente ilustra los pasos de nivel alto que es necesario realizar para proteger datos:


Cómo funciona Arcserve Unified Data Protection
Agregar los nodos que desea proteger
Instalar Arcserve UDP
Nodos de Linux
Máquinas virtuales en los servidores ESX/vCenter e Hyper-V
Nodos de Windows
Agregar un destino
Servidor de punto de recuperación o carpeta local/compartida remota
Crear almacenes de datos en servidores de puntos de recuperación
Tarea de copia de archivo
Tarea Copiar punto de recuperación
Tarea de copia de seguridad
Tarea de Virtual Standby
Tarea de replicación
Crear planes
Realizar las tareas de copia de seguridad, Virtual Standby y replicación
Realizar una restauración o creación de Virtual Standby si es necesario

Máquina virtual instantánea (IVM) frente a la máquina de Virtual Standby (VSB)

Mientras se restauran datos después de un desastre o durante la formación de la recuperación ante desastres, es posible que se deban iniciar las instancias virtualizadas de los servidores que Arcserve UDP protegía anteriormente.

Arcserve UDP proporciona las siguientes dos funciones que permiten iniciar la máquina virtual desde los puntos de recuperación:

- **Máquina virtual instantánea (IVM)**: Crea una máquina virtual de manera instantánea desde un punto de recuperación. El uso de una máquina virtual instantánea ayuda a acceder de forma inmediata a los datos y aplicaciones presentes en las sesiones de copia de seguridad de Arcserve UDP. Una máquina virtual instantánea elimina el tiempo de reposo asociado a una restauración tradicional o conversión de la sesión de copia de seguridad a una máquina física o virtual.

  Para obtener más detalles sobre la máquina virtual instantánea, consulte Cómo crear y gestionar una máquina virtual instantánea.

- **Máquina de Virtual Standby:** Convierte los puntos de recuperación a formatos de máquina virtual y prepara una instantánea para poder recuperar fácilmente los datos cuando sea necesario. Esta función también proporciona la capacidad de alta disponibilidad y garantiza que la máquina virtual puede tomar el control inmediatamente cuando se produce un error en el equipo de origen. La máquina de Virtual Standby se crea convirtiendo los puntos de recuperación a cualquier formato de máquina virtual de VMware, Hyper-V o Nutanix AHV.

  Para obtener más detalles sobre Virtual Standby, consulte Cómo crear un plan de Virtual Standby.

Para determinar qué función funciona mejor, es necesario tener en cuenta el objetivo de tiempo de recuperación (RTO) y el escenario. La tabla siguiente proporciona la comparación entre las funciones de la máquina virtual instantánea y la máquina de Virtual Standby:

FUNCIONES	MÁQUINA VIRTUAL INSTANTÁNEA	MÁQUINA DE VIRTUAL STANDBY
Máquinas virtuales en alimentación del modo en espera desde el último punto de recu-	Sí (no se necesita conversión)	Sí, SOLO si se ha agregado una tarea de VSB al plan de copia de seguridad. Por ejemplo, se necesita la planificación avanzada.

peración		
Requiere el proceso del tiempo de la copia de seguridad	No requerido	Obligatorio, es necesario para agregar una tarea de VSB al plan que se utiliza para realizar la copia de seguridad de la máquina de origen.
Tiempo de arranque de la máquina virtual	Un proceso más lento (hasta un 30 %) debido a un redireccionamiento de E/S.	El mismo tiempo que cualquier otra máquina virtual que se encuentre en el mismo hipervisor.
Requisitos de espacio en disco	Espacio de almacenamiento mínimo para hospedar a un disco secundario o para almacenar cambios al ejecutar una máquina virtual.	Sí, se consume el espacio de almacenamiento en el hipervisor de destino donde se mantiene la máquina virtual en espera de Virtual Standby. Requiere que el espacio de almacenamiento sea igual a o mayor que el tamaño de la máquina de origen.
Opción de alta disponibilidad (HA)	N/D	DISPONIBLE Monitoriza el equipo de origen y puede iniciar la máquina virtual de VSB si el equipo de origen deja de estar disponible.
Rendimiento de la máquina virtual	Es posible que se ejecute más lentamente que las máquinas virtuales normales (hasta un 30 %) a causa del redireccionamiento de E/S. Sin embargo, el rendimiento depende de la naturaleza de la carga de trabajo de la aplicación.	El rendimiento es el mismo que el de las máquinas virtuales normales.
Gestión y configuración	Se gestiona desde la Consola de UDP, se puede iniciar o detener la máquina virtual instantánea a petición cuando el usuario requiere tener acceso.	Se ha agregado como una tarea a un plan para que todos los datos de la copia de seguridad se conviertan automáticamente en un formato de máquina virtual. La tarea de VSB se aplica a todos los nodos que están protegidos por el plan.
Conservación de los datos y migración de la máquina virtual a producción	El disco virtual de la máquina virtual instantánea hace referencia a los bloques de datos que se encuentran en el punto de recuperación y desde los que se ha iniciado la máquina virtual. Por lo tanto, cuando la máquina virtual instantánea accede a los bloques de datos del disco virtual, los datos se solicitan realmente al servidor de	El disco o los discos virtuales de la máquina virtual de VSB ya contienen la mayor parte de los datos recientes desde el punto de recuperación correspondiente. Dado que el redireccionamiento de E/S no se produce (que es lo mismo que la máquina virtual instantánea), el rendimiento de la máquina virtual de VSB es el mismo que el de las máquinas virtuales nor-

	puntos de recuperación (este proceso es transparente para el usuario). Tal redireccionamiento de E/S genera un impacto adicional en el rendimiento. Si se pretende utilizar la máquina virtual instantánea en producción, se recomienda hacer que la máquina virtual instantánea sea persistente y rellenar el disco virtual de la máquina virtual con los datos reales. Al copiar o replicar la máquina virtual, se puede rellenar la máquina virtual instantánea. En función del tipo de hipervisor utilizado en el entorno de producción, para conservar los datos de la máquina virtual instantánea se puede utilizar la replicación o la migración de almacenamiento de la máquina virtual de Hyper-V o VMware Storage vMotion para copiar la máquina virtual instantánea donde los datos se conviertan en permanentes.	males cuando no hay ninguna dependencia en el servidor de puntos de recuperación o en el punto de recuperación (en comparación con el escenario de la máquina virtual instantánea).

Seguridad del usuario

Esta sección incluye los siguientes temas:

- Roles para los servicios de Arcserve UDP
- Privilegios de usuario para las funciones de Arcserve UDP

Roles para los servicios de Arcserve UDP

La tabla siguiente describe los roles para los servicios de Arcserve UDP:

Servicio	Descripción	Rol en el que se ejecuta
Supervisión del registro de eventos de Arcserve	Proporciona el servicio del SDK de licencias para aceptar las claves de licencia.	Consola/servidor de puntos de recuperación/agente
Servicio de extensión del explorador del agente de Arcserve UDP	Proporciona el servicio back-end para la vista de UDP en el Explorador de Windows.	Servidor de puntos de recuperación/agente
Servicio del Agente de Arcserve UDP	Proporciona la interfaz de usuario web y el servicio web para el Agente de Arcserve UDP, incluyendo el envío de la tarea de restauración o copia de seguridad.	Servidor de puntos de recuperación/agente
Servicio de identidad de Arcserve UDP	Proporciona el servicio de autenticación y autorización para la Consola de Arcserve Unified Data Protection.	Consola
Servicio de uso compartido de puertos de gestión de Arcserve UDP	Proporciona el servicio de uso compartido de puertos que permite a la consola, a la puerta de enlace y al servidor de identidad compartir un solo puerto.	Consola
Consola de gestión de Arcserve UDP	Proporciona el servicio web para la Consola de gestión central de Arcserve Unified Data Protection.	Consola
Servicio de puerta de enlace de gestión remota de Arcserve	Proporciona la capacidad de controlar las solicitudes bidireccionales entre la puerta de enlace y la consola a través de la intranet o Internet.	Puerta de enlace
Servicio de almacén de datos del servidor de puntos de recuperación de Arcserve UDP	Proporciona el servicio web para la gestión del almacén de datos de UDP incluyendo la creación, la modificación, la supresión, el inicio y la detención.	Servidor de puntos de recuperación
Servicio de uso compartido de puertos del servidor de puntos de recuperación de Arcserve	Solo se muestra un puerto para que el servidor de puntos de recu-	Servidor de puntos de recuperación

UDP	peración pueda gestionar la comunicación con la interfaz de usuario web o servicio del agente, el servicio web del servidor de puntos de recuperación y la tarea de replicación.	
Servicio de actualización de Arcserve UDP	Detecta una actualización de Arcserve UDP y la descarga, si está disponible.	Consola/servidor de puntos de recuperación/agente

Privilegios de usuario para las funciones de Arcserve UDP

La tabla siguiente describe los privilegios de usuario para las funciones de Arcserve UDP:

Funciones	Usuario	Privilegio	Comentarios
Instalación	**Grupo de administradores locales**	**Grupo de administradores locales**	
Consola y puerta de enlace	**Grupo de administradores locales**	**Grupo de administradores locales**	
Servidor de puntos de recuperación	**Grupo de administradores locales**	**Grupo de administradores locales**	
Copia de seguridad del cliente de Windows	**Grupo de administradores locales**	**Grupo de administradores locales** Políticas de seguridad: • Actuar como parte del sistema operativo • Inicio de sesión local • Inicio de sesión como servicio • Inicio de sesión como tarea de proceso por lotes	**Muchas de las operaciones relacionadas con la copia de seguridad, como la instantánea VSS, requieren privilegios de administrador.**
Recurso compartido de la red para el almacén de datos sin deduplicación	Si se activa el Control de cuentas de usuario del servidor de puntos de recuperación, el administrador integrado o la		

	cuenta del dominio.		
Truncamiento del registro de SQL	Grupo de administradores locales	Administrador local con el rol de la base de datos sysadmin de SQL o db_owner fijado.	El truncamiento del registro requiere la consulta de la base de datos de copias de seguridad, la lista de trabajos pendientes y la reducción de consultas (reducción de la base de datos).
Truncamiento del registro de Exchange	Grupo de administradores del dominio	Grupo de administradores del dominio	Debe tener acceso a la base de datos de Exchange.
Protección de Active Directory	Grupo de administradores del dominio	Grupo de administradores del dominio	
Restauración del cliente de Windows			
Recurso compartido de la red para el almacén de datos sin deduplicación	Si se activa el Control de cuentas de usuario del servidor de puntos de recuperación, el administrador integrado o la cuenta del dominio.		
SQL	Grupo de administradores locales	Administrador local con el rol de la base de datos sysadmin de SQL o db_owner fijado.	
Exchange	Grupo de administradores del dominio	Grupo de administradores del dominio	Debe tener acceso a la base de datos de Exchange.
Active Directory	Grupo de administradores del dominio	Grupo de administradores del dominio	
Utilidad Exchange Granular Restore	Restauración en el buzón de correo: La cuenta utilizada para la restauración debe disponer del privilegio para suplan-	Restauración en el buzón de correo: La cuenta que se utiliza para la restauración debe	

	tar en el buzón de correo de destino. Para las otras opciones de restauración, la cuenta no necesita ningún requisito especial.	disponer del privilegio para suplantar en el buzón de correo de destino. Para otras opciones de restauración, no hay ningún requisito especial en la cuenta.	
Copia de seguridad sin agente basada en el host			
Agregar el nodo de la máquina virtual desde vCenter/ESXi	• vCenter: Administrador integrado • ESXi: raíz		Para vCenter, si desea utilizar un administrador que no sea integrado, consulte este vínculo.
Agregar nodo de la máquina virtual desde Nutanix AHV	Administrador del clúster o Administrador de usuarios	Administrador del clúster o Administrador de usuarios	
Agregar el nodo de la máquina virtual desde Hyper-V	• Hyper-V independiente: Administrador local integrado, administrador del dominio integrado o cuenta del dominio que es miembro del grupo de administradores locales. • Clúster de Hyper-V: Administrador del dominio integrado o cuenta del dominio que es miembro del grupo de administradores locales.		Si se utiliza una cuenta administrativa distinta, se debe desactivar el acceso remoto de UAC. Consulte el vínculo.
Cambiar el método de desactivación de la instantánea de VMware en el	Administrador local integrado o administrador del dominio integrado		Si se utiliza una cuenta administrativa distinta,

plan	**Nota:** Las credenciales necesarias aquí se configuran mediante la opción Actualizar nodo.		se debe desactivar la función UAC. Consulte el vínculo.
Restauración a nivel de la base de datos de la aplicación para la máquina virtual de Hyper-V o la máquina virtual de Nutanix	Administrador local integrado, administrador del dominio integrado o cuenta del dominio que es miembro del grupo de administradores locales. **Notas:** • Las credenciales necesarias aquí se configuran mediante la opción Actualizar nodo. • Si el sistema operativo invitado de la máquina virtual es la versión de cliente de Windows (por ejemplo, Windows 10), se deberá configurar manualmente el cortafuegos para permitir el servicio Windows Management Instrumentation (WMI).		Si se utiliza una cuenta administrativa distinta, se debe desactivar el acceso remoto de UAC. Consulte el vínculo.
PFC	• Máquina virtual de VMware: Administrador local integrado o administrador del dominio integrado • Máquina virtual de Hyper-V: Administrador local integrado, administrador del		Si se utiliza una cuenta administrativa distinta: • La función UAC debe desactivarse para la máquina virtual de VMware. Consulte

	dominio integrado o cuenta del dominio que es miembro del grupo de administradores locales. • Máquina virtual de Nutanix: Administrador local integrado, administrador del dominio integrado o cuenta del dominio que es miembro del grupo de administradores locales. **Notas:** • Las credenciales necesarias aquí se configuran mediante la opción Actualizar nodo. • Para la máquina virtual de Hyper-V o de Nutanix, si el sistema operativo invitado de la máquina virtual es la versión de cliente de Windows (por ejemplo, Windows 10), se deberá configurar manualmente el cortafuegos para permitir el servicio Windows Management Instrumentation		este vínculo. • El acceso remoto de UAC debe desactivarse para la máquina virtual de Hyper-V. Consulte este vínculo.

	(WMI).		
Comando previo/posterior	• Máquina virtual de VMware: Administrador local integrado o administrador del dominio integrado • Máquina virtual de Hyper-V: Administrador local integrado, administrador del dominio integrado o cuenta del dominio que es miembro del grupo de administradores locales. • Máquina virtual de Nutanix: Administrador local integrado, administrador del dominio integrado o cuenta del dominio que es miembro del grupo de administradores locales. **Notas:** • Las credenciales necesarias aquí se establecen mediante la opción Actualizar nodo y en la ficha Opciones avanzadas de un plan. • Para la máquina virtual de Hyper-V, si el sistema ope-		Si desea utilizar las credenciales establecidas mediante la opción Actualizar nodo y en la ficha Opciones avanzadas de un plan, consulte este vínculo.

	rativo invitado de la máquina virtual es la versión de cliente de Windows (por ejemplo, Windows 10), se deberá configurar manualmente el cortafuegos para permitir el servicio Windows Management Instrumentation (WMI). • Para la máquina virtual de Hyper-V o de Nutanix, si el sistema operativo invitado de la máquina virtual es la versión de cliente de Windows (por ejemplo, Windows 10), se deberá configurar manualmente el cortafuegos para permitir el servicio Windows Management Instrumentation (WMI).		
Truncamiento del registro de SQL	Igual que Comando previo/posterior		Igual que Comando previo/posterior
Truncamiento del registro de Exchange	Igual que Comando previo/posterior		Igual que Comando previo/posterior
Restauración a nivel del archivo en la ubicación original	Administrador local integrado, administrador del dominio integrado o cuenta del dominio que		Si se utiliza una cuenta administrativa distinta, se debe desactivar

	es miembro del grupo de administradores locales. **Notas:** • Las credenciales necesarias aquí se configuran mediante la opción Actualizar nodo. • Para la máquina virtual de Hyper-V o de Nutanix, si el sistema operativo invitado de la máquina virtual es la versión de cliente de Windows (por ejemplo, Windows 10), se deberá configurar manualmente el cortafuegos para permitir el servicio Windows Management Instrumentation (WMI).		el acceso remoto de UAC. Consulte este vínculo.
Virtual StandBy			
Para Hyper-V	• Administrador local integrado • Administrador del dominio integrado • La cuenta del dominio que es miembro del grupo de administradores locales. • La cuenta local que es miembro del grupo de administradores locales.	Grupo de administradores locales	Si se utiliza una cuenta administrativa local, se debe desactivar el acceso remoto de UAC. Consulte este vínculo.

Para Nutanix	Administrador del clúster	Administrador del clúster	
Para VMware	• vCenter: Administrador integrado • ESXi: raíz		Para vCenter, si desea utilizar un administrador que no sea integrado, consulte este vínculo.
Máquina virtual instantánea/recuperación asegurada			
Para Hyper-V	• Administrador local integrado • Administrador del dominio integrado • La cuenta del dominio que es miembro del grupo de administradores locales. • La cuenta local que es miembro del grupo de administradores locales.		Si se utiliza una cuenta administrativa local, se debe desactivar el acceso remoto de UAC. Consulte este vínculo.
Para VMware	• vCenter: Administrador integrado • ESXi: raíz	Grupo de administradores locales	Para vCenter, si desea utilizar un administrador que no sea integrado, consulte este vínculo.
Copia de archivo y archivado	**Grupo de administradores locales**	**Grupo de administradores locales**	
Copiar punto de recuperación en la nube	**Grupo de administradores locales**	**Grupo de administradores locales**	
Protección de la ruta UNC/NFS	**Cualquier usuario puede iniciar sesión y ser suplantado**	**Permiso de lectura en la ruta UNC/NFS**	
Virtual StandBy a AWS EC2	**Los usuarios de Amazon IAM que tienen los permisos necesarios para la interacción con la API de**		Para AWS EC2, consulte este vínculo.

	AWS		
Virtual StandBy a Microsoft Azure	**Aplicación**	**Rol de colaborador de la suscripción seleccionada**	
Linux			
Instalación	root	Lectura, escritura, ejecución	
Registro de la consola	Administrador de la consola		
Copia de seguridad basada en el agente			
-Recurso compartido de red	Administrador de almacenamiento	Lectura, escritura	
Conexión del nodo	root/no root/sudo	Lectura, escritura, ejecución	
Restauración a nivel del archivo			
-Recurso compartido de red	Administrador de almacenamiento	Lectura, escritura	
Conexión del nodo	root/no root/sudo	Lectura, escritura, ejecución	El usuario root puede realizar la restauración en cualquier ubicación. Los otros usuarios pueden realizar la restauración solamente en los directorios propios.
Reconstrucción completa		Información de acceso del hardware	
BMR de migración			
Máquina virtual instantánea para Hyper-V			
Máquina virtual instantánea para VMware			
Máquina virtual instantánea para Nutanix AHV	Administrador del clúster	Administrador del clúster	
Máquina virtual instantánea a Amazon EC2	**Usuario de IAM**	**Acceso completo de EC2**	

Máquina virtual instantánea a Microsoft Azure	Aplicación	Rol de colaborador de la suscripción seleccionada	
Protección de Exchange Online	Cualquier cuenta de Exchange Online	Dispone del privilegio de suplantación de la aplicación en la cuentas protegidas	
Protección de SharePoint Online	Administrador de la colección de sitios de SharePoint Online	Administrador de la colección de sitios de SharePoint Online	
OneDrive	Administradores de Azure Active Directory	Administradores de Azure Active Directory	

Capítulo 3: Instalación de Arcserve UDP

Esta sección incluye los siguientes temas:

Cómo instalar Arcserve UDP

Arcserve UDP - Completa: Después de la instalación, inicie sesión en la Consola de Arcserve UDP y realice las funciones de gestión de datos. La Consola le permite gestionar y controlar nodos, servidores de puntos de recuperación, copias de seguridad, restauraciones y replicaciones.

Arcserve UDP - Agente: Instala solamente el Agente de Arcserve UDP. Instale el agente en los nodos que se desea proteger. Realice este paso solamente cuando se desea instalar el agente manualmente en un nodo. Normalmente, el agente se implementa automáticamente en los nodos desde donde se ha creado un plan.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Selección del tipo de instalación
3. Instalación de Arcserve Unified Data Protection mediante el Asistente de instalación
4. Instalación de Arcserve Unified Data Protection mediante la línea de comandos
5. Instalación de Arcserve Unified Data Protection con el instalador unificado
6. Verificación de la instalación
7. (Opcional) Puertos de comunicación utilizados
8. (Opcional) Cómo afecta el proceso de instalación a los sistemas operativos

Revisión de las consideraciones y requisitos previos

Revise los siguientes requisitos previos y las consideraciones de instalación antes de instalar Arcserve UDP:

Requisitos previos

- Revise las Notas de la versión de Arcserve UDP 8.0. Las Notas de la versión contienen una descripción de los requisitos del sistema, los sistemas operativos compatibles y una lista de problemas conocidos para esta versión.
- Verifique que los sistemas cumplen con los requisitos de software y hardware necesarios para instalar los componentes de Arcserve Unified Data Protection.
- Verifique que la cuenta de Windows dispone de privilegios de administrador o de cualquier otro privilegio similar para instalar software en los equipos donde se van a instalar los componentes de Arcserve Unified Data Protection.
- Verifique que dispone de los nombres de usuario y contraseñas de los sistemas donde se están instalando los componentes de Arcserve Unified Data Protection.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Consideraciones

Antes de llevar a cabo la instalación, se debe decidir cómo configurar la instalación de Arcserve Unified Data Protection:

- El sistema donde se desea instalar la Consola.
- Los nodos que se desean proteger.
- El número de servidores de punto de recuperación que servirán como destinos de la copia de seguridad.
- El número de servidores de réplica que replicarán a los servidores de punto de recuperación.

Selección del tipo de instalación

Se puede instalar Arcserve UDP mediante cualquiera de los métodos siguientes:

- **Instalación estándar mediante el asistente para la instalación:** Este método le permite instalar Arcserve Unified Data Protection mediante el asistente para la instalación. En este método, se pide en cada paso que elija las opciones deseadas.
- **Instalación silenciosa mediante la línea de comandos:** este método le permite realizar una instalación desatendida mediante la línea de comandos de Windows.
- **Instalación utilizando el instalador unificado:** Este método le permite instalar Arcserve UDP, Arcserve Backup y Arcserve RHA desde un único instalador. Puede instalar todos los tres productos a la vez o cada producto por separado. El programa de instalación se puede descargar del sitio web de Arcserve.

Instalación de Arcserve Unified Data Protection mediante el Asistente de instalación

Arcserve Unified Data Protection permite gestionar y controlar centralmente los nodos, servidores de puntos de recuperación, máquinas virtuales en servidores vCenter, ESX o Microsoft Hyper-V, servidores réplica e informes de Arcserve Unified Data Protection.

Instale Arcserve Unified Data Protection en un servidor desde donde se puedan gestionar nodos protegidos y otros componentes de Arcserve Unified Data Protection.

Siga estos pasos:

1. Acceda al paquete de instalación de Arcserve UDP desde el sitio web de Arcserve o desde el CD del producto.

   Nota: Si se detecta uno de los sistemas operativos compatibles con un idioma distinto al inglés, tendrá que seleccionar el idioma de la instalación del producto.

2. Haga doble clic en el paquete de instalación.

   Se abre el cuadro de diálogo **Acuerdo de licencia**.

3. Lea y acepte los términos del acuerdo de licencia y haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Tipo de instalación**.

4. Seleccione uno de los tipos de instalación.

   Instalación estándar

   Permite instalar el Agente o todos los componentes de Arcserve Unified Data Protection.

   Arcserve Unified Data Protection - Agente

   Solo instala el Agente de Arcserve UDP.

   Para obtener más información, consulte *Instalación del Agente de Arcserve Unified Data Protection para Windows mediante el Asistente para la instalación* en la *Guía del usuario del Agente de UDP para Windows*.

   Arcserve Unified Data Protection- Completa

   Instala la Consola, el Servidor de puntos de recuperación y el Agente de Arcserve Unified Data Protection.

   Instalación avanzada

   Permite instalar uno o más de los siguientes componentes de Arcserve Unified Data Protection:

- Agente de Arcserve UDP
- Servidor de puntos de recuperación de Arcserve UDP
- Consola de Arcserve UDP

5. Especifique si desea instalar el controlador de seguimiento de cambios de Agente de Arcserve Unified Data Protection para Windows.

   De forma predeterminada, esta opción está activada.

   - Sin este controlador instalado, el Agente de Arcserve Unified Data Protection para Windows siempre realiza la copia de seguridad completa.
   - Con el controlador instalado, todavía es necesario disponer de una licencia válida del Agente de Arcserve Unified Data Protection para Windows para realizar una copia de seguridad local.
   - No se requiere este controlador si este Agente se utiliza como el controlador de Virtual Standby o el servidor proxy de copia de seguridad de la máquina virtual basada en host.

     Nota: Se puede instalar este controlador en cualquier momento después de que la instalación finalice mediante la ejecución de la utilidad InstallDriver.bat desde la ubicación siguiente:

     <carpeta de instalación de Arcserve UDP>\Engine\BIN\DRIVER

6. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Carpeta del destino**.

7. Especifique la carpeta donde desea instalar Arcserve Unified Data Protection y haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Configuración**.

8. En el cuadro de diálogo **Configuración**, especifique la información siguiente:

   a. Seleccione el protocolo.

      Nota: Para una comunicación más segura, seleccione el protocolo HTTPS.

   b. Si es aplicable, introduzca el número de puerto para el agente. Normalmente, el número de puerto es 8014.

   c. Si es aplicable, introduzca el número de puerto para la consola. Normalmente, el número de puerto es 8015.

   d. Introduzca el nombre y la contraseña del administrador de Windows.

   e. Especifique si desea mostrar el Controlador del Agente de Arcserve UDP a todos los usuarios o solamente al usuario actual.

9. Haga clic en **Siguiente**.

Aparecerá el cuadro de diálogo **Configuración de la base de datos**.

10. En el cuadro de diálogo **Configuración de la base de datos**, haga clic en la lista desplegable **Bases de datos** para elegir un tipo de base de datos. Puede especificar uno de los siguientes valores:

    - Microsoft SQL Server 2014 Express (incluido)
    - Microsoft SQL Server

      Importante: Cuando se tienen más de 500 nodos que se deben gestionar desde la consola, asegúrese de que se selecciona Microsoft SQL Server y no SQL Express.

    Tras especificar un tipo de base de datos, las opciones necesarias para la base de datos seleccionada aparecerán en el cuadro de diálogo **Configuración de la base de datos.** Proporcione detalles sobre la configuración de la base de datos para una de las bases de datos que seleccione.

    Microsoft SQL Server 2014 Express (incluido):

    En el cuadro de diálogo **Configuración de la base de datos,** complete lo siguiente:

    a. Especifique la ubicación donde se desee instalar Microsoft SQL Server 2014 Express. Se puede aceptar la ruta predeterminada o bien especificar una ruta alternativa.

    b. Especifique la ubicación en la que desea instalar el archivo de datos para la base de datos predeterminada de Arcserve Unified Data Protection. Se puede aceptar la ruta predeterminada o bien especificar una ruta alternativa.

       Nota: Microsoft SQL Server 2014 Express no es compatible con la comunicación remota. Por lo tanto, se debe instalar la base de datos predeterminada y el archivo de datos en el equipo donde se está instalando la aplicación.

    Bases de datos de Microsoft SQL Server

    En el cuadro de diálogo **Configuración de la base de datos,** complete lo siguiente:

    a. **Tipo de SQL Server**: especifique el tipo de comunicación que la aplicación utilizará para comunicarse con la base de datos de SQL Server.

       Local: especifique esta opción si la aplicación y SQL Server están instalados en el mismo equipo.

       Remoto: especifique esta opción si la aplicación y SQL Server están instalados en equipos distintos.

    b. **Nombre de SQL Server**: si el tipo de SQL Server especificado es Remoto, deberá especificar el nombre del servidor remoto de SQL Server. Si se utiliza

SQL Server de forma local, se deberá seleccionar el servidor en la lista desplegable.

c. **Seguridad**: especifique el tipo de credenciales que se desea utilizar para autenticar SQL Server.

Utilizar seguridad de Windows: se autentica mediante las credenciales de Windows. Se puede iniciar sesión utilizando las credenciales de la Consola de Arcserve UDP.

Utilizar seguridad de SQL Server: se autentica mediante las credenciales de SQL Server. Especifique el ID de inicio de sesión y la contraseña para acceder a la cuenta de SQL Server.

11. Haga clic en **Siguiente**. Se abrirá el cuadro de diálogo **Excepciones de Firewall.**

El cuadro de diálogo **Excepciones de Firewall** enumera los servicios y programas que se deben registrar en el Firewall de Windows como excepciones para Arcserve UDP.

Nota: Se deben especificar excepciones de Firewall obligatoriamente si se desea configurar y gestionar Arcserve UDP desde equipos remotos.

12. Haga clic en **Siguiente**. Se abrirá el cuadro de diálogo **Mensaje**.
13. Haga clic en **Siguiente**. Se abrirá el cuadro de diálogo **Resumen**.
14. Haga clic en **Instalar** para iniciar el proceso de instalación.

Aparecerá el cuadro de diálogo **Progreso de la instalación** que indica el estado de la instalación. Cuando se finaliza la instalación, se muestra el cuadro de diálogo **Informe de instalación**.

(Opcional) Si se desea buscar cualquier última actualización del producto, siga estos pasos:

a. Seleccione **Buscar una actualización inmediatamente** y haga clic en **Finalizar**.

Se abre el cuadro de diálogo **Buscar actualizaciones**.

b. Seleccione el servidor desde donde se desea descargar las actualizaciones y haga clic en **Descargar e instalar actualizaciones**.

El cuadro de diálogo **Proceso de la actualización** se muestra indicando el estado de la descarga.

Cuando la actualización se haya completado, se mostrará un mensaje de alerta.

(Opcional) Para instalar el Agente de Arcserve UDP para Linux, siga las instrucciones que se describen en la sección **Instalación del Agente de Arcserve Unified Data Protection para Linux**.

15. Haga clic en **Finalizar**.

    Arcserve UDP se instala en el equipo.

Instalación de Arcserve Unified Data Protection mediante la línea de comandos

Arcserve Unified Data Protection se puede instalar de manera silenciosa. Una instalación silenciosa elimina la necesidad de interacción por parte del usuario. En los siguientes pasos se describe cómo instalar la aplicación silenciosamente a través de la línea de comandos de Windows:

Siga estos pasos:

1. Abra la línea de comandos de Windows en el equipo en el que desea iniciar el proceso de instalación silenciosa.
2. Descargue el paquete de instalación autoextraíble en el equipo.

   Inicie el proceso de instalación silenciosa mediante la siguiente sintaxis de línea de comandos:

   Arcserve_Unified_Data_Protection.exe -s -a -q -Products:<ListaProductos> -Path:<DIRINSTLACIÓN> -User:<NombreUsuario> -Password:<Contraseña> -Https:<HTTPS> -ConsolePort:<Número de puerto> -AgentPort:<Número de puerto> -Driver:<CONTROLADOR> -MonitorFlag:<ETIQUETACONTROLADOR> -StopUA:<DETENER UA> -SummaryPath:<RUTARESUMEN> -AutoReboot:<REINICIOAUTOMÁTICO>

   Ejemplo:

   Arcserve_Unified_Data_Protection.exe -s -a -q -Products:Agent -User:administrator -Password:test
3. Configure la instalación silenciosa mediante la sintaxis y los argumentos siguientes:

   Importante: Si los parámetros incluyen cualquiera de los caracteres especiales siguientes, ponga los parámetros entre comillas:

   - <espacio>
   - &()[]{}^=;!'+,`~

   Por ejemplo: si la contraseña es abc^*123, la entrada debe ser -Password:"abc^*123".

   -s

   Ejecuta el paquete de archivos ejecutable en el modo silencioso.

   -a

   Especifica las opciones de línea de comandos adicionales.

   -q

   Instala la aplicación en el modo silencioso.

-Products:<ProductList>

(Opcional) Especifica los componentes que se deben instalar silenciosamente. Si no se especifica un valor para este argumento, el proceso de instalación silenciosa instalará todos los componentes. Se pueden especificar los siguientes componentes:

Agent (Agente): instala el componente del agente de protección de datos.

Servidor de puntos de recuperación: instala el componente del servidor de puntos de recuperación.

Console (Consola): instala el componente de la consola.

All (Todo): Instala todos los componentes de Arcserve Unified Data Protection.

Ejemplo:

Para instalar el Agente de protección de datos:

-Products:Agent

Para instalar el servidor de punto de recuperación:

-Products:Agent,RPS

Para instalar el Agente de protección de datos, el servidor de punto de recuperación y la consola de protección de datos:

-Products:Agent,RPS,Console

Para instalar todos los componentes de la generación:

-Products:All

-User:<NombreUsuario>

Especifica el nombre de usuario que se desea utilizar para instalar y ejecutar la aplicación.

Nota: El nombre de usuario debe ser un administrador o una cuenta con privilegios administrativos.

-Password:<Contraseña>

Especifica la contraseña del nombre de usuario.

-Https:<HTTPS>

(Opcional) Especifica el protocolo de comunicación. Las opciones son 0 y 1. Utilice 0 para http y 1 para https.
Predeterminado: 0
Ejemplo:

-https:1

-Path:<INSTALLDIR>

(Opcional) Especifica la ruta de instalación de destino del agente de protección de datos.

Ejemplo:

-Path:C:\Archivos de programa\Arcserve\Unified Data Protection

Nota: Si el valor de INSTALLDIR contiene un espacio, encierre la ruta con comillas. De forma adicional, la ruta no puede terminar con un carácter de barra diagonal inversa.

-ConsolePort:<Número de puerto>

(Opcional) Especifica el número de puerto de comunicación para la consola.

Predeterminado: 8015

Ejemplo:

-ConsolePort:8015

Nota: Utilice esta opción cuando desee instalar la consola.

-AgentPort:<Número de puerto>

(Opcional) Especifica el número de puerto de comunicación para acceder al Agente de Arcserve Unified Data Protection.

Predeterminado: 8014

Ejemplo:

-AgentPort:8014

Nota: Utilice esta opción cuando desee instalar el Agente de Arcserve Unified Data Protection.

-Driver:<CONTROLADOR>

(Opcional) Especifica si se debe instalar el controlador de seguimiento de cambios del Agente de Arcserve Unified Data Protection. Las opciones son 0 y 1.

0: No instala el controlador
1: Instala el controlador.

Valor predeterminado: 1

Ejemplo:

-driver:1

-MonitorFlag:<ETIQUETACONTROLADOR>

(Opcional) Especifica la visualización del controlador del Agente de Arcserve Unified Data Protection a los usuarios. Las opciones son 0 y 1.

0: Se muestra el controlador del agente a todos los usuarios.
1: Se muestra el controlador del agente solamente al usuario actual.

Predeterminado: 0.

Ejemplo:

-MonitorFlag:0

-StopUA:<DETENERUA>

(Opcional) Especifica detener el servicio del agente universal de Arcserve.

0: No se detiene el servicio del agente universal de Arcserve si se está ejecutando durante el proceso de instalación.
1: Se detiene el servicio del agente universal de Arcserve si se está ejecutando durante el proceso de instalación.
Predeterminado: 0

Ejemplo:

-StopUA:1

Nota: Utilice esta opción mientras se actualiza a una versión nueva. Verifique que se establece el valor en 1 o detenga el servicio antes de iniciar el proceso de actualización. Esto ayuda a garantizar que la instalación no produce un error.

-SummaryPath:<RUTARESUMEN>

(Opcional) Especifica la ruta de destino para generar el archivo de resumen de la instalación.

Ejemplo:

-SummaryPath:C:\Result

Nota: Si el valor de SUMMARYPATH contiene un espacio, encierre la ruta con comillas. De forma adicional, la ruta no puede terminar con un carácter de barra diagonal inversa.

-AutoReboot:<REINICIOAUTOMÁTICO>

(Opcional) Permite configurar el reinicio del equipo después de la instalación si la instalación requiere un reinicio. Las opciones son 0 y 1.

0: No se reinicia el equipo.

1: Se reinicia el equipo si la instalación requiere un reinicio.

Predeterminado: 0

Ejemplo:

-AutoReboot:1

Nota: Si la instalación no requiere un reinicio, la configuración no reiniciará el equipo incluso si este parámetro se establece en 1.

Se ha completado correctamente la instalación silenciosa.

Instalación de Arcserve UDP mediante el instalador unificado

Arcserve UDP permite instalar todos sus componentes mediante un instalador unificado. En función de los requisitos, el instalador sugiere la licencia que se adapta mejor a sus necesidades y, a continuación, descarga e instala los componentes.

Siga estos pasos:

1. Descargue el archivo ASDownloader desde el sitio web de Arcserve.

   Nota: Si se detecta uno de los sistemas operativos compatibles con un idioma distinto al inglés, tendrá que seleccionar el idioma de la instalación del producto.

2. Haga doble clic en el paquete de instalación.

   Se abre el cuadro de diálogo **Acuerdo de licencia**.

3. Lea y acepte los términos del acuerdo de licencia y haga clic en **Siguiente**.

   Se abre el cuadro de diálogo **Primeros pasos**.

4. Haga clic en **Siguiente**.

   Se abre el cuadro de diálogo **Seleccionar componentes para su descarga**.

5. Seleccione una o más de las opciones siguientes en función de los requisitos y haga clic en **Siguiente**.

   Arcserve Unified Data Protection

   Instala Arcserve UDP. Arcserve UDP permite proteger nodos físicos y virtuales de Windows y Linux. Se pueden gestionar todas las necesidades de protección de datos desde una única consola. Se pueden utilizar las funciones de deduplicación, replicación, replicación remota y otras funciones a nivel del origen para gestionar los datos.

   Arcserve Backup

   Instala Arcserve Backup. Cuando se combina con Arcserve UDP, se puede gestionar la copia de seguridad en cinta desde la Consola de Arcserve UDP y aprovechar todas las ventajas de Arcserve UDP.

   Se abrirá el cuadro de diálogo **Descarga del producto**.

6. Haga clic en **Descargar**.

   El producto empieza a descargarse en formato zip. Se puede comprobar el estado de la descarga en la barra de progreso. También se puede pausar y reanudar la descarga. En función del ancho de banda y el número de componentes para la des-

carga, esto puede tardar un rato.

Hasta que finalice la descarga, el siguiente botón estará inactivo.

7. Cuando se haya completado la verificación, haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Método de instalación**.

8. Seleccione uno de los tipos de instalación.

   Instalación rápida

   Instala los componentes mediante la configuración predeterminada. Haga clic en **Ver configuración predeterminada y componentes** para ver los componentes que se instalarán.

   Instalación avanzada

   Permite instalar cada componente por separado.

9. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Configuración de cuenta**.

10. Especifique el nombre de usuario y la contraseña. A continuación, haga clic en **Instalar**.

    Comenzará la instalación. Se puede ver el progreso en el cuadro de diálogo. Al finalizar la instalación, cierre el asistente.

    Arcserve UDP se instala en el equipo.

Verificación de la instalación

Siga estos pasos:

1. Verifique que el icono de Arcserve UDP aparece en la bandeja del sistema.
2. Verifique que los servicios del agente y del servidor se están ejecutando en el Gestor de servicios de Windows.

   Arcserve Unified Data Protection se ha instalado correctamente y está listo para realizar la copia de seguridad del equipo Windows.

Puertos de comunicación usados por Arcserve UDP

Esta sección proporciona información sobre los puertos utilizados para los siguientes componentes:

- Componentes instalados en Microsoft Windows
- Componentes instalados en Linux
- Componentes instalados en Hypervisor

Se requieren los puertos enumerados para las copias de seguridad y otras tareas cuando se tiene un entorno LAN.

*Se es compatible con el uso compartido de puertos para las tareas de replicación. Todos los datos de los diferentes puertos se pueden enviar al puerto 8014 (puerto predeterminado para el servidor de UDP, se puede modificar durante la instalación). Cuando una tarea de replicación se ejecuta entre dos servidores de punto de recuperación a través de WAN, solo se requiere que el puerto 8014 esté abierto.

De forma similar, para las replicaciones remotas, el administrador remoto debe abrir o enviar el puerto 8014 (para la replicación de datos) y el puerto 8015 (puerto predeterminado para la Consola de UDP; se puede modificar durante la instalación) con el objetivo de que los servidores de puntos de recuperación locales obtengan el plan de replicación asignado.

Componentes instalados en Microsoft Windows

Esta sección proporciona información sobre los puertos utilizados en la Consola de UDP y en el Servidor de puntos de recuperación (RPS) de UDP:

- Consola de UDP
- Servidor de puntos de recuperación de UDP
- Agente de UDP de Windows

Consola de UDP

La tabla siguiente incluye los puertos utilizados por la Consola de Arcserve UDP:

Número de puerto	Tipo de puerto	Iniciado por	Proceso de escucha	Puerto interno/externo	Descripción
1433	TCP	Java remoto	sqlsvr.exe	Externo	Puerto de comunicación predeterminado entre la consola de UDP y las bases de datos de Microsoft SQL Server cuando residen en equipos diferentes. **Nota:** Se puede modificar el puerto de comunicación predeterminado al instalar SQL Server.
6052	TCP	Cuadro de mandos global de Arcserve Backup	Arcserve.CommunicationFoundation.WindowsService.exe	Externo	Comunicación que permite a la Consola UDP y al servidor principal del cuadro de mandos global de

					Arcserve Backup. **Nota**: Este puerto solo es necesario cuando se desea sincronizar los datos del cuadro de mandos global de Arcserve Backup con la Consola de UDP.
6054	TCP	Servidor principal de Arcserve Backup	Arcserve.CommunicationFoundation.WindowsService.exe	Externo	Comunicación que permite a la consola y al servidor principal de Arcserve Backup sincronizar datos. **Nota**: Este puerto solo es necesario cuando se desea sincronizar los datos del cuadro de mandos global de Arcserve Backup con la Consola de UDP.
8012	TCP	Consola de UDP	java.exe	Interno	Puerto predeterminado utilizado

					internamente por el servicio de identidad de la Consola de UDP. **Nota:** No se puede personalizar el puerto y se puede ignorar para la configuración del cortafuegos. Si el puerto 8012 está ocupado por otros programas, el programa de instalación de UDP asignará dinámicamente otro puerto disponible.
8015	TCP	Consola de UDP Puerta de enlace de UDP	httpd.exe	Externo	Puerto de comunicación de HTTP/HTTPS predeterminado para visitar la Consola de UDP y la Puerta de enlace de UDP.

					Nota: Se puede modificar el puerto de comunicación predeterminado cuando se instalan los componentes de UDP.
8029	TCP	Consola de UDP	tomcat9.exe	Interno	Puerto predeterminado utilizado internamente por el servicio de gestión de la Consola de UDP. **Nota:** No se puede personalizar el puerto y se puede ignorar para la configuración del cortafuegos. Si el puerto 8029 está ocupado por otros programas, el programa de instalación de UDP asignará dinámicamente

					otro puerto disponible.
8030	TCP	Consola de UDP	tomcat9.exe	Interno	Puerto predeterminado utilizado internamente por el servicio de gestión de la Consola de UDP. **Nota:** No se puede personalizar el puerto y se puede ignorar para la configuración del cortafuegos. Si el puerto 8030 está ocupado por otros programas, el programa de instalación de UDP asignará dinámicamente otro puerto disponible.
18007	TCP	TOMCAT	tomcat9.exe	Interno	Utilizados internamente por el servicio de gestión de Tomcat. **Nota**: Este

					puerto solo puede cambiarse mediante la modificación de los archivos de configuración de TOMCAT. Este puerto se puede ignorar para la configuración del cortafuegos.

Servidor de puntos de recuperación de UDP

La tabla siguiente incluye los puertos utilizados por el Servidor de puntos de recuperación de Arcserve UDP:

Número de puerto	Tipo de puerto	Iniciado por	Proceso de escucha	Puerto interno/externo	Descripción
8014	TCP	UDP	httpd.exe	Externo	Puerto de comunicación de HTTP/HTTPS predeterminado para visitar el servidor de puntos de recuperación de UDP y el Agente de UDP. **Notas:** ■ Este puerto es el puerto compartido predeterminado y el único puerto que se debe abrir cuando se utiliza el servidor de puntos de recuperación de UDP como destino de la replicación. No abra el puerto 5000-5060 utilizado por los almacenes de datos con la deduplicación global activada. ■ Se puede modificar el puerto de comunicación predeterminado cuando se instalan los componentes de UDP.
8016	TCP	UDP	tomcat9.exe	Interno	Utilizados internamente por los servicios web del servidor de puntos de recuperación de UDP para comunicarse con el servicio del uso compartido de puertos del servidor de puntos de recuperación de UDP en el mismo servidor. **Nota:** No se puede personalizar el puerto y se puede ignorar para la configuración del cortafuegos.
5000-5060	TCP	UDP	GDDServer.exe	Interno	Este intervalo de puertos está reservado para el servicio de almacén de datos del servidor de puntos de recuperación de UDP. Un almacén de datos de deduplicación del servidor de puntos de recuperación de

					UDP utilizará 4 puertos libres y un almacén de datos sin deduplicación utilizará 1 puerto libre, y ambos comienzan a partir del 5000. Se necesita cuando se utiliza el almacén de datos activada para la copia de seguridad o restauración. Si se utiliza el servidor de puntos de recuperación solo como el destino de replicación, no será necesario abrirlo en la configuración del cortafuegos. **Nota:** Cambie lo siguiente para personalizar el intervalo de puertos en el Registro: ■ HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore ■ Nombre de clave: PortRangeForGDD ■ Tipo: REG_SZ ■ Valor predeterminado: 5000-5060 Solo el almacén de datos creado después de los cambios en el registro utilizará el intervalo de puertos recién modificado.
18005	TCP	TOMCAT	tomcat9.exe	Interno	Para cerrar Tomcat utilizado por el agente o servidor de puntos de recuperación de UDP. **Nota**: Este puerto solo puede cambiarse mediante la modificación de los archivos de configuración de TOMCAT. Este puerto se puede ignorar para la configuración del cortafuegos.
7788	TCP	UDP	Sync_util_d.exe	Interno	Puerto de comunicación de HTTP/HTTPS predeterminado para aceptar la replicación de las solicitudes.
445	TCP			Externo	Utilizado por el servicio SMB del sistema operativo Windows. El puerto se utiliza cuando el ser-

					vidor de puntos de recuperación hospeda el almacén de datos en un disco local. El almacén de datos expone la carpeta compartida como el destino de la copia de seguridad de los datos que realiza el Agente de UDP.

Agente de UDP de Windows

La tabla siguiente incluye los puertos utilizados por el Agente de Arcserve UDP para Windows:

Número de puerto	Tipo de puerto	Iniciado por	Proceso de escucha	Puerto interno/externo	Descripción
8014	TCP	Agente de UDP de Windows	tomcat9.exe	Externo	Puerto de comunicación HTTP/HTTPS para visitar el servidor de punto de recuperación y el Agente de UDP. **Nota:** Se puede modificar el puerto de comunicación predeterminado cuando se instalan los componentes de UDP.
18005	TCP	TOMCAT	tomcat9.exe	Interno	Para cerrar Tomcat utilizado por el agente o servidor de puntos de recuperación de UDP. **Nota**: Este puerto solo puede cambiarse mediante la modificación de los archivos de configuración de TOMCAT. Este puerto se puede ignorar para la configuración del cortafuegos.
4090	TCP	Agente de UDP de Windows	HATransServer.exe	Externo	Para transferir datos para la tarea de Virtual Standby en el modo de proxy. **Nota:** Este puerto solo es necesario cuando se especifica este Agente de UDP de Windows como controlador de Virtual Standby.

135	TCP			Externo	Puerto de comunicación para el servicio del servidor de puntos de recuperación en el SO Windows. **Nota:** Este puerto solo es necesario cuando la consola de UDP implemente de forma remota El Agente de UDP de Windows en este equipo de agente. Si el Agente de UDP de Windows está instalado de forma que se ejecuta el programa de instalación localmente, este puerto no es necesario.
445	TCP			Externo	Puerto de comunicación para que el servicio SMB active la carpeta compartida en el SO Windows. **Nota:** Este puerto solo es necesario cuando la consola de UDP implemente de forma remota El Agente de UDP de Windows en este equipo de agente. Si el Agente de UDP de Windows está instalado de forma que se ejecuta el programa de instalación localmente, este puerto no es necesario.

Componentes instalados en Linux

Esta sección proporciona información sobre los puertos utilizados en el servidor de copias de seguridad de Linux y los nodos de Linux protegidos por el servidor de copia de seguridad de Linux de forma remota.

Servidor de copia de seguridad de Linux

La tabla siguiente enumera los puertos utilizados por el servidor de copia de seguridad de Linux:

Número de puerto	Tipo de puerto	Iniciado por	Proceso de escucha	Puerto interno/externo	Descripción
67	UDP	UDP Linux	bootpd	Externo	Entrante, utilizado para el servidor de arranque de PXE. Solo es necesario si el usuario desea utilizar la función de arranque de PXE. **Nota:** No se puede personalizar este número de puerto.
69	UDP	UDP Linux	tftpd	Externo	Entrante, utilizado para el servidor de arranque de PXE. Solo es necesario si el usuario desea utilizar la función de arranque de PXE. **Nota:** No se puede personalizar este número de puerto.
8014	TCP	UDP Linux	java	Externo	Tanto entrante como saliente. Puerto de comunicación de HTTP/HTTPS predeterminado para visitar el Agente de UDP para Linux. **Nota:** Se puede modificar el puerto de comunicación predeterminado cuando se instalan los componentes de UDP.
8021	TCP	UDP Linux	cresvc	Externo	Entrante, utilizado para el servicio de copia de seguridad.
18005	TCP	UDP Linux	java	Interno	Utilizado por Tomcat. Ignore este puerto para la configuración del cortafuegos. **Nota**: Este puerto solo puede cambiarse mediante

					la modificación de los archivos de configuración de TOMCAT.
50000 o más de 50000	TCP	UDP Linux	ssh	Externo	Dependencia de terceros de UDP para Linux. Solo es necesario cuando se ejecuta la reconstrucción completa de la migración de Linux desde la nube a un recurso local. Se selecciona y se utiliza un puerto disponible desde el puerto 50000. De forma predeterminada, UDP Linux abre el puerto seleccionado en el sistema.
22	TCP	Servicio SSH	sshd	Externo	Dependencia de terceros de UDP para Linux. Valor predeterminado para el servicio SSH, sin embargo, se puede cambiar este puerto. Este puerto se requiere para comunicaciones tanto entrantes como salientes.
8016	TCP	UDP Linux	d2ddss	Externo	Entrante, utilizado para el servicio de datos de reconstrucción completa instantánea o de máquina virtual instantánea. Solo es necesario si el usuario desea utilizar las funciones de reconstrucción completa instantánea o de máquina virtual instantánea.
111	TCP	Asignador de puertos	rpcbind	Externo	Dependencia de terceros de UDP para Linux. Valor predeterminado para el asignador de puertos. Solo es necesario cuando se ejecuta la máquina virtual instantánea de Linux desde el punto de recuperación de la copia de seguridad sin agente en el servidor ESX de vSphere.

2049	TCP	Servidor NFS	nfsd	Externo	Dependencia de terceros de UDP para Linux. Valor pre-determinado del servidor NFS. Solo es necesario cuando se ejecuta la máquina virtual instantánea de Linux desde el punto de recuperación de la copia de seguridad sin agente en el servidor ESX de vSphere.
Puerto dinámico	TCP	Servicio de montaje de NFS	rpc.mountd	Externo	Dependencia de terceros de UDP para Linux. Consulte la página man de rpc.mountd para obtener cómo se debe hacer que escuche al puerto fijo. Solo es necesario cuando se ejecuta la máquina virtual instantánea de Linux desde el punto de recuperación de la copia de seguridad sin agente en el servidor ESX de vSphere.

Nodos de Linux protegidos por el servidor de copia de seguridad de Linux de forma remota

La tabla siguiente enumera los puertos utilizados por los nodos de Linux protegidos por el servidor de copia de seguridad de Linux de forma remota:

Número de puerto	Tipo de puerto	Iniciado por	Proceso de escucha	Puerto interno/externo	Descripción
22	TCP	Servicio SSH		Externo	Dependencia de terceros de UDP para Linux. Valor predeterminado para el servicio SSH, sin embargo, se puede cambiar este puerto. Este puerto se requiere para comunicaciones tanto entrantes como salientes.

Componentes instalados en Hypervisor

Esta sección proporciona información sobre los puertos utilizados para el host de Hyper-V.

Host de Hyper-V

La tabla siguiente muestra los puertos utilizados por el host de Hyper-V:

Número de puerto	Tipo de puerto	Iniciado por	Proceso de escucha	Interno o externo	Descripción
135	TCP			Externo	Utilizado por el servicio WMI del sistema operativo Windows. UDP utiliza WMI para interactuar con el host de Hyper-V en algunas situaciones.
445	TCP			Externo	Utilizado por el servicio SMB del sistema operativo Windows. UDP utiliza SMB para interactuar con el host de Hyper-V en algunas situaciones.
27000	TCP	Servicio de seguimiento de bloques modificados de UDP	cbt_rep.exe	Externo	Utilizado por el servicio de seguimiento de bloques modificados de copia de seguridad basada en el host de UDP. No es necesario registrar este puerto para la excepción del cortafuegos porque UDP registra automáticamente este puerto durante la copia de seguridad. Se debe comprobar que no se ha configurado ninguna otra aplicación con el mismo puerto.
5895 o 5986	TCP	Servicio WinRM		Externo	5895 para WinRM en protocolo HTTP, 5896 para WinRM en protocolo HTTPS. Solo es necesario uno de ellos. Solo es necesario cuando se ejecuta la máquina virtual instantánea de Linux en Hyper-V.
1024 ~ 65535	TCP			Externo	▪ Se utiliza durante la importación de máquinas virtuales desde el host de Hyper-V o el clúster para el plan de copia de seguridad. ▪ De forma predeterminada, la tarea de restauración de la máquina virtual elige aleatoriamente un puerto disponible en el intervalo de

					1024 y 65535. Se puede especificar manualmente el intervalo de los valores del registro establecido en el host de Hyper-V. Para obtener más información, consulte este vínculo.

Cómo afecta el proceso de instalación a los sistemas operativos

Los procesos de instalación siguientes actualizan diversos sistemas operativos de Windows:

- Instalación de archivos binarios sin firmar
- Instalación de archivos binarios que contienen una versión incorrecta del archivo
- Instalación de archivos binarios sin SO en el manifiesto

Instalación de archivos binarios sin firmar

Nombre binario	Origen	Nombre binario	Origen
AxShockwaveFlashObjects.dll	Adobe	freetype.dll	Oracle
ShockwaveFlashObjects.dll	Adobe	hprof.dll	Oracle
httpd.exe	Apache	instrument.dll	Oracle
libapr-1.dll	Apache	j2pcsc.dll	Oracle
libapriconv-1.dll	Apache	j2pkcs11.dll	Oracle
libaprutil-1.dll	Apache	jaas_nt.dll	Oracle
libeay32.dll	Apache	jabswitch.exe	Oracle
libexpat.dll	Apache	java-rmi.exe	Oracle
libhttpd.dll	Apache	java.dll	Oracle
openssl.exe	Apache	java.exe	Oracle
pcre.dll	Apache	JavaAccessBridge-64.dll	Oracle
rotatelogs.exe	Apache	javaw.exe	Oracle
ssleay32.dll	Apache	java_crw_demo.dll	Oracle
tcnative-1.dll	Apache	jawt.dll	Oracle
CAPatch.dll	APM	JAWTAccessBridge-64.dll	Oracle
AsyncClient.net.dll	Axcient	jdwp.dll	Oracle
doclib.dll	Axcient	jjs.exe	Oracle
docxlib.dll	Axcient	jli.dll	Oracle
DspchConnector.dll	Axcient	jpeg.dll	Oracle
esr.exe	Axcient	jsdt.dll	Oracle
esrdf.dll	Axcient	jsound.dll	Oracle
esrsdll.dll	Axcient	jsoundds.dll	Oracle
eswrapper.dll	Axcient	keytool.exe	Oracle
html2text.dll	Axcient	kinit.exe	Oracle
licensemanager.dll	Axcient	klist.exe	Oracle
mhdll.dll	Axcient	ktab.exe	Oracle
pdflib.dll	Axcient	lcms.dll	Oracle
pptlib.dll	Axcient	management.dll	Oracle
pptxlib.dll	Axcient	mlib_image.dll	Oracle
protection.dll	Axcient	net.dll	Oracle
pstgen.dll	Axcient	nio.dll	Oracle
resources.dll	Axcient	npt.dll	Oracle
rtf2html.dll	Axcient	ojdkbuild_giflib.dll	Oracle
rtflib.dll	Axcient	ojdkbuild_libjpeg-tur-bo.dll	Oracle

SourceLibrary.dll	Axcient	ojdkbuild_libpng.dll	Oracle
uicommon.dll	Axcient	ojdkbuild_nss.dll	Oracle
xlslib.dll	Axcient	orbd.exe	Oracle
xlsxlib.dll	Axcient	pack200.exe	Oracle
libbind9.dll	Bind	policytool.exe	Oracle
libdns.dll	Bind	rmid.exe	Oracle
libisc.dll	Bind	rmiregistry.exe	Oracle
libisccfg.dll	Bind	sawindbg.dll	Oracle
liblwres.dll	Bind	servertool.exe	Oracle
libxml2.dll	Bind	splashscreen.dll	Oracle
msvcm80.dll	Bind	sunec.dll	Oracle
win_nsupdate.exe	Bind	sunmscapi.dll	Oracle
msvcm90.dll	Microsoft	tnameserv.exe	Oracle
RDXCleanerX64.EXE	Microsoft	unpack.dll	Oracle
RDXForceCleanX64.EXE	Microsoft	unpack200.exe	Oracle
MSCHRT20.OCX	Microsoft	verify.dll	Oracle
Microsoft.Exchange.WebServices.dll	Office365	w2k_lsa_auth.dll	Oracle
SQLite.CodeFirst.dll	Office365	WindowsAccessBridge-64.dll	Oracle
System.Data.SQLite.dll	Office365	zip.dll	Oracle
System.Data.SQLite.EF6.dll	Office365	jvm.dll	Oracle
System.Data.SQLite.Linq.dll	Office365	JavaAccessBridge-32.dll	Oracle
System.Management.Automation.dll	Office365	JavaAccessBridge.dll	Oracle
SQLite.Interop.dll	Office365	JAWTAccessBridge-32.dll	Oracle
libxml.dll	OpenSSL	JAWTAccessBridge.dll	Oracle
attach.dll	Oracle	WindowsAccessBridge-32.dll	Oracle
awt.dll	Oracle	WindowsAccessBridge.dll	Oracle
dt_shmem.dll	Oracle	plink.exe	Putty
dt_socket.dll	Oracle	sqlite3.exe	SQLite
fontmanager.dll	Oracle	MinHook.x64.dll	Tsuda Kageyu
javacpl.cpl	Oracle	zlib10.dll	Zlib

Instalación de archivos binarios que contienen una versión incorrecta del archivo

Nombre binario	Origen	Nombre binario	Origen
AxShockwaveFlashObjects.dll	Adobe	libisccfg.dll	bind
ShockwaveFlashObjects.dll	Adobe	liblwres.dll	bind
openssl.exe	Apache	libxml2.dll	bind
UpdateData.exe	Licencias de Arcserve	win_nsupdate.exe	bind
AsyncClient.net.dll	Axcient	libxml.dll	NetApp
doclib.dll	Axcient	decora-sse.dll	Oracle
docxlib.dll	Axcient	fxplugins.dll	Oracle
DspchConnector.dll	Axcient	glass.dll	Oracle
esr.exe	Axcient	glib-lite.dll	Oracle
esrdf.dll	Axcient	gstreamer-lite.dll	Oracle
esrsdll.dll	Axcient	javafx-font.dll	Oracle
eswrapper.dll	Axcient	javafx-iio.dll	Oracle
html2text.dll	Axcient	jfxmedia.dll	Oracle
licensemanager.dll	Axcient	jfxwebkit.dll	Oracle
mhdll.dll	Axcient	libxml2.dll	Oracle
pdflib.dll	Axcient	libxslt.dll	Oracle
pptlib.dll	Axcient	prism-d3d.dll	Oracle
pptxlib.dll	Axcient	sqlite3.exe	sqlite
protection.dll	Axcient	libcurl.dll	VMware
pstgen.dll	Axcient	libexpat.dll	VMware
resources.dll	Axcient	liblber.dll	VMware
rtf2html.dll	Axcient	libldap.dll	VMware
rtflib.dll	Axcient	libldap_r.dll	VMware
uicommon.dll	Axcient	libxml2.dll	VMware
xlslib.dll	Axcient	ssoclient.dll	VMware
xlsxlib.dll	Axcient	vddkReporter.exe	VMware
libbind9.dll	bind	zlib1.dll	zlib
libdns.dll	bind	zlib10.dll	zlib
libisc.dll	bind		

Instalación de archivos binarios sin SO en el manifiesto

Nombre binario	Origen
openssl.exe	Apache
win_nsupdate.exe	bind
plink.exe	putty
sqlite3.exe	sqlite
vddkReporter.exe	VMware

Configuración de antivirus

El software de antivirus puede interferir en la correcta ejecución del Agente de Arcserve UDP (Windows) mediante un bloqueo del acceso a los archivos de manera temporal, o bien poniendo en cuarentena o suprimiendo archivos que se han clasificado incorrectamente como sospechosos o peligrosos. Se puede configurar un software antivirus para excluir archivos o carpetas y así evitar dedicar tiempo a explorar datos que no se deben proteger.

Se debe configurar correctamente el software antivirus para excluir el destino de la copia de seguridad. La configuración adecuada permite evitar interferencias con las operaciones de copia de seguridad y restauración o con cualquier otro proceso como la generación y combinación de catálogos.

Rutas que se deben excluir de la exploración del software antivirus:

Exploración realizada por el antivirus	Rutas que se deben excluir
Servidor de puntos de recuperación	Carpeta del almacén de datos Ruta de destino de los datos Ruta de destino del índice Ruta de destino del hash
Agente de Windows no gestionado por la Consola	Destino de copia de seguridad

Cómo instalar actualizaciones de Arcserve UDP

Para obtener e instalar actualizaciones de Arcserve UDP se debe realizar un proceso que consta de dos pasos que implican, en primer lugar, la comprobación y descarga de la actualización y, a continuación, la instalación de la misma.

Nota: Todas las actualizaciones publicadas para Arcserve UDP son acumulativas. Por lo tanto, cada una de las actualizaciones también incluye todas las actualizaciones publicadas anteriormente para asegurar que el equipo esté siempre actualizado. El cuadro de diálogo de ayuda **Acerca de** muestra el nivel de actualización instalado en un equipo. Si resulta necesario, se puede utilizar esta información para construir otro servidor con el mismo nivel de configuración/parches.

Realice las tareas siguientes para instalar las actualizaciones de Arcserve UDP:

1. Revisión de las consideraciones para instalar las actualizaciones
2. Especifique las preferencias de actualización
3. Compruebe e instale las actualizaciones
4. (Opcional) Instalación de las actualizaciones de Arcserve UDP en modo silencioso
5. Comprobación de que las actualizaciones se han instalado correctamente

Revisión de las consideraciones para instalar las actualizaciones

Revise las consideraciones siguientes antes de instalar las actualizaciones de Arcserve UDP:

- Cuando se instala una actualización de Arcserve UDP o una del Agente de Arcserve Unified Data Protection para Windows, es importante mantener un rendimiento óptimo entre la Consola, el servidor de puntos de recuperación (RPS) y los Agentes. Por ello, cuando instale la actualización en un entorno que contenga tanto una consola como un agente, debe instalarse siempre la actualización en la consola primero, luego en el servidor de puntos de recuperación y, finalmente, en el Agente (en el caso del agente instalado en la consola o el RPS, la actualización se instalará automáticamente en dicho agente al mismo tiempo).
- Si es necesario, descargue las actualizaciones disponibles desde Arcserve, bien directamente a un equipo cliente, bien a un servidor de almacenamiento intermedio primero, y luego a un equipo cliente.
- Si es necesario, utilice su nodo de estación de trabajo como servidor de almacenamiento intermedio para descargar las actualizaciones de Arcserve UPD.
- Verifique que los valores de configuración preferentes de la actualización se han configurado correctamente.
  - Se pueden instalar las actualizaciones a través de la interfaz de usuario o utilizando la línea de comandos en modo silencioso.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

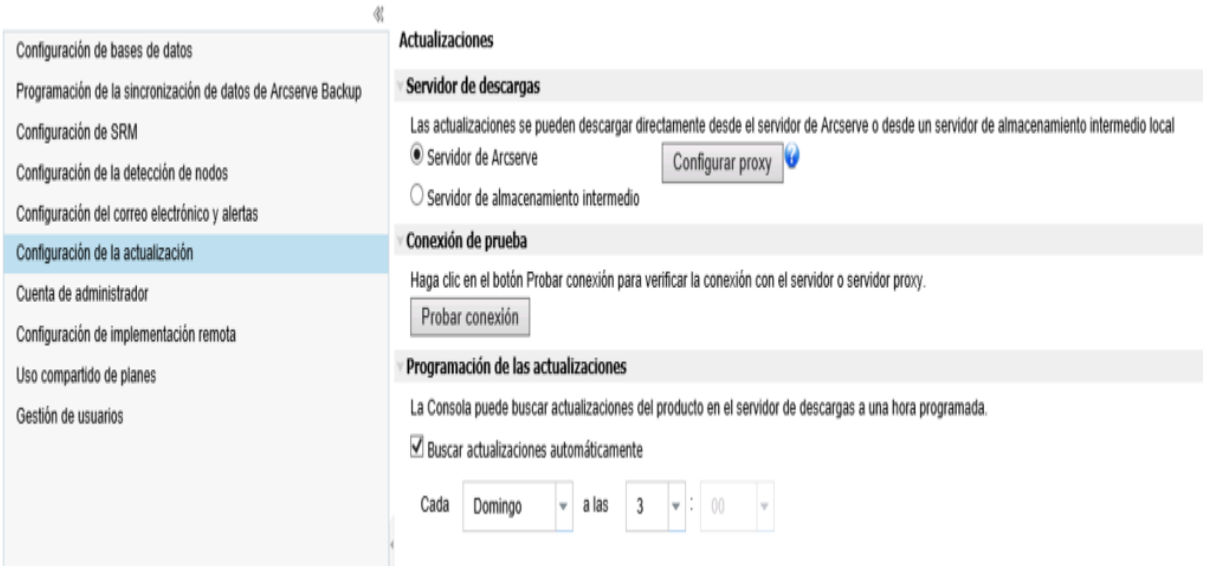
Especificación de las preferencias de actualización

Arcserve UDP permite especificar las preferencias de actualización.

Siga estos pasos:

1. En la Consola de Arcserve UDP, haga clic en la ficha **configuración**.
2. En el panel de la izquierda, haga clic en **Actualizar configuración**.

   En el panel derecho, se muestra la página **Actualizaciones**.



3. Especifique los valores de configuración de **Preferencias de actualizaciones**.

   Servidor de descargas

   Especifique el servidor de origen desde el cual se conectará el servidor de Arcserve UDP y se descargarán las actualizaciones disponibles.

   - **Servidor de Arcserve**

     Especifique si desea que las actualizaciones se descarguen directamente del servidor de Arcserve al servidor local.

     Se trata de la configuración predeterminada.

   - **Servidor de almacenamiento intermedio**

     Especifique si desea que las actualizaciones se descarguen desde el servidor de almacenamiento intermedio.

     Nota: Si es necesario, se puede crear un servidor de almacenamiento intermedio. Para obtener más información, consulte Cómo crear un servidor de almacenamiento intermedio.

Si se especifica más de un servidor de almacenamiento intermedio, el primer servidor enumerado se designará como el servidor de almacenamiento intermedio primario. Arcserve UDP intenta inicialmente conectarse al servidor de almacenamiento intermedio principal. Si el primer servidor enumerado no está disponible, el siguiente servidor enumerado se convertirá en el servidor de almacenamiento intermedio primario. La misma secuencia continuará hasta que el último servidor enumerado se convierta en el servidor de almacenamiento intermedio primario. (La lista de servidores de almacenamiento intermedio está limitada a un máximo de 5 servidores).

- Se pueden utilizar los botones **Mover hacia arriba** y **Mover hacia abajo** para cambiar la secuencia del servidor de almacenamiento intermedio.
- Se puede utilizar el botón **Suprimir** para eliminar un servidor de esta lista.
- Se puede utilizar el botón **Agregar servidor** para agregar un servidor nuevo a este listado. Al hacer clic en el botón **Agregar servidor**, se abre el cuadro de diálogo **Servidor de almacenamiento intermedio** para especificar el nombre del servidor de almacenamiento intermedio agregado.

Cuando se selecciona el servidor de almacenamiento intermedio como servidor de descarga, se pueden dar los escenarios siguientes:

- Si el servidor de almacenamiento intermedio especificado tiene cualquier actualización, la Consola de Arcserve UDP puede obtener la actualización del servidor de almacenamiento intermedio.
- Si el servidor de almacenamiento intermedio especificado no tiene ninguna actualización, la Consola de Arcserve UDP no puede descargar la actualización de este servidor de almacenamiento intermedio. El registro muestra el mensaje siguiente:

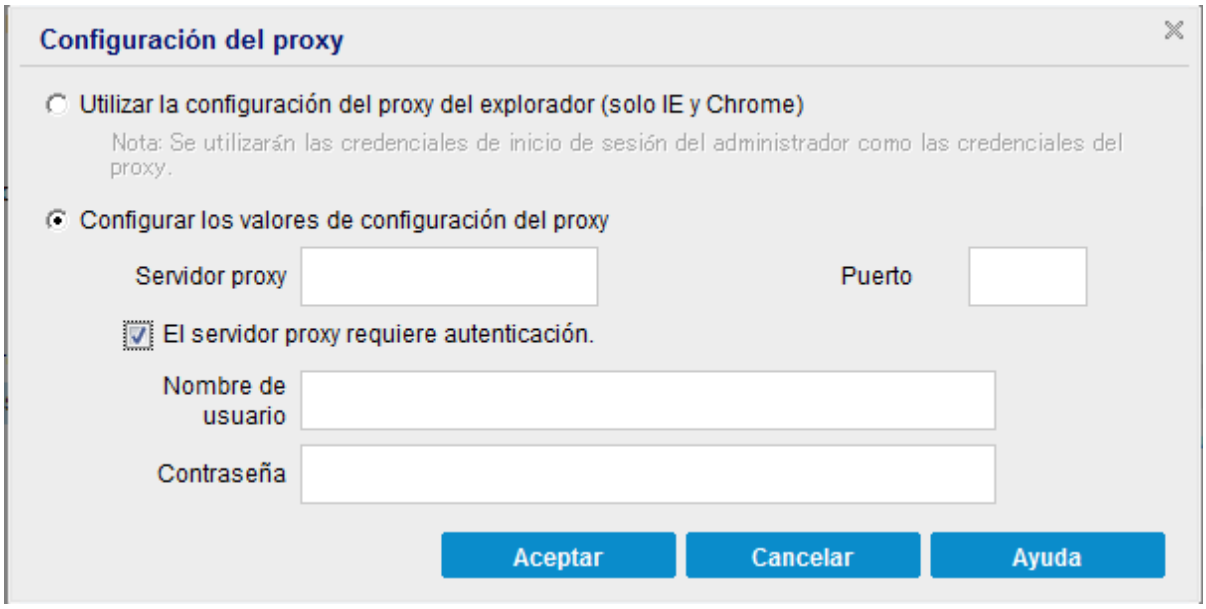
  No hay nuevas actualizaciones disponibles.

- **Configuración proxy**

  Nota: La opción **Servidor proxy** solo está disponible cuando se selecciona el servidor de Arcserve como servidor de descargas.

  Seleccione Configuración del proxy.

  Cuando se selecciona esta opción, se abre el cuadro de diálogo **Configuración del proxy**.



Utilizar la configuración de proxy del explorador

Esta selección es solamente aplicable a Windows Internet Explorer (IE) y Google Chrome.

Cuando se selecciona, se indica a Arcserve UDP que detecte y utilice automáticamente los mismos valores de configuración del proxy que se aplican al explorador para conectarse al servidor de Arcserve para obtener la información de actualización de Arcserve UDP.

Configuración del proxy

Cuando se selecciona, permite al servidor proxy especificado conectarse al servidor de Arcserve para obtener la información de actualización de Arcserve UDP. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet.

Además, se puede especificar también si su servidor proxy requiere autenticación. Si se selecciona, especifica que la información de autenticación es necesaria (ID de usuario y contraseña) para utilizar el servidor proxy.

Nota: El formato para el nombre de usuario debe ser un nombre de usuario del dominio completamente calificado con la forma <nombre del dominio>\<nombre de usuario>.

Conexión de prueba

Permite probar las conexiones siguientes y mostrar un mensaje de estado al finalizar:

- Si se selecciona el servidor de Arcserve como servidor de descargas, se realiza una prueba de la conexión entre el equipo y el servidor de Arcserve a través del servidor proxy especificado.
- Si se selecciona Servidor de almacenamiento intermedio como el servidor de descarga, se realiza una prueba de la conexión entre el equipo y el servidor de almacenamiento intermedio especificado. El botón de conexión de prueba se utiliza para probar la disponibilidad de cada servidor de almacenamiento intermedio enumerado y aparece el estado correspondiente en el campo **Estado de la conexión.** Si ninguno de los servidores de almacenamiento intermedio configurados está disponible, se muestra el mensaje siguiente en la parte superior de la Consola de Arcserve UDP: El servidor actualizado no está disponible.

  Nota: La conexión de prueba se realiza automáticamente cuando se abre la página **Configuración de la actualización** en la ficha **configuración** de la Consola de Arcserve UDP. Cuando se realiza esta prueba automática, se comprueba el estado de la última conexión del servidor de descargas previamente configurado (ya sea el servidor de Arcserve o los servidores de almacenamiento intermedio). Si ha configurado previamente más de un servidor de almacenamiento intermedio, esta prueba automática se realiza en todos los servidores de almacenamiento intermedio para obtener el último estado de conexión.

Programación de actualización

Especifica la fecha y hora de comprobación (y descarga) de las nuevas actualizaciones de Arcserve UDP.

4. Haga clic en **Guardar**.

Se guardan los valores de configuración de preferencias de actualizaciones.

Cómo crear un servidor de almacenamiento intermedio

El servidor de almacenamiento intermedio es un nodo en el que está instalado el Agente o la Consola de Arcserve UDP. El nodo debe terminar de descargar las actualizaciones desde el servidor de descarga de Arcserve para que funcione como un servidor de almacenamiento intermedio para proporcionar actualizaciones a otros.

Adición de un servidor de almacenamiento intermedio:

Se puede agregar el servidor de almacenamiento intermedio en cualquier nodo que cumpla los dos requisitos siguientes:

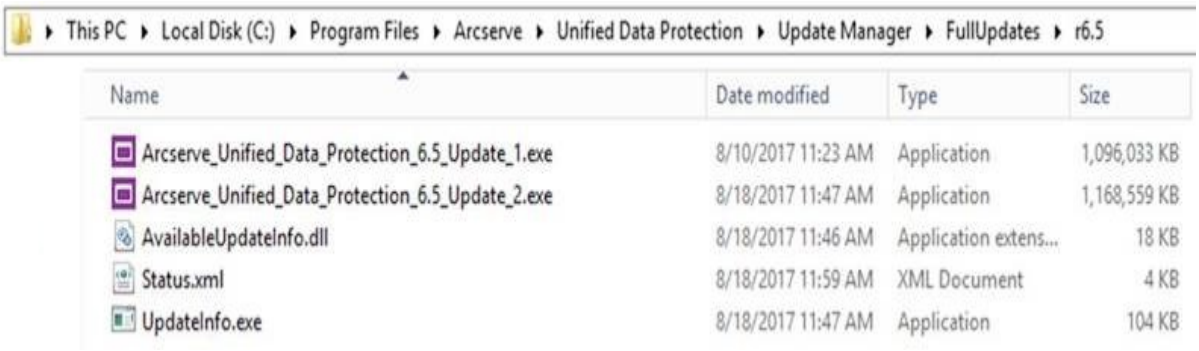
- El nodo tiene instalado el Agente de Arcserve UDP o la Consola de Arcserve UDP.
  - La Consola de Arcserve UDP solo puede descargar las actualizaciones desde el servidor de almacenamiento intermedio de la consola.
  - El Agente de Arcserve UDP puede descargar las actualizaciones desde el servidor de almacenamiento intermedio de la consola o del agente.
- El nodo ha descargado correctamente las actualizaciones desde el servidor de descarga de Arcserve al menos una vez.

Nota: No se necesita ninguna otra configuración si el servidor de almacenamiento intermedio de destino cumple los requisitos previos.

Configuración de la actualización desde el servidor de almacenamiento intermedio

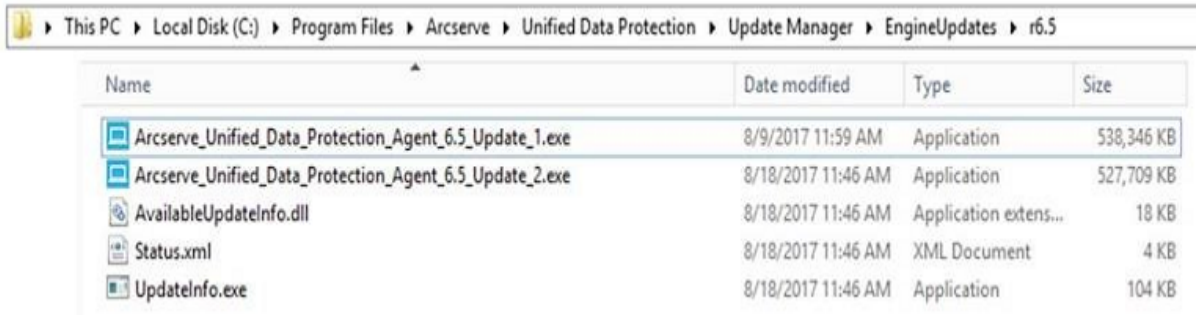
- Cuando se selecciona el servidor de almacenamiento intermedio por la Consola de Arcserve UDP instalada en ese nodo, considere las siguientes notas:
  - Puerto predeterminado: 8015
  - La Consola de Arcserve UDP puede obtener actualizaciones desde este servidor de almacenamiento intermedio
  - El Agente de Arcserve UDP puede obtener actualizaciones desde este servidor de almacenamiento intermedio

  Nota: En el directorio <Ruta instalación de UDP\Update Manager\FullUpdates> del servidor de almacenamiento intermedio de destino, compruebe la última versión de actualización disponible. Consulte el ejemplo que se muestra a continuación.



- Cuando se selecciona el servidor de almacenamiento intermedio por el Agente de Arcserve UDP instalado en ese nodo, considere las siguientes notas:
  - Puerto predeterminado: 8014
  - La Consola de Arcserve UDP no puede obtener actualizaciones desde este servidor de almacenamiento intermedio
  - El Agente de Arcserve UDP puede obtener actualizaciones desde este servidor de almacenamiento intermedio

  Nota: En el directorio <Ruta instalación de UDP\Update Manager\EngineUpdates> del servidor de almacenamiento intermedio de destino, compruebe la última versión de actualización disponible. Consulte el ejemplo que se muestra a continuación.



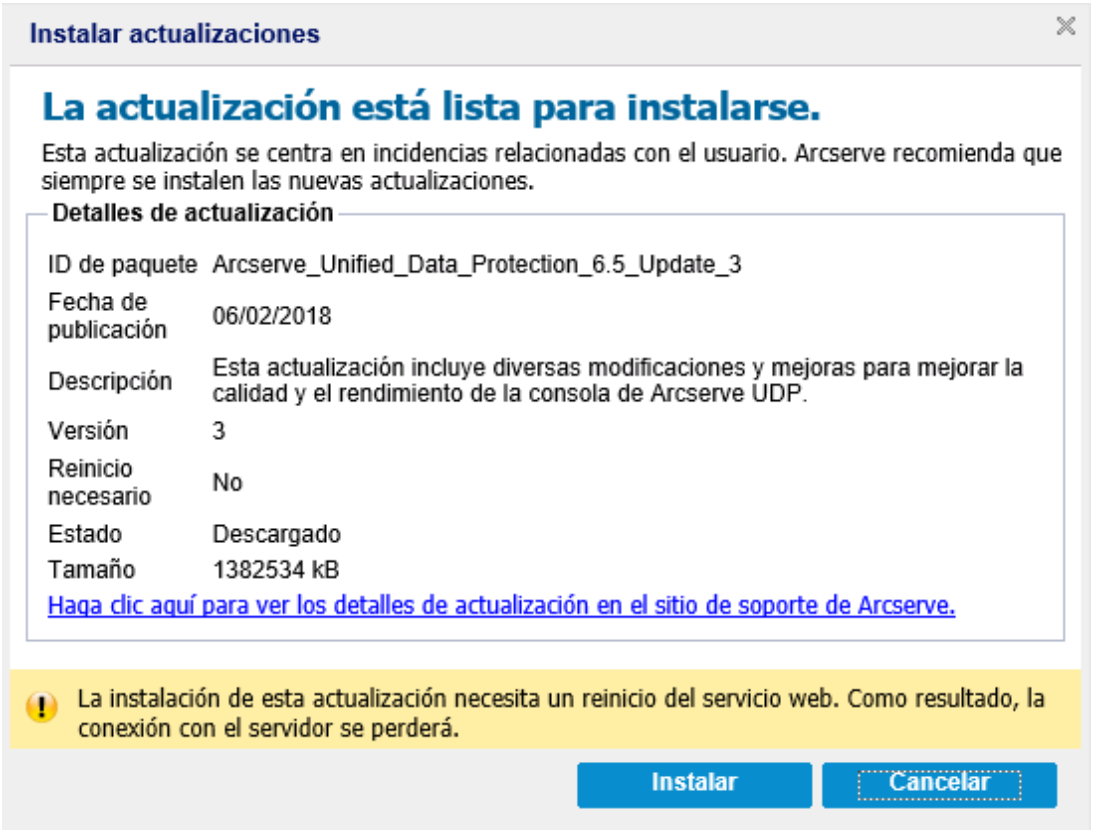
Compruebe e instale las actualizaciones

En la Consola de UDP se puede determinar si hay actualizaciones nuevas disponibles.

Siga estos pasos:

1. En el menú desplegable **Ayuda**, haga clic en **Buscar actualizaciones.** Cuando hay una nueva actualización disponible, aparece un mensaje en la barra superior de la pantalla. Además, se muestra el cuadro de diálogo **Update Installation (Instalación de la actualización)**.
2. Si se activa la programación de la actualización, cuando hay una nueva actualización disponible, se descarga automáticamente en el servidor de UDP. Se muestra el vínculo **Hay una nueva actualización disponible** en la barra superior con el fin de indicar de manera visual que hay una nueva actualización lista para su instalación.
3. Haga clic en el vínculo **Hay una nueva actualización disponible** ubicado en la barra superior.

   El cuadro de diálogo **Instalar actualizaciones** muestra información relacionada con la actualización disponible. El cuadro de diálogo incluye información como la descripción, el estado de descarga, el tamaño, el requisito de reinicio y un vínculo al servidor de Arcserve para obtener más detalles acerca de la actualización.



4. Haga clic en **Instalar.**

   Se inicia la instalación de las actualizaciones de Arcserve UDP.

Actualización de agentes en nodos remotos mediante la puerta de enlace

Los nodos remotos y el servidor de un sitio interactúan con la Consola mediante una puerta de enlace. Mediante Arcserve UDP, se puede detectar la última versión del agente e implementarla en los nodos. Para actualizar o instalar el Agente de Arcserve UDP en un nodo de un sitio, utilice Instalar/actualizar producto.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En panel **Exploración** de la izquierda, seleccione un sitio de la lista desplegable.
3. Se mostrará la página **Nodos: todos los nodos**.
4. Seleccione uno o más nodos.
5. En el panel central, haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Instalar/actualizar agente**.

   Los detalles de la instalación o actualización se muestran en el panel central.
6. Verifique los detalles y haga clic en **Aceptar**.

   El nodo se actualiza o instala con la última versión del Agente de Arcserve UDP.

Actualización del servidor de puntos de recuperación en el servidor remoto mediante la puerta de enlace

Los nodos remotos y el servidor de un sitio interactúan con la Consola mediante una puerta de enlace. Al utilizar Arcserve UDP se podrá detectar e implementar la última versión del componente del servidor de punto de recuperación (RPS) en servidores de punto de recuperación. Después de implementar el componente del servidor de puntos de recuperación, el servidor está preparado para almacenar sesiones de copia de seguridad y actúa como un servidor de puntos de recuperación. Para actualizar o instalar el componente del servidor de puntos de recuperación de Arcserve UDP en servidores de puntos de recuperación de un sitio, utilice Instalar o actualizar el servidor de punto de recuperación.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En panel **Exploración** de la izquierda, seleccione un sitio de la lista desplegable.
3. Haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destino: Servidor de puntos de recuperación**.
4. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en un servidor de punto de recuperación.
   - Seleccione un servidor de punto de recuperación y en el panel central haga clic en la lista desplegable **Acciones**.

   Aparecerá una lista de opciones.
5. Haga clic en **Instalar o actualizar el servidor de punto de recuperación**.

   Se muestra la página **Instalación y actualización**.
6. Modifique los valores de configuración de la implementación y haga clic en **Aceptar** para implementar el servidor de puntos de recuperación en el nodo seleccionado.

   La implementación del servidor de punto de recuperación se inicia. Se puede ver el progreso de la implementación en el panel derecho.

(Opcional) Instalación de las actualizaciones de Arcserve UDP en modo silencioso

La instalación silenciosa permite realizar una instalación de la actualización desatendida y no solicita ninguna introducción de datos.

Siga estos pasos:

1. Inicie la instalación silenciosa de la actualización de Arcserve UDP.

   "<UpdateExeFile>" /s /v"<Additional Arguments>"

2. Configure la instalación silenciosa mediante la sintaxis y los argumentos siguientes:

   UpdateExeFile

   Especifica la ejecución del archivo ejecutable autoextraíble.

   s

   Especifica la ejecución del archivo ejecutable autoextraíble mediante el modo silencioso.

   v

   Especifica los argumentos adicionales para la instalación de la actualización.

   Argumentos adicionales

   /s

   Especifica la ejecución de la instalación de la actualización mediante el modo silencioso.

   /AutoReboot

   Especifica la realización de un reinicio automático después de la instalación de la actualización. En el caso de que sea necesario realizar un reinicio para finalizar la actualización, el equipo volverá a reiniciarse automáticamente sin ninguna notificación.

   ### Ejemplos

   - Para instalar una actualización mediante el modo silencioso y reiniciar automáticamente después de la finalización, utilice el comando siguiente:

     "<UpdateExeFile>" /s /v"/s /AutoReboot"

   - Para instalar una actualización mediante el modo silencioso y no reiniciar automáticamente después de la finalización, utilice el comando siguiente:

     "<UpdateExeFile>" /s /v"/s"

Verificación de la instalación correcta de las actualizaciones

En la Consola de Arcserve UDP, seleccione **Ayuda**, haga clic en **Acerca de** y, a continuación, verifique que el cuadro de diálogo Acerca de Arcserve UDP muestra la última versión del producto actualizada.

Cómo desinstalar Arcserve UDP

Arcserve Unified Data Protection se puede desinstalar mediante los métodos siguientes:

- **Desinstalación estándar**: Utilice este método para desinstalar mediante el Panel de control de Windows.
- **Desinstalación silenciosa**: Utilice este método para realizar una desinstalación desatendida usando la línea de comandos de Windows.

Desinstalación estándar

Se pueden desinstalar los siguientes componentes:

- Consola de Arcserve Unified Data Protection
- Servidor de puntos de recuperación de Arcserve Unified Data Protection
- Agente de Arcserve Unified Data Protection

Siga estos pasos:

1. Abra el Panel de control de Windows.
2. Haga clic en Desinstalar un programa.

   Aparecerá el cuadro de diálogo Desinstalar o cambiar un programa.
3. Seleccione Arcserve Unified Data Protection y haga clic en Desinstalar.

   Se abre el cuadro de diálogo Arcserve Unified Data Protection.
4. Seleccione los componentes que se desean desinstalar y haga clic en Siguiente.

   Se abrirá el cuadro de diálogo **Mensajes**.
5. Haga clic en Siguiente.

   Se abrirá el cuadro de diálogo **Eliminar componentes**.
6. Haga clic en **Eliminar**.

   Los componentes seleccionados se desinstalan del equipo.

Desinstalación silenciosa

Una desinstalación silenciosa elimina la necesidad de interacción por parte del usuario mientras se lleva a cabo la desinstalación.

Siga estos pasos:

1. Inicie sesión en el equipo donde se desinstalarán los componentes de Arcserve UDP.

   Nota: Inicie sesión en el equipo con una cuenta administrativa.

2. Abra la línea de comandos de Windows y ejecute el comando siguiente que se corresponde al sistema operativo especificado:

   - **Sistema operativo X86:**

     Para desinstalar todos los componentes

     %ProgramFiles%\Arcserve\SharedComponents\Arcserve Unified Data Protection\Setup\uninstall /q /ALL

     Para desinstalar componentes seleccionados

     %ProgramFiles%\Arcserve\SharedComponents\Arcserve Unified Data Protection\Setup\uninstall /q /p <Product Code>

   - **Sistema operativo X64:**

     Para desinstalar todos los componentes

     %ProgramFiles(x86)%\Arcserve\SharedComponents\Arcserve Unified Data Protection\Setup\uninstall /q /ALL

     Para desinstalar componentes seleccionados

     %ProgramFiles(x86)%\Arcserve\SharedComponents\Arcserve Unified Data Protection\Setup\uninstall /q /p <Product Code>

   Los valores siguientes explican los códigos de retorno:

   0 = la desinstalación ha sido correcta.

   3010 = la desinstalación ha sido correcta, pero es necesario reiniciar.

   Otros = la desinstalación ha sido errónea.

   Uso:

   La tabla que se muestra a continuación define el código del producto que se debe especificar para el componente de Arcserve Unified Data Protection que desea desinstalar.

   Ejemplo:

La sintaxis siguiente permite desinstalar el Servidor de puntos de recuperación de Arcserve Unified Data Protection de forma silenciosa.

"%ProgramFiles(x86)%\Arcserve\SharedComponents\Arcserve Unified Data Protection\Setup\uninstall.exe" /q /p {CAAD8172-1858-4DC7-AE81-C887FA6AFB19}

Componente	<Código del producto>
Agente de Arcserve Unified Data Protection (plataformas de x86)	{CAAD8AEA-A455-4A9F-9B48-C3838976646A}
Agente de Arcserve Unified Data Protection (plataformas de x64)	{CAAD1E08-FC33-462F-B5F8-DE9B765F2C1E}
Arcserve Unified Data Protection Servidor de puntos de recuperación	{CAAD8172-1858-4DC7-AE81-C887FA6AFB19}
Arcserve Unified Data Protection Consola	{CAAD3E40-C804-4FF0-B1C0-26D534D438C0}
Arcserve Unified Data Protection Puerta de enlace	{FB95E75D-494F-4146-9B35-F867434B264A}

Después de ejecutar el comando, se desinstalan los componentes de Arcserve UDP.

Eliminación de los componentes que ha dejado el desinstalador

Importante:

1. La licencia de Arcserve se comparte con todos los productos de Arcserve. Verifique que no haya ningún otro producto de Arcserve instalado en el equipo, ya que de lo contrario podría perder la licencia de todos los productos de Arcserve instalados en el equipo.
2. Si se eliminan los componentes, es posible que cualquier programa que se haya instalado después del Agente de Arcserve Unified Data Protection para Windows y que dependa de estos componentes eliminados no funcione correctamente.

   Si desea eliminar manualmente estos componentes, realice lo siguiente:

   Elimine manualmente el componente de la licencia de Arcserve.

1. Vaya al directorio *C:\Archivos de programa (x86)\Arcserve\SharedComponents\CA_LIC*.
2. Busque el archivo zip llamado "*lic98_uninstaller.zip*" y descomprima ese archivo en alguna otra ubicación (por ejemplo: "C:\temp").
3. Vaya a la ubicación en la que se han extraído los archivos y busque dos archivos de script llamados "*rmlic.exe*" y "*rmlicense.bat*".
4. Haga clic en "*rmlicense.bat*" para ejecutar el script que desinstala los componentes.
5. Suprima manualmente las carpetas siguientes:
   - C:\Archivos de programa(x86)\Arcserve
   - C:\Archivos de programa\Arcserve
   - Carpeta en la que se ha extraído el archivo zip.
6. Elimine la clave de registro para el componente de la licencia de Arcserve.
   - Para la plataforma x64: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Arcserve\License
   - Para la plataforma x86: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\License

   Elimine Microsoft C++ Visual y Microsoft SQL Server Express manualmente.

1. Acceda a la aplicación estándar Agregar o quitar programas ubicada en el Panel de control de Windows (Panel de control, Programas y Funciones, Eliminar programas).

2. Seleccione *Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501* y, a continuación, haga clic en Desinstalar.
3. Seleccione *Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501* y, a continuación, haga clic en Desinstalar.
4. Seleccione Microsoft SQL Server 2014 (64 bits) y, a continuación, haga clic en Desinstalar.
5. Para eliminar solamente la base de datos de Arcserve UDP, seleccione "ARCSERVE_APP" y haga clic en Desinstalar.

Capítulo 4: Actualización a Arcserve UDP versión 8.0

Esta sección incluye los siguientes temas:

Nota: Para obtener las prácticas recomendadas sobre cómo proteger el servidor de Arcserve UDP, consulte Protección del servidor de Arcserve UDP.

Versiones compatibles con la actualización

Arcserve UDP 8.1 es compatible con la actualización y con las versiones anteriores de acuerdo con las reglas siguientes:

- Arcserve UDP 8.1 admite la actualización desde Arcserve UDP 8.0, 7.0 Actualización 2, 7.0 Actualización 1, 7.0 versión final y Arcserve UDP 6.5 Actualización 4.

  Notas: Antes de actualizar a Arcserve UDP 8.1 desde otras versiones anteriores, tenga en cuenta lo siguiente:

  - Para Arcserve UDP 6.5 con la Actualización 3, Actualización 2, Actualización 1 o la versión final, actualice primero a UDP 6.5 Actualización 4.
  - Para Arcserve UDP versión 6.0 Actualización 3 para Windows, primero actualice a Arcserve UDP versión 7.0.
  - Para Arcserve UDP versión 6.0 Actualización 2, Actualización 1 o la versión final para Windows, actualice primero a Arcserve UDP versión 6.5 Actualización 4.
  - Para Arcserve UDP versión 6.0 Actualización 1 o la versión final para Linux, primero actualice a Arcserve UDP versión 6.5 Actualización 4.
  - Para Arcserve UDP 5.0 Actualización 4, primero se debe actualizar a UDP 6.5 Actualización 4.
  - Para Arcserve UDP 5.0 con la Actualización 3, Actualización 2, Actualización 1 o la versión final, primero se debe actualizar a UDP 6.0 Actualización 3 y, a continuación, a UDP 7.0.

- Arcserve UDP 8.1 no admite la actualización desde Arcserve D2D r16.5, Arcserve Central Protection Management r16.5, Arcserve Data Protection Console r16.5, Arcserve Central Reporting r16.5 ni Arcserve Central Virtual Standby r16.5.

  Para obtener más información, consulte Cómo actualizar la licencia de Arcserve UDP.

Secuencia de actualización en el dispositivo de Arcserve

Arcserve versión 8.0 admite la actualización en el dispositivo de UDP. La actualización podría implicar una de las secuencias siguientes:

- Actualización de Arcserve UDP
  - Actualización del dispositivo de Arcserve que funciona como Consola de Arcserve UDP y como servidor de puntos de recuperación
  - Actualización del dispositivo de Arcserve que solo funciona como servidor de puntos de recuperación de Arcserve UDP
  - Pasos de actualización cuando se utilizan dos o más dispositivos de Arcserve en el entorno
- Actualización del Agente de Linux de Arcserve Backup en el Dispositivo de Arcserve
- Actualización de Arcserve Backup en el dispositivo de Arcserve

Actualización del dispositivo de Arcserve que funciona como Consola de Arcserve UDP y como servidor de puntos de recuperación

Actualice este dispositivo de Arcserve y, a continuación, siga la secuencia de actualización descrita para actualizar el entorno.

Actualización del Dispositivo de Arcserve que solo funciona como servidor de puntos de recuperación de Arcserve UDP

Actualice el entorno de producción completo. Para obtener más información, consulte Secuencia de actualización.

Pasos de actualización cuando se utilizan dos o más Dispositivos de Arcserve en el entorno

Actualice todo el entorno de producción. Para obtener más información, consulte Secuencia de actualización.

Actualización del Agente de Linux de Arcserve Backup en el dispositivo de Arcserve

1. Actualice la Consola de Arcserve UDP que gestiona el entorno del servidor de copia de seguridad de Linux.
2. Actualice el servidor de copia de seguridad de Linux que se encuentra en el dispositivo de Arcserve Para obtener más información, consulte la *Ayuda en línea del Agente de Arcserve Unified Data Protection para Linux*.

Actualización de Arcserve Backup en el dispositivo de Arcserve

Consulte la *Guía de implementación de Arcserve Backup* para completar la actualización en el dispositivo de Arcserve

Política de compatibilidad con versiones anteriores

Se recomienda actualizar todos los componentes a Arcserve UDP 8.1 en todo el entorno para que se puedan explorar las nuevas funciones de Arcserve UDP 8.1. Los planes de copia de seguridad existentes no se ven afectados si la actualización no se completa para todos los componentes en el mismo momento.

La compatibilidad con versiones anteriores es compatible con Arcserve UDP versión 8.0, 7.0, 7.0 Actualización 1, 7.0 Actualización 2 y Arcserve UDP 6.5 Actualización 4.

Esta sección incluye los siguientes temas:

Política de compatibilidad con versiones anteriores para Arcserve UDP versión 8.0

Compatibilidad con versiones anteriores entre la diferentes Consolas de UDP a través de la tarea de replicación en un servidor de puntos de recuperación gestionado de forma remota

Si se tienen planes para realizar la tarea de *replicación en un servidor de puntos de recuperación gestionado de forma remota*, se recomienda actualizar la Consola y el servidor de puntos de recuperación en el destino antes de actualizar la Consola, el servidor de puntos de recuperación o el Agente en el origen.

- Se admite la replicación si el servidor de puntos de recuperación de origen tiene instalado UDP 8.1, mientras que el servidor de puntos de recuperación de destino todavía tiene UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2.
- Se admite la replicación si el servidor de puntos de recuperación de origen tiene UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2, y el servidor de puntos de recuperación de destino tiene UDP 8.1.
- Comportamientos de la replicación:
  - Si se actualiza a UDP 8.1 en ambos sitios, se puede replicar desde una instancia de Cloud Hybrid a una instancia local sin una dirección IP pública (comportamiento nuevo de UDP).
  - Si se actualiza a UDP 8.1 solo en uno de los sitios y el otro sitio utiliza una versión compatible de UDP, se puede replicar desde la instancia de Cloud Hybrid a la instancia local utilizando la dirección IP pública.

Compatibilidad con versiones anteriores para el Agente (o proxy de copia de seguridad sin agente) o servidor de puntos de recuperación de Windows

- La Consola de Arcserve UDP 8.1 admite los servidores de puntos de recuperación (RPS) y los agentes (o servidores proxy de copia de seguridad sin agente) de UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2 para la copia de seguridad si el plan no cambia tras una actualización.
- La Consola y el servidor de puntos de recuperación de Arcserve UDP 8.1 admiten los agentes (o servidores proxy de copia de seguridad sin agente) de UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2 para la copia de seguridad si el plan no cambia tras una actualización.
- La Consola de Arcserve UDP 8.1 admite la implementación de un plan existente sin cambios cuando el servidor de puntos de recuperación y los agentes (o servidores proxy de copia de seguridad sin agente) todavía se ejecutan en UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2. El Agente no se actualiza automáticamente.
- La Consola de Arcserve UDP 8.1 admite acciones como pausar o reanudar un plan existente sin ninguna modificación cuando los servidores de puntos de recuperación y los agentes (o servidores proxy de la copia de seguridad sin agente) todavía se están ejecutando en UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2. El Agente no se actualiza automáticamente.
- La Consola de Arcserve UDP 8.1 admite la creación de un nuevo plan o la modificación de un plan existente para configurar las funciones heredadas ya admitidas en la versión anterior cuando el servidor de puntos de recuperación y los agentes (o servidores proxy de copia de seguridad sin agente) todavía se ejecutan en UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2. El Agente no se actualiza automáticamente.
- La Consola de Arcserve UDP 8.1 admite la creación de un nuevo plan o la modificación de un plan existente para incluir las nuevas funciones de UDP 8.1 cuando los servidores de puntos de recuperación asociados, el proxy y el agente ya están actualizados a la versión esperada.

  Por ejemplo:

  - Se admite especificar la red para la copia de seguridad cuando la Consola, el servidor de puntos de recuperación, el servidor proxy y el agente se actualizan a UDP 7.0, 7.0 Actualización 1, 7.0 Actualización 2, 8.0 y 8.1.
- La Consola de Arcserve UDP 8.1 admite la actualización del nodo cuando el servidor de puntos de recuperación y los agentes (o servidores proxy de copia de seguridad sin agente) todavía se ejecutan en UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2. Se implementará el plan. El Agente no se actualiza automáticamente.

- La Consola de Arcserve UDP 8.1 admite la agregación de la versión 8.0 del servidor de puntos de recuperación. Sin embargo, el servidor de puntos de recuperación no se actualiza automáticamente a Arcserve UDP versión 8.1 cuando se agrega.
- La Consola de Arcserve UDP 8.1 admite la agregación de una versión anterior del Agente (o servidor proxy de copia de seguridad sin agente) sin necesidad de actualizar automáticamente el Agente.
- La Consola de Arcserve UDP 8.1 es compatible con la adición de nodos a un plan existente.
  - Se admite la adición de un nodo al plan existente cuando el servidor de puntos de recuperación asociado se actualiza a la versión 8.1. De lo contrario, se guarda el plan pero se produce un error en la implementación del plan.
  - Se admite la adicción del nodo de la versión anterior a un plan existente si la versión es similar a la versión del servidor de puntos de recuperación en ejecución. El Agente no se actualiza automáticamente.
  - Se admite la adición del nodo de Arcserve UDP 8.1 al plan existente cuando el servidor de puntos de recuperación asociado se actualiza a UDP 8.1.
- La puerta de enlace se actualiza automáticamente para que coincida con la versión de la Consola de Arcserve UDP.
- Política de compatibilidad con versiones anteriores de replicación:
  - Se admite la replicación cuando la Consola se actualiza a Arcserve UDP 8.1 pero todos los servidores de puntos de recuperación (RPS) asociados todavía se ejecutan en UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2.
    - Se admite la replicación desde el servidor de puntos de recuperación de origen de Arcserve UDP 8.1 al servidor de puntos de recuperación de destino de UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2.
    - Se admite la replicación desde el servidor de puntos de recuperación de origen de Arcserve UDP UDP 8.0, 7.0, 7.0 Actualización 1 y 7.0 Actualización 2 al servidor de puntos de recuperación de destino de UDP 8.1.
- Política de compatibilidad con versiones anteriores de Virtual Standby:
  - Si el destino de la copia de seguridad es una carpeta compartida, la versión del servidor proxy o del controlador de Virtual Standby debe ser

similar a la versión del Agente.

- Si el destino de la copia de seguridad es el servidor de puntos de recuperación, la versión del servidor proxy o del controlador de Virtual Standby debe ser similar a la versión del servidor de puntos de recuperación.

- Política de compatibilidad con versiones anteriores de la máquina virtual instantánea:

  La versión del servidor de recuperación de la máquina virtual instantánea debe ser similar a la versión de la Consola de Arcserve UDP.

Política de compatibilidad con versiones anteriores para Arcserve UDP versión 7.x

Compatibilidad con versiones anteriores entre la diferentes Consolas de UDP a través de la tarea de replicación en un servidor de puntos de recuperación gestionado de forma remota

Si se tienen planes para realizar la tarea de *replicación en un servidor de puntos de recuperación gestionado de forma remota*, se recomienda actualizar la Consola y el servidor de puntos de recuperación en el destino antes de actualizar la Consola, el servidor de puntos de recuperación o el Agente en el origen.

- Se admite la replicación si el servidor de puntos de recuperación de origen tiene instalado UDP 8.1, mientras que el servidor de puntos de recuperación de destino todavía tiene UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2.
- Se admite la replicación si el servidor de puntos de recuperación de origen tiene UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2, y el servidor de puntos de recuperación de destino tiene UDP 8.1.
- Comportamientos de la replicación:
  - Si se actualiza a UDP 8.1 en ambos sitios, se puede replicar desde una instancia de Cloud Hybrid a una instancia local sin una dirección IP pública (comportamiento nuevo de UDP).
  - Si se actualiza a UDP 8.1 solo en uno de los sitios y el otro sitio utiliza una versión compatible de UDP, se puede replicar desde la instancia de Cloud Hybrid a la instancia local utilizando la dirección IP pública.

Compatibilidad con versiones anteriores para el Agente (o proxy de copia de seguridad sin agente) o servidor de puntos de recuperación de Windows

- La Consola de Arcserve UDP 8.1 admite los servidores de puntos de recuperación (RPS) y los agentes (o servidores proxy de copia de seguridad sin agente) de UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2 para la copia de seguridad si el plan no cambia tras una actualización.
- La Consola y el servidor de puntos de recuperación de Arcserve UDP 8.1 admiten los agentes (o servidores proxy de copia de seguridad sin agente) de UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2 para la copia de seguridad si el plan no cambia tras una actualización.
- La Consola de Arcserve UDP 8.1 admite la implementación de un plan existente sin cambios cuando el servidor de puntos de recuperación y los agentes (o servidores proxy de copia de seguridad sin agente) todavía se ejecutan en UDP 7.0,

7.0 Actualización 1 y 7.0 Actualización 2. El Agente no se actualiza automáticamente.

- La Consola de Arcserve UDP 8.1 admite acciones como pausar o reanudar un plan existente sin ninguna modificación cuando los servidores de puntos de recuperación y los agentes (o servidores proxy de la copia de seguridad sin agente) todavía se están ejecutando en UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2. El Agente no se actualiza automáticamente.
- La Consola de Arcserve UDP 8.1 admite la creación de un nuevo plan o la modificación de un plan existente para configurar las funciones heredadas ya admitidas en la versión anterior cuando el servidor de puntos de recuperación y los agentes (o servidores proxy de copia de seguridad sin agente) todavía se ejecutan en UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2. El Agente no se actualiza automáticamente.
- La Consola de Arcserve UDP 8.1 admite la creación de un nuevo plan o la modificación de un plan existente para incluir las nuevas funciones de UDP 8.1 cuando los servidores de puntos de recuperación asociados, el proxy y el agente ya están actualizados a la versión esperada.

  Por ejemplo:

  - Se admite especificar la red para la copia de seguridad cuando la Consola, el servidor de puntos de recuperación, el servidor proxy y el agente se actualizan a UDP 7.0, 7.0 Actualización 1, 7.0 Actualización 2, 8.0 y 8.1.
- La Consola de Arcserve UDP 8.1 admite la actualización del nodo cuando el servidor de puntos de recuperación y los agentes (o servidores proxy de copia de seguridad sin agente) todavía se ejecutan en UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2. Se implementará el plan. El Agente no se actualiza automáticamente.
- La Consola de Arcserve UDP 8.1 admite la adición de una versión de UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2 del servidor de puntos de recuperación. Sin embargo, el servidor de puntos de recuperación no se actualiza automáticamente a Arcserve UDP 8.1 cuando se agrega.
- La Consola de Arcserve UDP 8.1 admite la agregación de una versión anterior del Agente (o servidor proxy de copia de seguridad sin agente) sin necesidad de actualizar automáticamente el Agente.
- La Consola de Arcserve UDP 8.1 es compatible con la adición de nodos a un plan existente.

  - Se admite la adición de un nodo al plan existente cuando el servidor de puntos de recuperación asociado se actualiza a UDP 8.1. De lo contrario,

se guarda el plan pero se produce un error en la implementación del plan.

- Se admite la adicción del nodo de la versión anterior a un plan existente si la versión es similar a la versión del servidor de puntos de recuperación en ejecución. El Agente no se actualiza automáticamente.
- Se admite la adición del nodo de Arcserve UDP 8.1 al plan existente cuando el servidor de puntos de recuperación asociado se actualiza a UDP 8.1.

- La puerta de enlace se actualiza automáticamente para que coincida con la versión de la Consola de Arcserve UDP.
- Política de compatibilidad con versiones anteriores de replicación:
  - Se admite la replicación cuando la Consola se actualiza a Arcserve UDP 8.1 pero todos los servidores de puntos de recuperación (RPS) asociados todavía se ejecutan en UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2.
    - Se admite la replicación desde el servidor de puntos de recuperación de origen de Arcserve UDP 8.1 al servidor de puntos de recuperación de destino de UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2.
    - Se admite la replicación desde el servidor de puntos de recuperación de origen de Arcserve UDP UDP 7.0, 7.0 Actualización 1 y 7.0 Actualización 2 al servidor de puntos de recuperación de destino de UDP 8.1.
- Política de compatibilidad con versiones anteriores de Virtual Standby:
  - Si el destino de la copia de seguridad es una carpeta compartida, la versión del servidor proxy o del controlador de Virtual Standby debe ser similar a la versión del Agente.
  - Si el destino de la copia de seguridad es el servidor de puntos de recuperación, la versión del servidor proxy o del controlador de Virtual Standby debe ser similar a la versión del servidor de puntos de recuperación.
- Política de compatibilidad con versiones anteriores de la máquina virtual instantánea:

  La versión del servidor de recuperación de la máquina virtual instantánea debe ser similar a la versión de la Consola de Arcserve UDP.

Política de compatibilidad con versiones anteriores para Arcserve UDP versión 6.5 Actualización 4

Compatibilidad con versiones anteriores entre la diferentes Consolas de UDP a través de la tarea de replicación en un servidor de puntos de recuperación gestionado de forma remota

Si se tienen planes para realizar la tarea de *replicación en un servidor de puntos de recuperación gestionado de forma remota*, se recomienda actualizar la Consola y el servidor de puntos de recuperación en el destino antes de actualizar la Consola, el servidor de puntos de recuperación o el Agente en el origen.

- Se admite la replicación si el servidor de puntos de recuperación de origen tiene UDP 8.1, mientras que el servidor de puntos de recuperación de destino todavía tiene la versión 6.5 Actualización 4.
- Se admite la replicación si el servidor de puntos de recuperación de origen tiene la versión 6.5 Actualización 4 y el servidor de puntos de recuperación de destino tiene UDP 8.1 y se ha aplicado el parche P00001738. Si el servidor de puntos de recuperación de origen tiene la versión 6.5 Actualización 1, 2 o 3, primero se deberá actualizar a la Actualización 4 y, a continuación, se deberá aplicar el parche P00001738.

Compatibilidad con versiones anteriores para el Agente (o proxy de copia de seguridad sin agente) o servidor de puntos de recuperación de Windows

- La Consola de Arcserve UDP 8.1 admite los servidores de puntos de recuperación (RPS) y los agentes (o servidores proxy de copia de seguridad sin agente) de la versión 6.5 Actualización 4 para la copia de seguridad si el plan no cambia tras una actualización.
- La Consola y el servidor de puntos de recuperación de Arcserve UDP 8.1 admiten los agentes (o servidores proxy de copia de seguridad sin agente) de la versión 6.5 Actualización 4 para la copia de seguridad si el plan no cambia tras una actualización.
- La Consola de Arcserve UDP 8.1 admite la implementación de un plan existente sin cambios cuando el servidor de puntos de recuperación y los agentes (o servidores proxy de copia de seguridad sin agente) todavía se ejecutan en la versión 6.5 Actualización 4. El Agente no se actualiza automáticamente.
- La Consola de Arcserve UDP 8.1 admite acciones como pausar o reanudar un plan existente sin ninguna modificación cuando los servidores de puntos de recuperación y los agentes (o servidores proxy de la copia de seguridad sin

agente) todavía se están ejecutando en la versión 6.5 Actualización 4. El Agente no se actualiza automáticamente.

- La Consola de Arcserve UDP 8.1 admite la creación de un nuevo plan o la modificación de un plan existente para configurar las funciones heredadas ya admitidas en la versión anterior cuando el servidor de puntos de recuperación y los agentes (o servidores proxy de copia de seguridad sin agente) todavía se ejecutan en la versión 6.5 Actualización 4. El Agente no se actualiza automáticamente.
- La Consola de Arcserve UDP 8.1 admite la creación de un nuevo plan o la modificación de un plan existente para incluir las nuevas funciones de UDP 8.1 cuando los servidores de puntos de recuperación asociados, el proxy y el agente ya están actualizados a la versión esperada.

  Por ejemplo:

  - Se admite especificar la red para la copia de seguridad cuando la Consola, el servidor de puntos de recuperación, el servidor proxy y el agente se actualizan a la versión 7.0 Actualización 1 o Actualización 2, o a UDP 8.1.
- La Consola de Arcserve UDP 8.1 es compatible con la actualización del nodo cuando el servidor de puntos de recuperación y los agentes (o servidores proxy de la copia de seguridad sin agente) todavía se están ejecutando en la versión 6.5 Actualización 4. Se implementará el plan. El Agente no se actualiza automáticamente.
- La Consola de Arcserve UDP 8.1 admite la agregación de la versión 6.5 Actualización 4 del servidor de puntos de recuperación. Sin embargo, el servidor de puntos de recuperación no se actualiza automáticamente a Arcserve UDP 8.1 cuando se agrega.
- La Consola de Arcserve UDP 8.1 admite la agregación de una versión anterior del Agente (o servidor proxy de copia de seguridad sin agente) sin necesidad de actualizar automáticamente el Agente.
- La Consola de Arcserve UDP 8.1 es compatible con la adición de nodos a un plan existente.
  - Se admite la adición de un nodo al plan existente cuando el servidor de puntos de recuperación asociado se actualiza a UDP 8.1. De lo contrario, se guarda el plan pero se produce un error en la implementación del plan.
  - Se admite la adicción del nodo de la versión anterior a un plan existente si la versión es similar a la versión del servidor de puntos de recuperación en ejecución. El Agente no se actualiza automáticamente.

- Se admite la adición del nodo de Arcserve UDP 8.1 al plan existente cuando el servidor de puntos de recuperación asociado se actualiza a UDP 8.1.

- La puerta de enlace se actualiza automáticamente para que coincida con la versión de la Consola de Arcserve UDP.
- Política de compatibilidad con versiones anteriores de replicación:
  - Se admite la replicación cuando la Consola se actualiza a Arcserve UDP 8.1 pero todos los servidores de puntos de recuperación asociados todavía se ejecutan en la versión 6.5 Actualización x.
    - Se admite la replicación del servidor de puntos de recuperación de origen de Arcserve UDP 6.5 Actualización x al servidor de puntos de recuperación de destino de la versión 6.5 Actualización 4.
    - Se admite la replicación del servidor de puntos de recuperación de origen de Arcserve UDP 6.5 Actualización 4 al servidor de puntos de recuperación de destino de la versión 6.5 Actualización x.
  - Se admite la replicación desde el servidor de puntos de recuperación de origen de Arcserve UDP 6.5 Actualización x al servidor de puntos de recuperación de destino de UDP 8.1.
  - Se admite la replicación del servidor de puntos de recuperación de origen de Arcserve UDP 8.1 al servidor de puntos de recuperación de destino de la versión 6.5 Actualización 4.
  - No se admite la replicación desde Arcserve UDP 8.1 del servidor de puntos de recuperación de origen a la versión 6.5 Actualización 3, Actualización 2, Actualización 1 o a la versión final del servidor de puntos de recuperación de destino.
- Política de compatibilidad con versiones anteriores de Virtual Standby:
  - Si el destino de la copia de seguridad es una carpeta compartida, la versión del servidor proxy o del controlador de Virtual Standby debe ser similar a la versión del Agente.
  - Si el destino de la copia de seguridad es el servidor de puntos de recuperación, la versión del servidor proxy o del controlador de Virtual Standby debe ser similar a la versión del servidor de puntos de recuperación.
- Política de compatibilidad con versiones anteriores de la máquina virtual instantánea:

  La versión del servidor de recuperación de la máquina virtual instantánea debe ser similar a la versión de la Consola de Arcserve UDP.

Compatibilidad con versiones anteriores para el servidor de copia de seguridad de Linux

Para el servidor de copia de seguridad de Linux 7.x y 6.5.x:

- La Consola de Arcserve UDP 8.1 es compatible con el servidor de copia de seguridad de Linux de las versiones 6.5.x y 7.x cuando los servidores de puntos de recuperación (RPS) tienen Arcserve UDP 8.1 instalado. Todas las tareas se ejecutan correctamente, excepto las nuevas funciones o mejoras de UDP 8.1.
- La Consola de Arcserve UDP 8.1 es compatible con los servidores de puntos de recuperación (RPS) y con el servidor de copia de seguridad de Linux de la versión 6.5.x y de la versión 7.x. Todas las tareas se deben ejecutar correctamente y sin problemas, excepto las nuevas características o mejoras de la versión 8.1.
- Después de actualizar el servidor de copia de seguridad de Linux a Arcserve UDP 8.1, se admiten todas las nuevas funciones de UDP 8.1.

Secuencia de actualización para la Consola de UDP, el Servidor de puntos de recuperación y el Agente

Según la política de compatibilidad con versiones anteriores, planifique la actualización con la siguiente secuencia para garantizar que se lleva a cabo una actualización sin problemas:

1. Actualice la Consola de Arcserve UDP.
2. Actualice el servidor de puntos de recuperación de Arcserve UDP (sitio de DR).
3. Actualice el servidor de puntos de recuperación de Arcserve UDP (Centro de datos).
4. Actualice el servidor proxy sin agente de Arcserve UDP y algunos o todos los agentes del Centro de datos.
5. Actualice el servidor de puntos de recuperación de Arcserve UDP (sitio remoto).
6. Actualice el servidor proxy sin agente de Arcserve UDP y algunos o todos los agentes en el sitio remoto.

   Nota: Repita los pasos 5 y 6 para cada ubicación remota.

   Notas:

   - En primer lugar, si se ha configurado la tarea de replicación del proveedor de servicios gestionados, actualice la Consola o el Servidor de puntos de recuperación del proveedor de servicios gestionados.
   - La Puerta de enlace se actualiza automáticamente para coincidir con la versión de la Consola.
   - Según la política de compatibilidad con la replicación de versiones anteriores, actualice siempre el servidor de puntos de recuperación de destino antes que el de origen.

Cómo actualizar a Arcserve UDP 8.0 desde una versión anterior

Actualizar una instalación significa reinstalar funciones o componentes de una versión superior. El proceso de actualización permite conservar la mayoría de los valores de configuración y migrar la información almacenada en la antigua base de datos de Arcserve UDP a la nueva base de datos de Arcserve UDP.

Consideraciones sobre la actualización

- Compruebe si se cumple el requisito de hardware de Arcserve UDP versión 8.0. Para obtener más información, consulte la sección *Información del sistema* en las *Notas de la versión v8.0*.
- Se requiere una versión de la aplicación, del sistema operativo, del hipervisor o de la plataforma compatible con Arcserve UDP versión 8.0. Para obtener información detallada, consulte la matriz de compatibilidad.
- Antes de actualizar desde la versión 6.5.3 u otra versión anterior compatible, evite pausar un plan existente. Si el plan se pausa antes de una actualización, no se puede reanudar el plan hasta que se actualicen todos los servidores de puntos de recuperación relacionados.
- Adquiera la clave de producto para Arcserve UDP versión 8.0 y téngala a mano.
- Se debe eliminar la versión anterior de la utilidad independiente Arcserve Exchange Granular Restore (AEGR) para Arcserve UDP versión 5.0. En caso de detectarse, el asistente de instalación solicita eliminarla.
- En condiciones ideales, los planes más antiguos deben funcionar correctamente en cada uno de los pasos de actualización que se describen a continuación.

Siga estos pasos para llevar a cabo la actualización:

1. Para MSP, actualice la Consola de Arcserve UDP Arcserve UDP 8.0.

   Este paso solo es necesario si **Tarea: Replicar desde un servidor de puntos de recuperación remoto** se ha configurado en la versión anterior.

   Notas:

   - Si el nodo tiene solo la Consola instalada, actualícela. No es necesario detener los trabajos en ejecución para actualizar la Consola.
   - Si el nodo tiene la Consola y el servidor de puntos de recuperación instalados, planifique la actualización de la Consola cuando no haya ninguna tarea en ejecución antes de la actualización. Si resulta necesario, detenga el

almacén de datos del servidor de puntos de recuperación para cancelar las tareas en ejecución antes de actualizar la Consola.

- Para obtener más información sobre cómo actualizar la Consola, consulte Instalación de Arcserve Unified Data Protection mediante el asistente para la instalación o Instalación de Arcserve UDP con el instalador unificado.

2. Para MSP, actualice el servidor de puntos de recuperación de Arcserve UDP a la versión 8.0 de Arcserve UDP.

   Este paso solo es necesario si **Tarea: Replicar desde un servidor de puntos de recuperación remoto** se ha configurado en la versión anterior.

   Notas:

   - Planifique la actualización del servidor de puntos de recuperación cuando no haya ninguna tarea en ejecución antes de la actualización. Si resulta necesario, detenga el almacén de datos del servidor de puntos de recuperación para cancelar las tareas en ejecución antes de actualizar el servidor de puntos de recuperación.
   - Para obtener más información sobre cómo actualizar el servidor de puntos de recuperación, consulte Instalar o actualizar el servidor de puntos de recuperación.

3. Para el cliente, actualice la Consola de Arcserve UDP a la versión 8.0 de Arcserve UDP.

   Notas:

   - Si el nodo tiene solo la Consola instalada, actualícela. No es necesario detener los trabajos en ejecución para actualizar la Consola.
   - Si el nodo tiene la Consola y el servidor de puntos de recuperación instalados y las tareas se están ejecutando en ese servidor, detenga el almacén de datos del servidor de puntos de recuperación para cancelar primero dichas tareas. A continuación, actualice la Consola.
   - Para obtener más información sobre cómo actualizar la Consola, consulte Instalación de Arcserve Unified Data Protection mediante el asistente para la instalación o Instalación de Arcserve UDP con el instalador unificado.

4. Para el cliente, actualice el servidor de puntos de recuperación de destino de la replicación de Arcserve UDP a Arcserve UDP 8.0.

   Notas:

   - Arcserve UDP 8.0 admite la replicación del servidor de puntos de recuperación de origen de Arcserve UDP 6.5.x al servidor de puntos de recuperación de destino de Arcserve UDP 8.0. Cuando el plan incluya varias tareas

de replicación, actualice primero el último servidor de puntos de recuperación de destino de la replicación.

- La replicación desde el servidor de puntos de recuperación de origen de Arcserve UDP 8.0 a una versión anterior del servidor de puntos de recuperación de destino solo se admite si el servidor de puntos de recuperación de destino es de Arcserve UDP 6.5 Actualización 4.
- Para obtener más información sobre cómo actualizar el servidor de puntos de recuperación, consulte Instalar o actualizar el servidor de puntos de recuperación.

5. Para el cliente, actualice el servidor de puntos de recuperación de origen de la replicación anterior a Arcserve UDP 8.0.

   Nota: Para obtener más información sobre cómo actualizar el servidor de puntos de recuperación, consulte Instalar o actualizar el servidor de puntos de recuperación.

6. Para el cliente, actualice el servidor proxy y los Agentes de versiones anteriores a Arcserve UDP 8.0.

   Notas:

   - Para obtener más información sobre cómo actualizar el agente y el proxy sin agente de Windows, consulte Implementación del Agente en los nodos.
   - Para obtener más información sobre cómo actualizar el servidor de copia de seguridad de Linux, consulte Cómo actualizar el Agente de Arcserve UDP (Linux).

7. Para el cliente, actualice el Controlador de Virtual Standby o el servidor de recuperación de la máquina virtual instantánea de una versión anterior a Arcserve UDP 8.0.

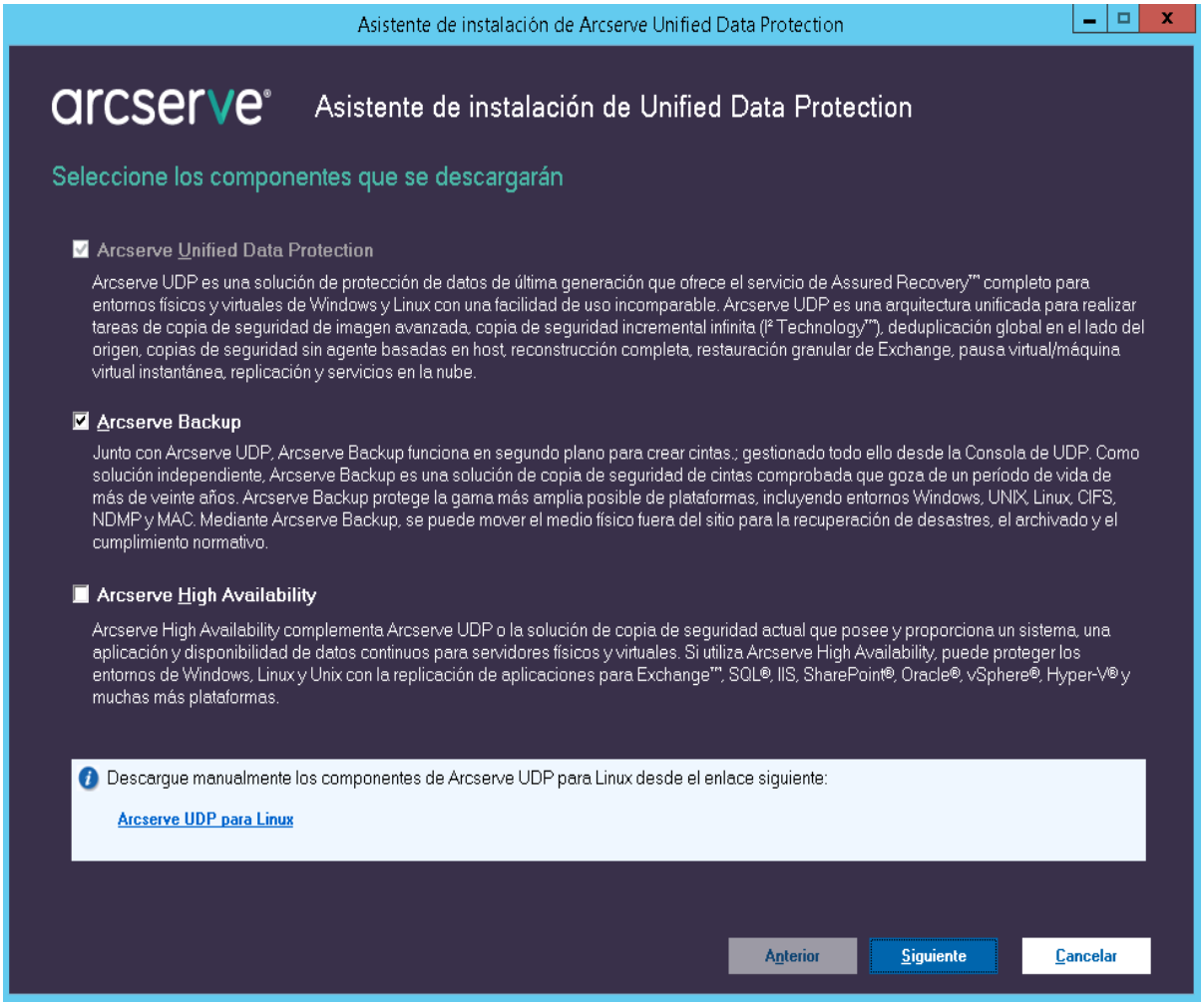
   Nota: Para obtener más información sobre cómo actualizar el controlador de Virtual Standby, consulte Instalación de Arcserve Unified Data Protection mediante el asistente para la instalación o Instalación de Arcserve UDP con el instalador unificado.

Cómo actualizar a Arcserve UDP 8.0 con el instalador único

Se puede actualizar a Arcserve UDP versión 8.0 utilizando el programa de instalación único. Consulte las sesiones compatibles antes de llevar a cabo la actualización.

Siga estos pasos:

1. Descargue ASDownloader.exe desde el vínculo de descarga de Arcserve.
2. Ejecute ASDownloader.exe, acepte el acuerdo de licencia y haga clic en **Siguiente**.
3. Haga clic en **Siguiente** en la pantalla **Iniciar**.
4. En la pantalla **Seleccionar los componentes que se descargarán**, seleccione los componentes que desea descargar.



Consideraciones para la selección de componentes:

- Para actualizar la versión anterior de Arcserve UDP, seleccione la opción **Arcserve Unified Data Protection**.
- Para actualizar la versión anterior de Arcserve Backup, seleccione la opción **Arcserve Backup**.

Nota: Algunos componentes se seleccionan automáticamente por dependencia cuando se elige la opción **Arcserve Backup**. Si no desea instalar los componentes en el mismo equipo, consulte Cómo actualizar a Arcserve UDP 8.0 desde una versión anterior y use el asistente de instalación para actualizar solo los componentes existentes. Desde aquí, puede descargar también la última configuración de Linux para Arcserve UDP.

5. Después de descargar los componentes, seleccione el método de instalación para actualizar aquellos seleccionados.

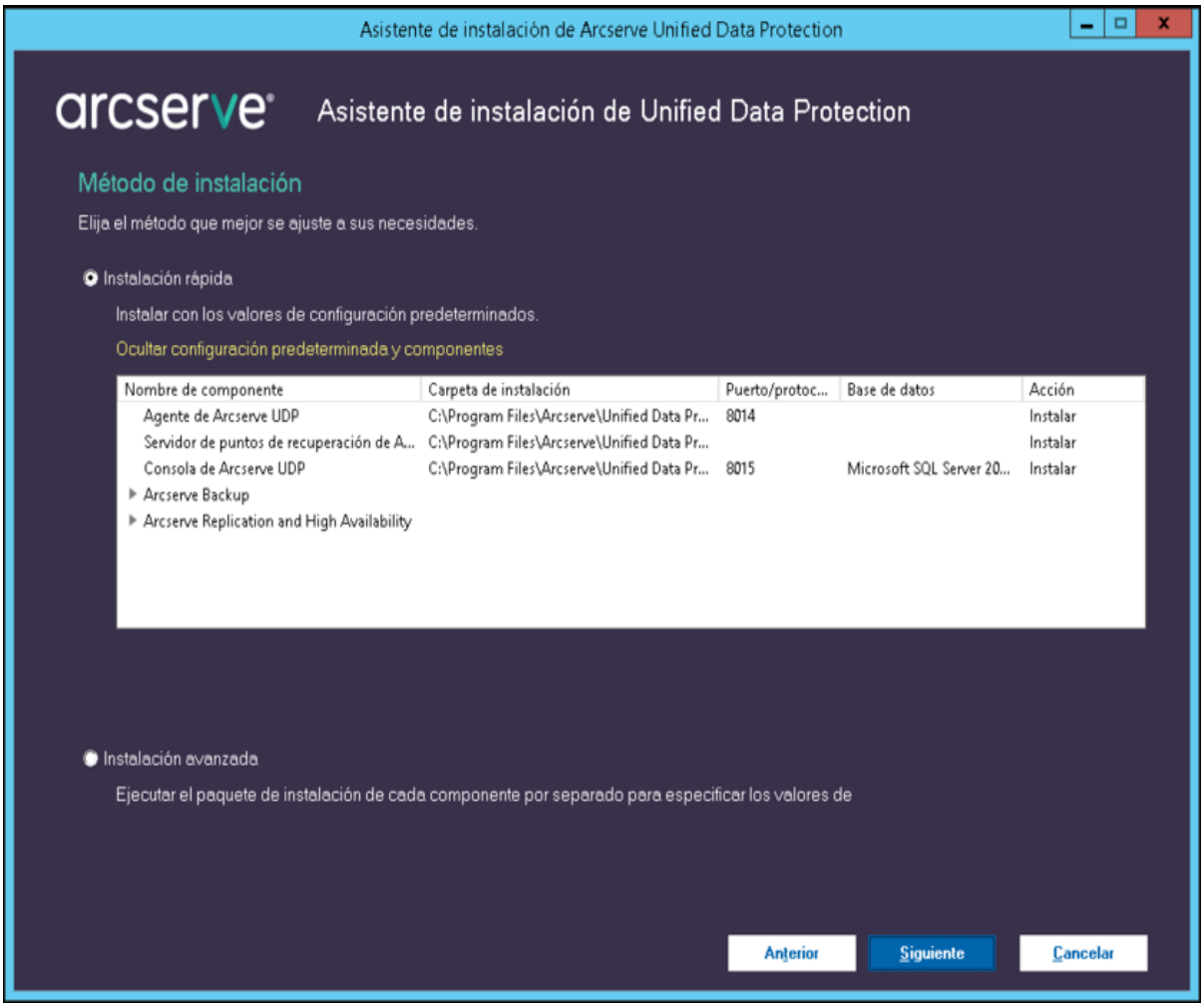
   Instalación rápida

   Se recomienda realizar una instalación rápida cuando se desea instalar todos los componentes con su configuración predeterminada en el mismo equipo.

   Notas:

   - Compruebe todos los requisitos previos para la actualización. Por ejemplo, .NET 4.5.1 resulta necesario para Arcserve Backup. Siga las instrucciones que se muestran en el instalador hasta que se cumplan todos los requisitos previos.
   - Compruebe el requisito de la Matriz de compatibilidad.
   - El método de instalación rápida instala los componentes según las configuraciones predeterminadas, por ejemplo, la ruta, el protocolo, el puerto y la base de datos. Cuando se actualiza utilizando el método de instalación

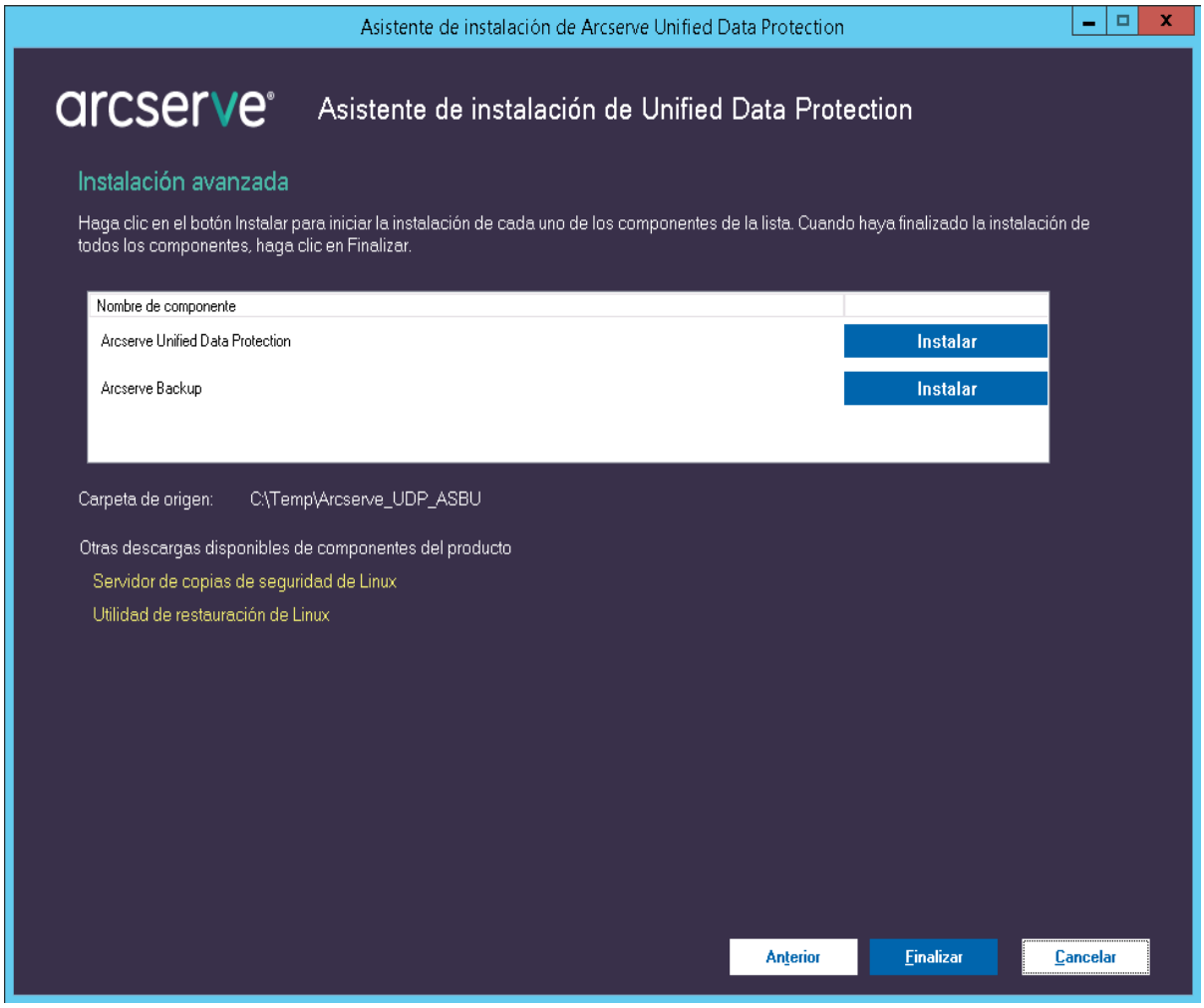
Express, se utiliza la configuración de la versión anterior.



Instalación avanzada

Se recomienda la instalación avanzada para la instalación o actualización de cada componente por separado en el mismo equipo. Haga clic en **Instalar** para actualizar o instalar cada componente por separado.

Nota: Para actualizar el Agente de Arcserve Unified Data Protection para Linux con el instalador unificado, descargue las imágenes mediante los vínculos compartidos que aparecen al final del instalador. Después de copiar las imágenes en el servidor de copia de seguridad de Linux, siga los pasos que se indican en *Cómo actualizar el Agente de Arcserve UDP (Linux)* en la Ayuda en línea del Agente para Linux.



Arcserve UDP se actualiza correctamente utilizando el instalador unificado.

Nota: Para obtener más información, consulte Cómo actualizar a Arcserve UDP 8.0 desde una versión anterior.

Cómo actualizar a Arcserve UDP 8.0 o Arcserve Backup 18.0 para activar la copia en cinta

Esta sección proporciona información sobre cómo actualizar a Arcserve UDP o Arcserve Backup 18.0 desde la versión anterior de Arcserve UDP o Arcserve Backup para permitir la copia en cinta. Arcserve UDP versión 8.0 se integra con Arcserve Backup 18.0 y proporciona una función para copiar los datos de la copia de seguridad a un destino de medio de cinta. Se puede modificar un plan existente o crear un plan con la tarea **Copia en cinta** en la Consola de Arcserve UDP.

Consideraciones sobre la actualización

- Para garantizar que el plan existente con la tarea Copia en cinta se ejecuta sin problemas, se debe actualizar Arcserve Backup a la versión 18.0 antes de actualizar Arcserve UDP a la versión 8.0.
- Compruebe el requisito de hardware de Arcserve UDP versión 8.0. Para obtener información más detallada sobre los requisitos de hardware, consulte la sección *Información del sistema* en las *Notas de la versión 8.0*.
- Se requiere una versión de la aplicación, del sistema operativo, del hipervisor o de la plataforma compatible con Arcserve UDP versión 8.0. Para obtener información detallada, consulte la matriz de compatibilidad.
- Antes de actualizar UDP 6.5.3 u otra versión anterior compatible, evite pausar un plan existente. Si el plan se pausa antes de una actualización, no se puede reanudar el plan hasta que se actualice el servidor de puntos de recuperación relacionado.
- Adquiera la clave de producto para Arcserve UDP versión 8.0 y téngala a mano.
- Se debe eliminar la versión anterior de la utilidad independiente Arcserve Exchange Granular Restore (AEGR) para Arcserve UDP versión 5.0. En caso de detectarse, el asistente de instalación solicita eliminarla.
- En condiciones ideales, los planes más antiguos deben funcionar correctamente en cada uno de los pasos de actualización que se describen a continuación.

Consideraciones sobre la copia en cinta

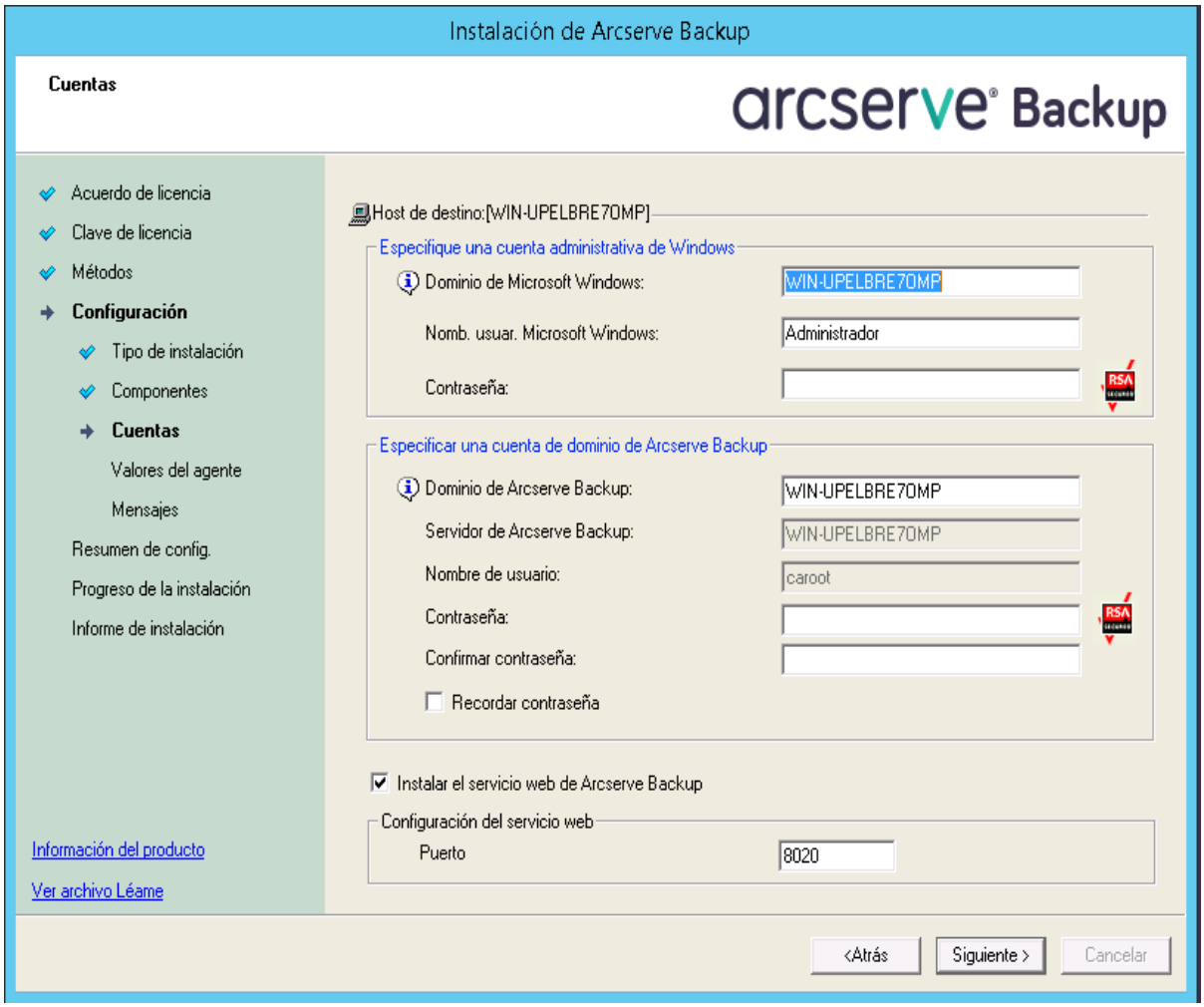
- Prepare el servidor de Arcserve Backup 18.0 instalando o actualizando desde cualquier ruta de actualización compatible anterior. Se requiere Arcserve Backup antes de configurar la tarea **Copiar en cinta** en un plan de Arcserve UDP.
- Compruebe si se cumplen los requisitos de Arcserve Backup 18.0. Para obtener

más información, consulte la Matriz de compatibilidad.

- Adquiera la clave del producto para Arcserve Backup 18.0 y téngala a mano.

Siga estos pasos para actualizar y activar la función Copiar en cinta:

1. Actualice a Arcserve Backup 18.0 desde una versión anterior o instale Arcserve Backup 18.0 con la opción **Servicio web de Arcserve Backup** activada.



Nota: Para obtener más información sobre la instalación y la actualización de Arcserve Backup, consulte la *Guía de implementación de Arcserve Backup 18.0*.

Cuando la actualización haya finalizado, realice las siguientes tareas:

- Verifique si se ha iniciado el motor de tareas en el gestor de Arcserve Backup.
- En la consola de servicios de Windows, verifique que el **servicio web de Arcserve Backup** se encuentre en ejecución.

2. Actualice a Arcserve UDP versión 8.0 desde una versión anterior.

Nota: Para obtener más información sobre cómo actualizar desde una versión anterior, consulte Cómo actualizar a Arcserve UDP 8.0 desde una versión anterior.

3. Configure la tarea **Copiar en cinta** en la Consola de Arcserve UDP para un plan nuevo o existente.

   Nota: Para obtener más información sobre cómo configurar la tarea Copiar en cinta, consulte Cómo crear un plan Copiar en cinta.

   El plan debe funcionar correctamente para cada paso.

Cómo migrar la Consola de Arcserve UDP de un servidor a otro

Para obtener más información, consulte el vínculo.

Cómo actualizar la puerta de enlace a la misma versión de su Consola registrada

La Puerta de enlace de Arcserve UDP debe coincidir con la versión de la Consola registrada. Tras la actualización de la Consola de Arcserve UDP, se verifica la versión de la puerta de enlace relacionada cuando se inicia el servicio. Si la versión de la puerta de enlace no coincide con la versión de la Consola, Arcserve UDP activa automáticamente una actualización automática para los servidores de la puerta de enlace.

Si la puerta de enlace no está disponible para una actualización automática, puede actualizarla manualmente más tarde.

Siga estos pasos para actualizar manualmente la puerta de enlace:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Haga clic en la ficha **recursos**, vaya a **Infraestructura** y haga clic en **Sitios**.
3. Seleccione el sitio que desea actualizar.
4. En la lista desplegable **Acciones**, haga clic en **Actualizar puerta de enlace**.

   Aparecerá un diálogo de confirmación.
5. Haga clic en **Sí**.

   La puerta de enlace se actualiza con la última versión de la puerta de enlace de Arcserve UDP.

Cómo realizar la migración de la Consola de Arcserve UDP

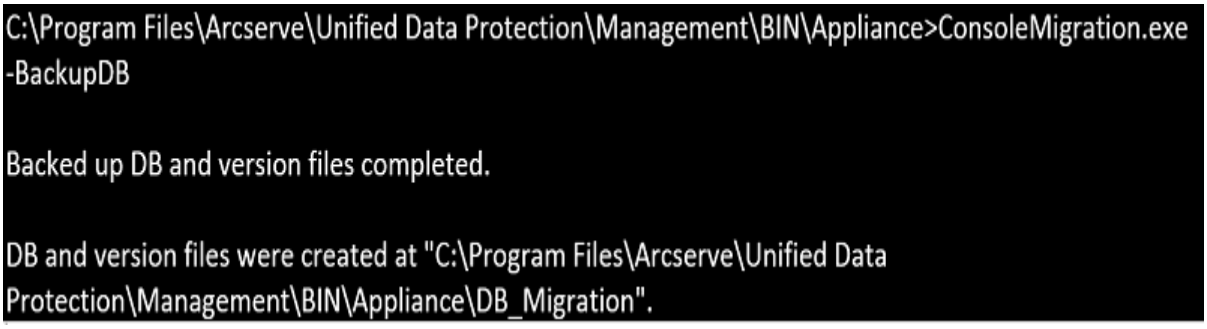
Se puede migrar una Consola de Arcserve UDP a otra Consola de Arcserve UDP utilizando *ConsoleMigration.exe*. A partir de Arcserve UDP v6.5 Actualización 2 en adelante, se puede migrar la Consola de Arcserve UDP entre dos Consolas de Arcserve UDP.

Utilice *ConsoleMigration.exe* para Base de datos de la copia de seguridad y Recuperar base de datos. La captura de pantalla siguiente muestra el uso de *ConsoleMigration.exe*:



Para completar el proceso de migración, siga estos pasos:

1. En la Consola de Arcserve UDP anterior, realice la copia de seguridad de la base de datos de Arcserve UDP

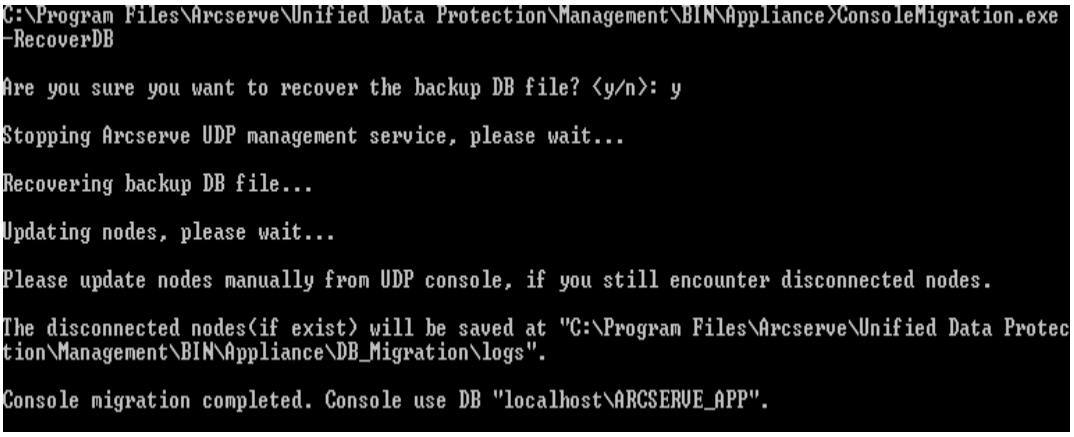


   Se crea la carpeta *DB_Migration* correctamente.

2. En la nueva Consola de Arcserve UDP, copie la carpeta *DB_Migration* en la ruta siguiente:

   <directorio_principal_UDP>\Management\BIN\Appliance

3. En la nueva Consola de Arcserve UDP, realice los pasos que se indican en la pantalla siguiente para recuperar la base de datos de la Consola deArcserve UDP



   Nota: En la Consola de Arcserve UDP, si existe algún otro sitio distinto al sitio local, siga los pasos que se mencionan en el archivo *NewRegistrationText.txt* para volver a registrarse en el sitio.

Se ha completado correctamente la migración de la Consola de Arcserve UDP a la nueva Consola de Arcserve UDP.

Se puede utilizar esta herramienta para realizar la migración de la consola para la Consola de Arcserve UDP conectada con la base de datos remota de SQL. Una vez completada la migración, la Consola de Arcserve UDP migrada estará configurada para conectarse con la misma base de datos remota de SQL.

Nota: En UDP v6.5 Actualización 2 y Actualización 3, cuando se utiliza la herramienta de migración de la Consola para realizar la migración de la consola entre dos Consolas de Arcserve UDP, las versiones de las dos Consolas de Arcserve UDP y las versiones de la base de datos de SQL deben ser coherentes en los dos sistemas de la Consola de Arcserve UDP. De lo contrario, se producirá un error en la migración de la consola y se mostrará un mensaje de error en la línea de comandos y en los archivos de registro de la siguiente ruta:

<directorio_principal_UDP>\Management\BIN\Appliance\logs

En Arcserve UDP v6.5 Actualización 4, la opción ***-force*** se ha introducido en el comando ***ConsoleMigration.exe*** para forzar la migración de archivos de la copia de seguridad de la base de datos de recuperación a la consola de destino en las siguientes condiciones:

1. Cuando se desea realizar la migración de consola entre dos consolas, donde la consola de origen utiliza SQL Server Enterprise Edition y la consola de destino utiliza SQL Server Express Edition. En este caso, el tamaño mínimo necesario de la base de datos de la Consola de UDP de origen es de 4000 MB.
2. Cuando se desea realizar la migración de consola desde una consola que utiliza una versión avanzada de la base de datos de SQL Server a una consola que utiliza una versión anterior de la base de datos de SQL Server. Por ejemplo, se migra desde una consola que utiliza SQL Server 2016 a una consola que utiliza SQL Server 2014.

Capítulo 5: Exploración y configuración de Arcserve UDP

Esta sección incluye los siguientes temas:

Inicio de sesión en la Consola de Arcserve UDP utilizando la autenticación multifactor

Arcserve UDP es compatible con la autenticación multifactor (MFA) que proporciona un nivel adicional de seguridad para todos los usuarios. MFA es un proceso de inicio de sesión en el que se solicita al usuario que proporcione una forma adicional de identificación. Este método de autenticación requiere más de un factor para verificar la identidad del usuario. En general, el proceso de inicio de sesión de MFA utiliza la autenticación de dos factores que permite dos factores para la identificación del usuario.

Arcserve UDP admite la autenticación de dos factores. Permite el nombre de usuario y la contraseña como el primer factor de autenticación. La autenticación del segundo factor utiliza uno de los siguientes:

- **Código de acceso de un solo uso basado en el tiempo (TOTP):** A diferencia de la OTP tradicional que se envía a una dirección de correo electrónico o por SMS, un TOTP se genera mediante una aplicación de autenticación. El TOTP es válido durante poco tiempo y se actualiza cada 30 segundos.
- **OTP de correo electrónico:** Esta función se autentica con una OTP que se envía a la dirección de correo electrónico registrada y la OTP es válida durante 30 segundos. Se activa solamente cuando se ha configurado la dirección de correo electrónico.

Esta sección incluye los siguientes temas:

Revisión de los requisitos previos

Tenga en cuenta los siguientes requisitos previos:

- Se debe activar la autenticación multifactor (MFA) para todos los usuarios. Para obtener más información sobre cómo activar la autenticación multifactor, consulte Configuración de la autenticación multifactor como usuario administrador.

  Nota: Solo los administradores pueden activar la autenticación multifactor (MFA) para todos los usuarios.

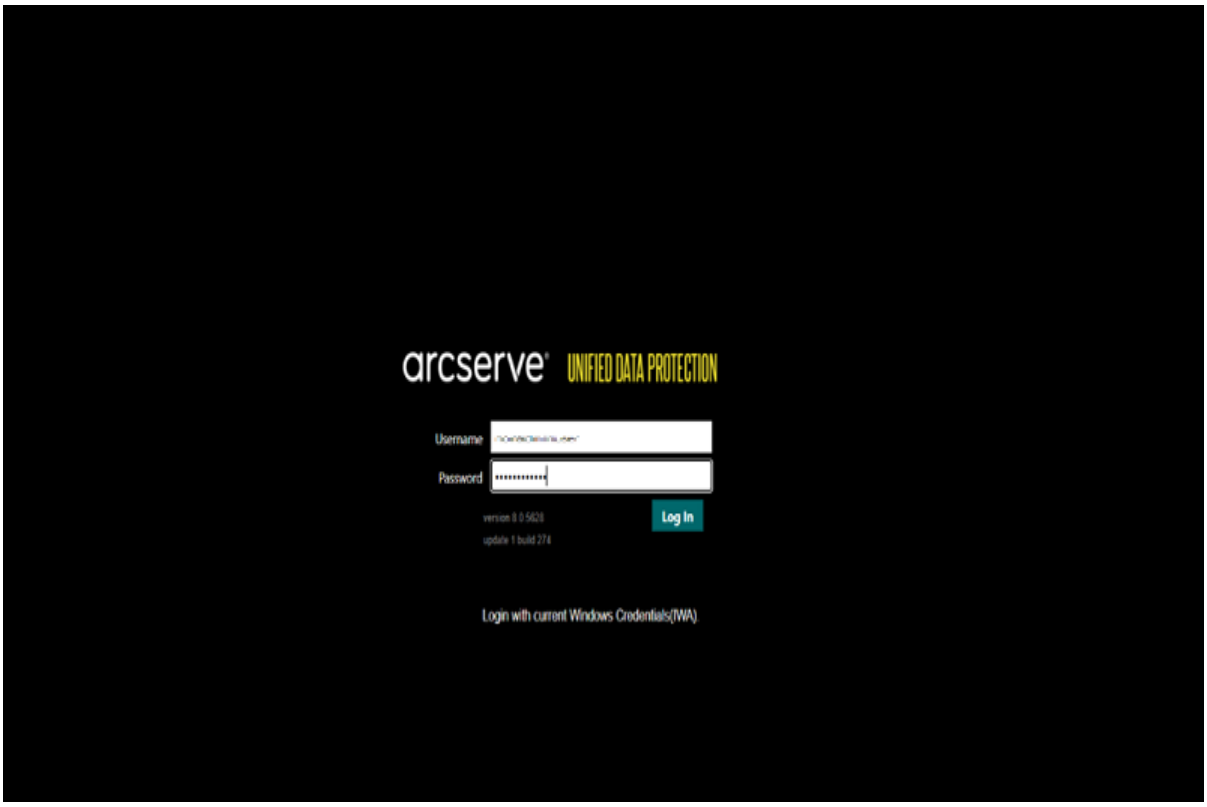
- Instale una aplicación de autenticación móvil en su dispositivo móvil. Puede encontrar las aplicaciones de autenticación como Google Authenticator o Microsoft Authentication en la tienda de aplicaciones de su dispositivo móvil.

Cómo iniciar sesión en la Consola de Arcserve UDP utilizando MFA

Esta sección proporciona información sobre cómo iniciar sesión en la Consola de Arcserve UDP utilizando MFA.

Siga estos pasos:

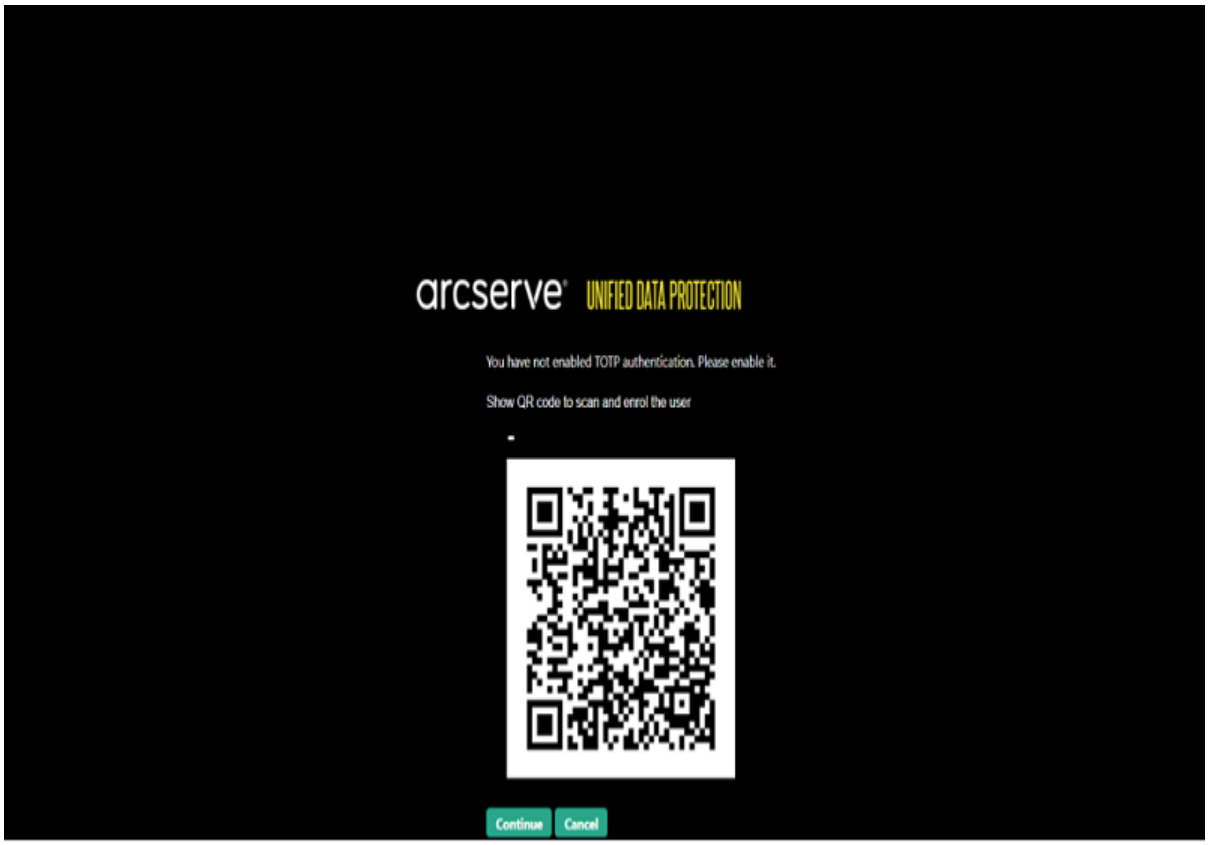
1. Vaya a la página de inicio de sesión de la Consola de UDP.
2. Escriba el nombre de usuario y la contraseña según sea necesario y, a continuación, haga clic en el botón **Iniciar sesión**.



Tras la correcta verificación de la autenticación del primer factor, aparece la página de la autenticación del segundo factor.

3. Si no se ha activado la autenticación TOTP, para activarla, haga lo siguiente:
   a. Haga clic en el vínculo **Mostrar código QR para explorar e inscribir al usuario**.

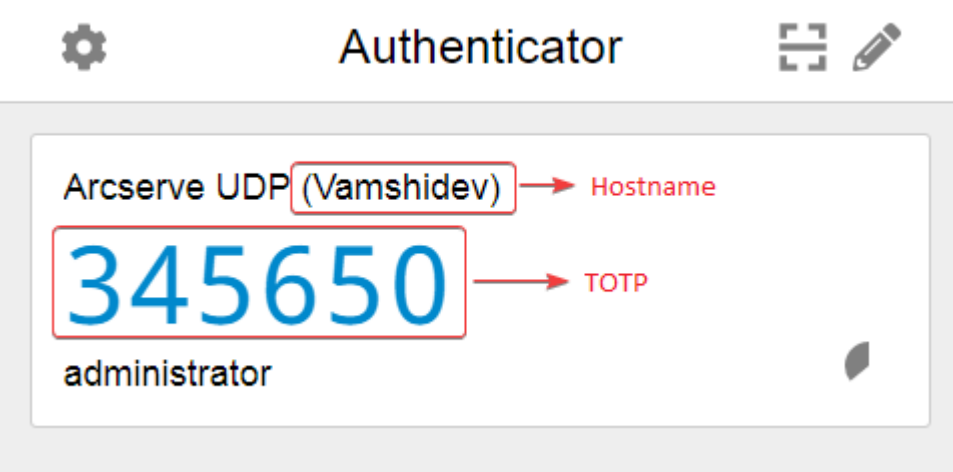
Aparece la imagen del código QR.



b. Para generar el TOTP, escanee la imagen del código QR con una aplicación de autenticación.

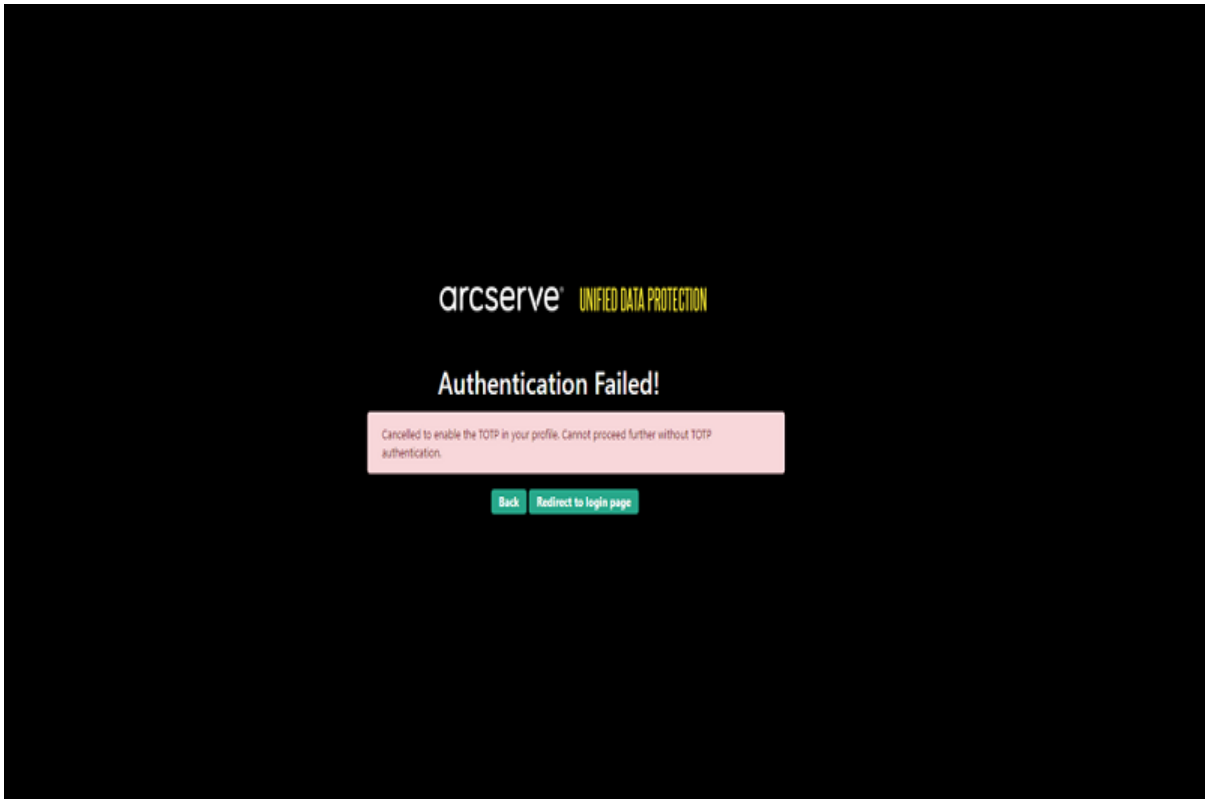
Notas:

- Se puede utilizar cualquiera de las aplicaciones de autenticación móvil como la aplicación Google Authenticator o la aplicación Microsoft Authenticator del dispositivo móvil. De forma alternativa, también se puede utilizar la extensión Authenticator para el explorador Chrome.
- Cuando se utiliza una aplicación de autenticación para varias cuentas de usuario, el nombre de host de la cuenta de usuario diferencia a los TOTP. En la aplicación de autenticación, se puede ver el nombre de host y su respectivo TOTP.



c. Haga clic en el botón **Continuar**.

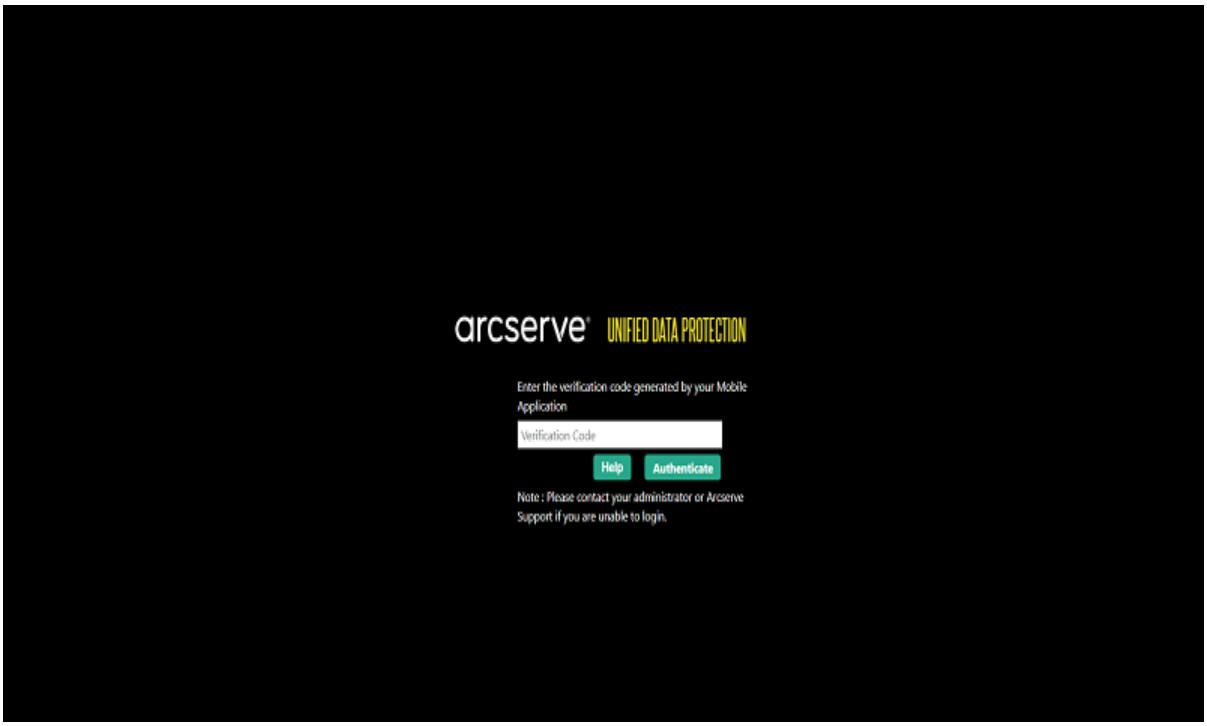
Si hace clic en el botón **Cancelar**, se producirá un error en la autenticación.



Nota: Si se ha activado previamente el factor de autenticación TOTP, no se le pedirá que realice el paso 3.

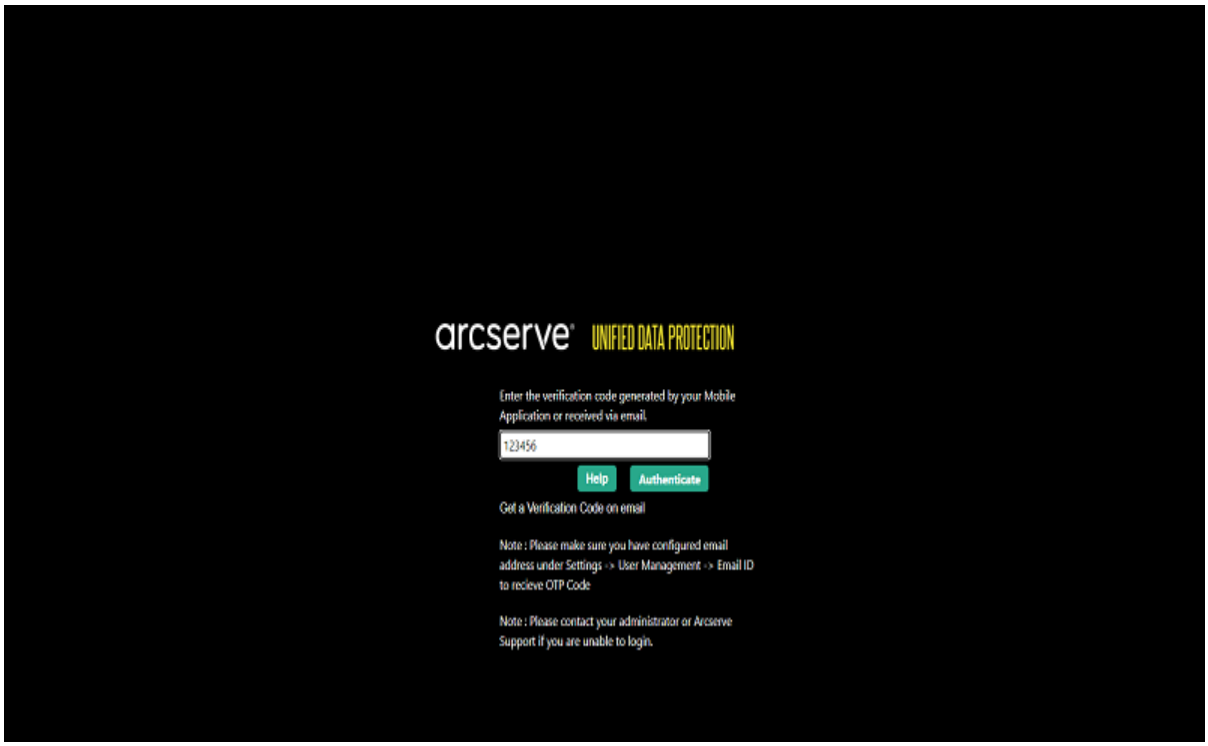
4. En el campo Código de verificación, escriba el TOTP.

Para el TOTP, abra la aplicación de autenticación móvil en el dispositivo móvil o la extensión Authenticator del explorador Chrome. El número es válido durante 30 segundos y se actualiza cada 30 segundos.



5. (Opcional) Si no dispone de TOTP, haga lo siguiente:
   a. Haga clic en el vínculo **Obtener un código de verificación en el correo electrónico**.

      La OTP temporal del correo electrónico se envía a la dirección de correo electrónico.



Notas:

- La opción de OTP de correo electrónico a la que solo se accede cuando un usuario administrador activa la OTP de correo electrónico y configura los valores de configuración del correo electrónico. Para obtener más información, consulte Configuración de la autenticación multifactor como usuario administrador.
- Asegúrese de configurar la dirección de correo electrónico en *Configuración* > *Gestión de usuarios* para recibir la OTP de correo electrónico.

b. En el campo del código de verificación, escriba la OTP de correo electrónico.

6. Haga clic en el botón **Autenticar**.

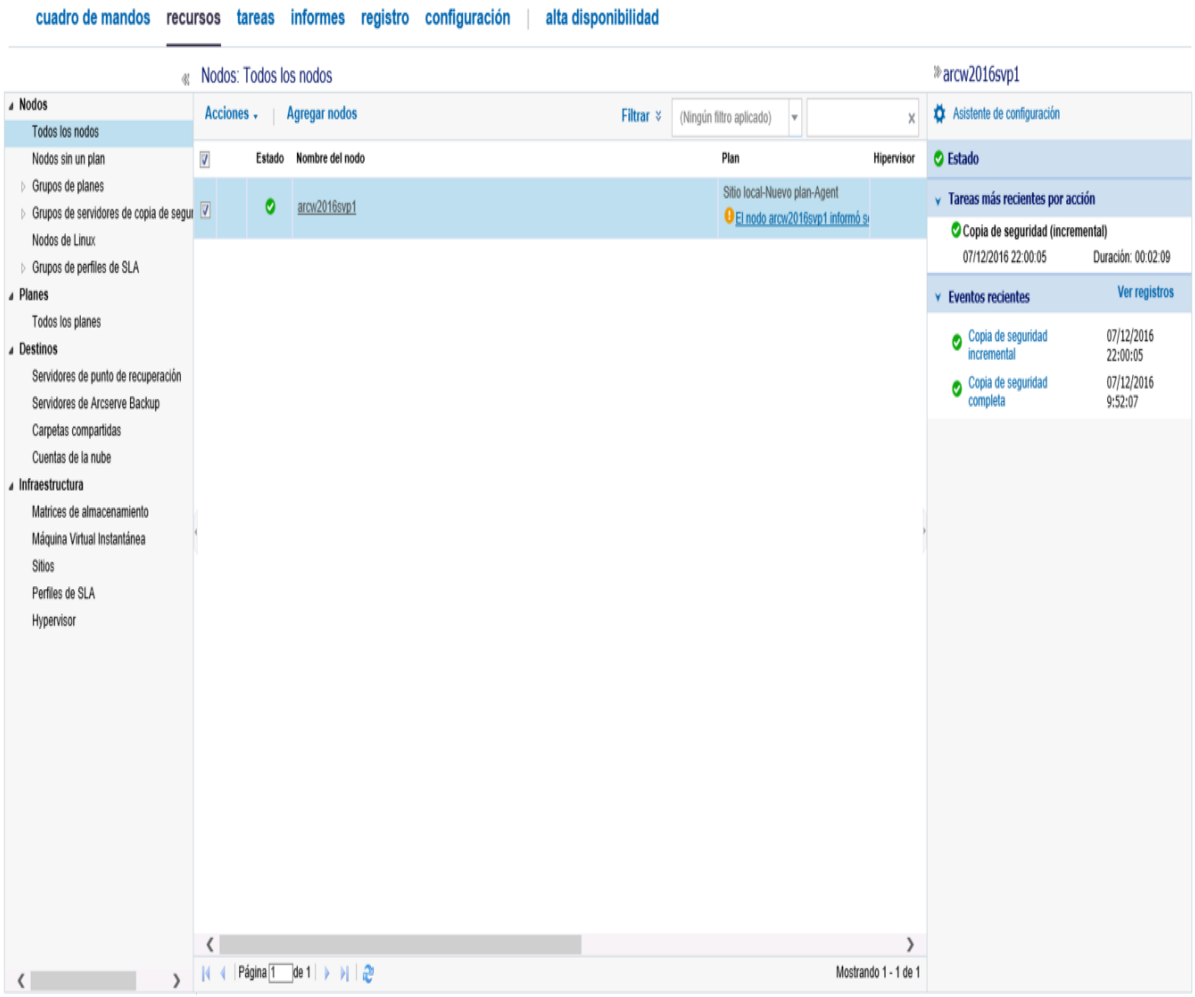
   Se ha iniciado sesión correctamente en la Consola de UDP.

Arcserve Unified Data Protection Interfaz de usuario

Antes de utilizar Arcserve Unified Data Protection, familiarícese con la interfaz de usuario. La interfaz de Arcserve Unified Data Protection permite realizar las tareas siguientes:

- Gestionar y controlar tareas
- Agregar y gestionar nodos de origen
- Agregar y gestionar servidores de punto de recuperación de destino
- Gestionar planes para crear programaciones de copia de seguridad
- Obtener estadística de protección de datos
- Ver registros de errores y advertencias
- Gestionar y controlar Arcserve High Availability
- Configurar los valores de configuración de protección de datos
- Restaurar datos de copias de seguridad

Navegación en Arcserve UDP



Fichas

Permiten ir a las distintas funciones de Arcserve Unified Data Protection.

Paneles

Cuando va a cada ficha, la pantalla mostrada se divide en los paneles siguientes. Cada panel se usa para realizar acciones relacionadas.

Panel izquierdo

Le permite ir a diversas funciones y operaciones. El resultado de cada clic se muestra en el panel central.

Panel central

Le permite realizar la mayor parte de las acciones en este panel como agregar, suprimir y modificar. Este panel también muestra el resultado y estado de cada actividad como tareas, planes e informes. La mayor parte de las

acciones se realizan en este panel. La información mostrada en esta página es en su mayoría el resultado de las opciones seleccionadas en el panel izquierdo.

Panel derecho

Se muestra un resumen de los elementos seleccionados en el panel central. Por ejemplo, en la ficha Tareas, si se ha seleccionado una tarea del panel central, entonces se mostrará en el panel derecho un breve resumen de la tarea ofreciendo la información como el controlador de tarea (si hay una tarea en ejecución) y los detalles de la tarea como el nombre de nodo de origen, la tarea, el servidor de punto de recuperación de destino y el almacén de datos de destino.

Fichas

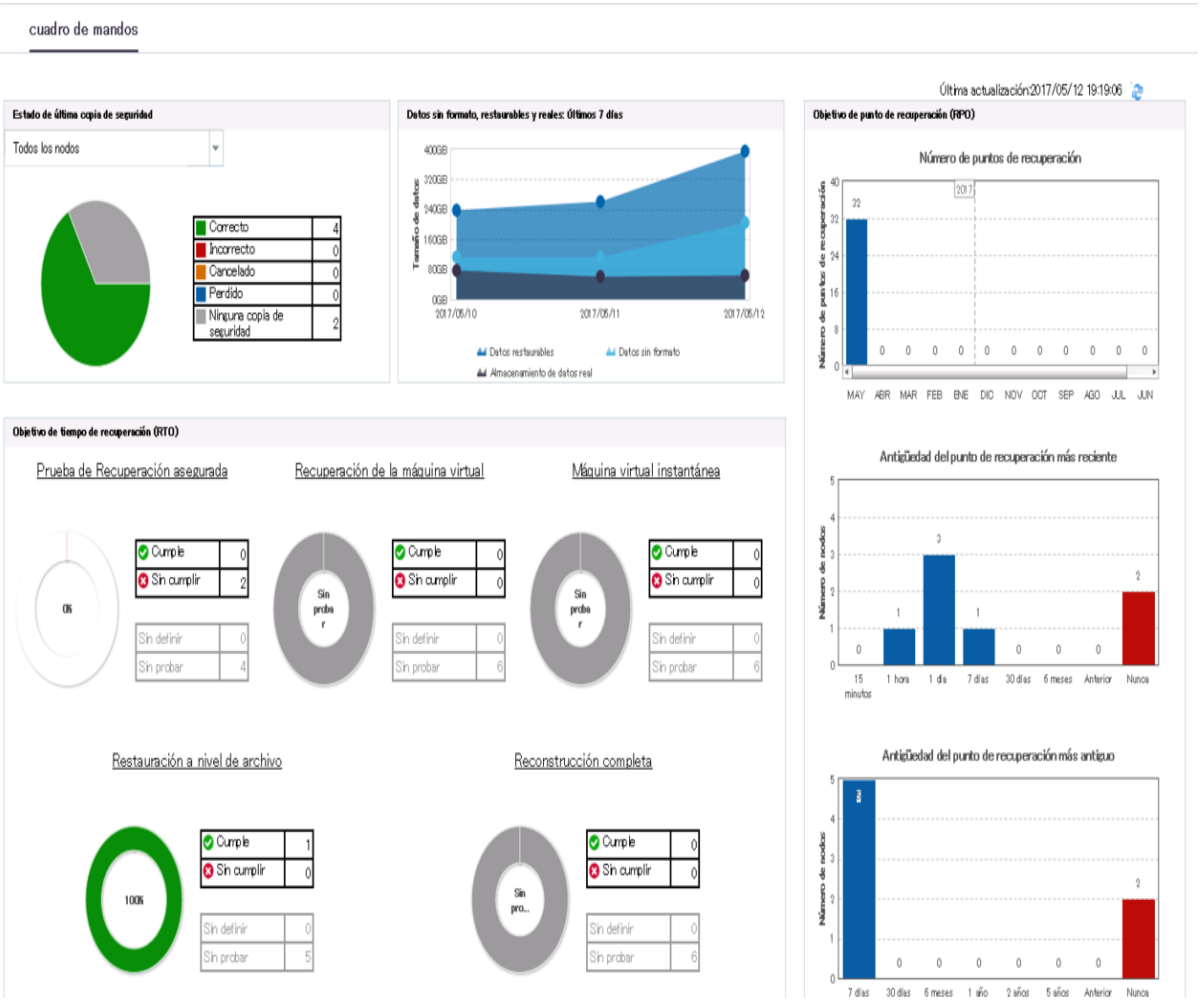
La solución Arcserve Unified Data Protection proporciona las fichas siguientes para desempeñar funciones de protección de datos:

- cuadro de mandos
- recursos
- tareas
- informes
- registro
- configuración
- High Availability

cuadro de mandos

La ficha **cuadro de mandos** le permite ver la representación gráfica del estado y del almacenamiento de datos de la tarea más reciente de los últimos siete días. Mediante la ficha **cuadro de mandos**, se pueden realizar las acciones siguientes en los informes:

- Ver la hora de la última actualización. Al hacer clic en el icono *Actualizar* se muestra los datos más recientes en el cuadro de mandos.
- Al hacer clic en el gráfico de barras del informe de RTO se abre directamente la página Informes de RTO.
- Vea el último estado de la tarea de los nodos o planes según los filtros que se seleccionan en el gráfico **Último estado de la tarea**.



Se pueden ver las gráficas para las siguientes opciones en la ficha cuadro de mandos:

Último estado de la tarea

Último estado de la tarea hace referencia al último estado de la tarea y proporciona varios filtros para ver el estado. En función de la selección de la opción de filtrado, se podrá ver el estado de la última tarea. Por ejemplo, seleccione **Todos los nodos** para ver el estado de la última tarea de todos los nodos o seleccione cualquier plan para ver el estado de la última tarea de los nodos protegidos por este plan. A continuación, filtre aún más con un tipo de tarea específico. Cuando se selecciona **Todos los nodos**, se puede ver el estado siguiente:

- **Correcto** indica que se ha realizado correctamente la copia de seguridad de los nodos.
- **Erróneo** indica que la última copia de seguridad no es correcta.
- **Cancelado** indica que se ha detenido la última copia de seguridad.
- **Perdido** indica que no se ha realizado la última copia de seguridad tal y como estaba programada.
- **No conectado** indica que se ha producido un error en la Consola de Arcserve UDP al conectarse con el nodo.
- **Incompleto** indica que la tarea de restauración no ha finalizado.

Cuando se hace clic en cada sector (del estado) del gráfico circular, la página **recursos** se abrirá y se mostrarán los nodos asociados. Por ejemplo, si se hace clic en **Correcto** en el gráfico circular, se abrirá la página **recursos**. La página **recursos** muestra los nodos que no tienen ningún plan. Además, el filtro **Correcto** está preseleccionado en la página **recursos**.

Tamaño de los datos sin formato, restaurables y reales: 7 días

La gráfica se refiere a los datos sin formato frente a los datos sin formato frente a los datos restaurables frente al almacenamiento de los datos reales.

Tamaño de los datos restaurables

Se refiere al tamaño de los datos que se pueden restaurar a partir de los datos almacenados en todo el almacenamiento de destino de ese día. Sin tener en cuenta el tipo de copia de seguridad, ya sea copia de seguridad completa o copia de seguridad incremental, cada punto de recuperación se utiliza para restaurar un origen completo. Este tamaño es el tamaño total disponible de todos los orígenes restaurados.

Por ejemplo, si el tamaño de los datos sin formato es de 30 GB y después de la compresión y de la deduplicación el tamaño es de 22 GB, pero los datos restaurables tienen un tamaño de 30 GB para la primera copia de

seguridad completa. Para realizar un cambio incrementales de 4 GB, el tamaño de los datos restaurables será 30 + 34 GB = 64 GB.

Tamaño del almacenamiento de datos real

Se refiere al tamaño de los datos finales. Después de la compresión de los datos sin formato, de la eliminación de los bloques de datos duplicados de los datos sin formato y de la adición de algunos metadatos, los datos sin formato se convierten en los datos finales y se guardan en el almacenamiento de destino.

Tamaño de los datos sin formato

Hace referencia a los datos leídos desde el origen y transferidos al destino.

Informe de acuerdo de nivel de servicio para RTO y RPO

Arcserve UDP presenta el informe del acuerdo de nivel de servicio (SLA) para ayudar a las organizaciones a generar informes de cumplimiento relacionados con el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO).

Informe de RTO

El informe de RTO de Arcserve UDP es un informe de cumplimiento que compara el valor real del tiempo de recuperación y el valor del objetivo de tiempo de recuperación para todos los tipos de tarea de recuperación ejecutados, tales como la restauración del sistema de archivos, la recuperación de la máquina virtual, la reconstrucción completa, la máquina virtual instantánea y la recuperación asegurada. El gráfico de barras utiliza varios colores para mostrar el estado de las tareas. Además, se puede filtrar por el estado del objetivo del tiempo de recuperación a nivel de nodo para visualizar únicamente resultados por objetivo cumplido, sin cumplir, sin probar o sin definir.

Informe de RPO

Arcserve UDPEl informe de RPO de muestra el número total de nodos con puntos de recuperación disponibles durante el período de tiempo específico en la vista de barras, categorizado por la antigüedad de los puntos de recuperación más recientes (15 minutos, última hora, últimas 12 horas, último día y así sucesivamente), por la antigüedad de los puntos de recuperación más antiguos (30 días y anteriores) o por mes (de enero a diciembre). Además, se pueden visualizar los detalles del estado del nodo según la categoría seleccionada.

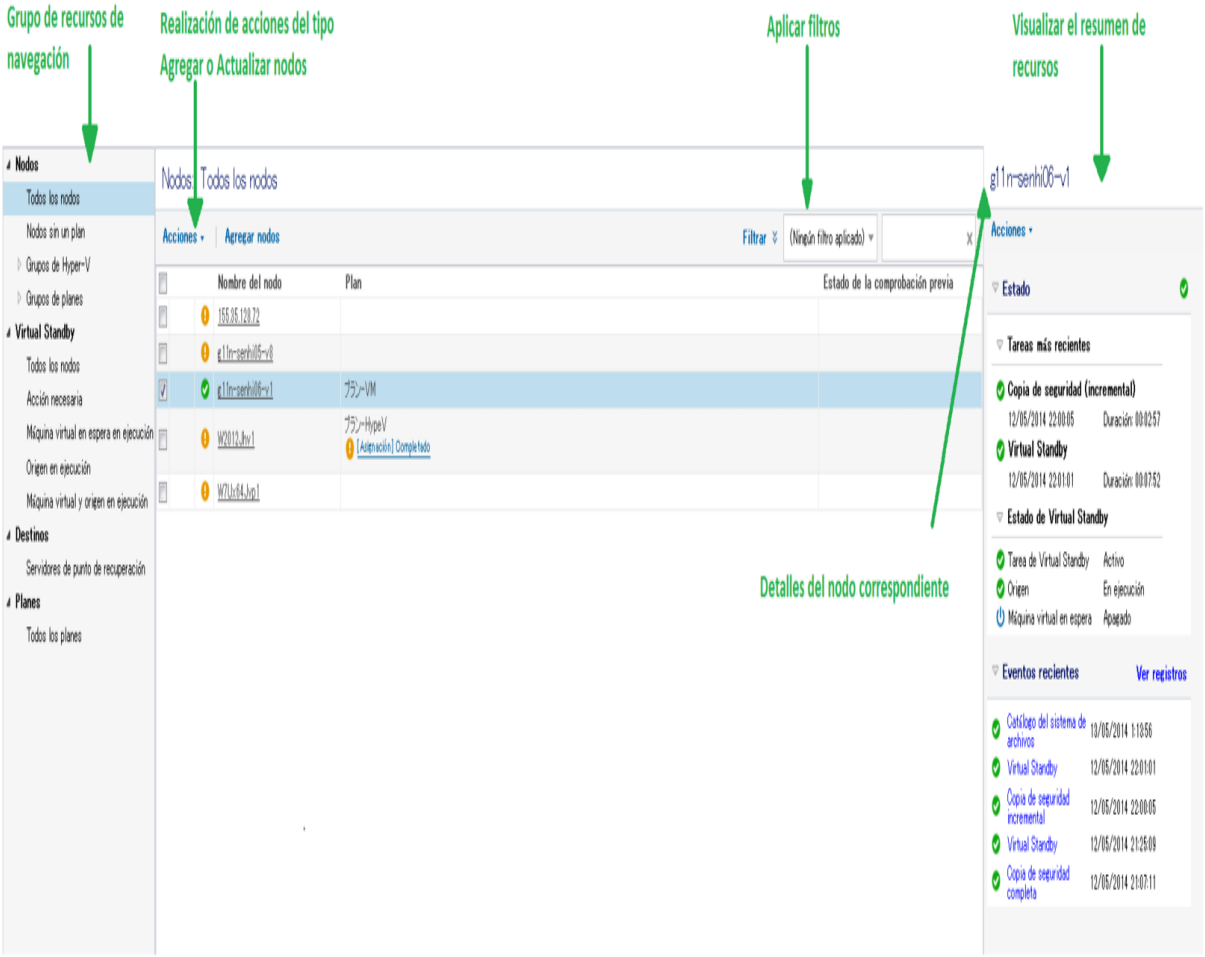
Nota: En el cuadro de mandos, se puede ver directamente el informe de RPO de un mes concreto. El informe se rellena directamente desde el Cuadro de mandos de Arcserve UDP. Al hacer clic dentro de la gráfica de barras de RPO en un mes en el Cuadro de mandos, se mostrará la pantalla de informe de RPO para ese mes específico en la pantalla de RPO.

recursos

La ficha **recursos** permite gestionar los recursos de Arcserve Unified Data Protection: Nodos, destinos, Virtual Standby y planes. Utilice esta ficha para agregar recursos a Arcserve Unified Data Protection, como los nodos que desea proteger o los servidores de puntos de recuperación de los que desea realizar una copia de seguridad. También se utiliza esta ficha para crear planes y tareas para la copia de seguridad, Virtual Standby y replicación. Mediante la ficha recursos, se pueden realizar las acciones siguientes en los informes:

- Gestión de nodos
- Gestión del destino
- Gestión de planes
- Gestión de la infraestructura

Nota: Solo la ficha **recursos** de la Consola identifica el sitio. En las demás fichas de la Consola se muestran datos consolidados de todos los sitios. Para obtener más información sobre los sitios, consulte Cómo agregar y gestionar un sitio.


Grupo de recursos de navegación
Realización de acciones del tipo Agregar o Actualizar nodos
Aplicar filtros
Visualizar el resumen de recursos
Nodos
Todos los nodos
Nodos sin un plan
Grupos de Hyper-V
Grupos de planes
Virtual Standby
Todos los nodos
Acción necesaria
Máquina virtual en espera en ejecución
Origen en ejecución
Máquina virtual y origen en ejecución
Destinos
Servidores de punto de recuperación
Planes
Todos los planes
Nodos Todos los nodos
Acciones
Agregar nodos
Filtrar
(Ningún filtro aplicado)
Nombre del nodo
Plan
Estado de la comprobación previa
Detalles del nodo correspondiente
g11n-senhi08-v1
Acciones
Estado
Tareas más recientes
Copia de seguridad (incremental)
12/05/2014 22:00:05
Duración 00:02:57
Virtual Standby
12/05/2014 22:01:01
Duración 00:07:52
Estado de Virtual Standby
Tarea de Virtual Standby
Activo
Origen
En ejecución
Máquina virtual en espera
Apagado
Eventos recientes
Ver registros
Catálogo del sistema de archivos
13/05/2014 1:18:56
Virtual Standby
12/05/2014 22:01:01
Copia de seguridad incremental
12/05/2014 22:00:05
Virtual Standby
12/05/2014 21:25:09
Copia de seguridad completa
12/05/2014 21:07:11

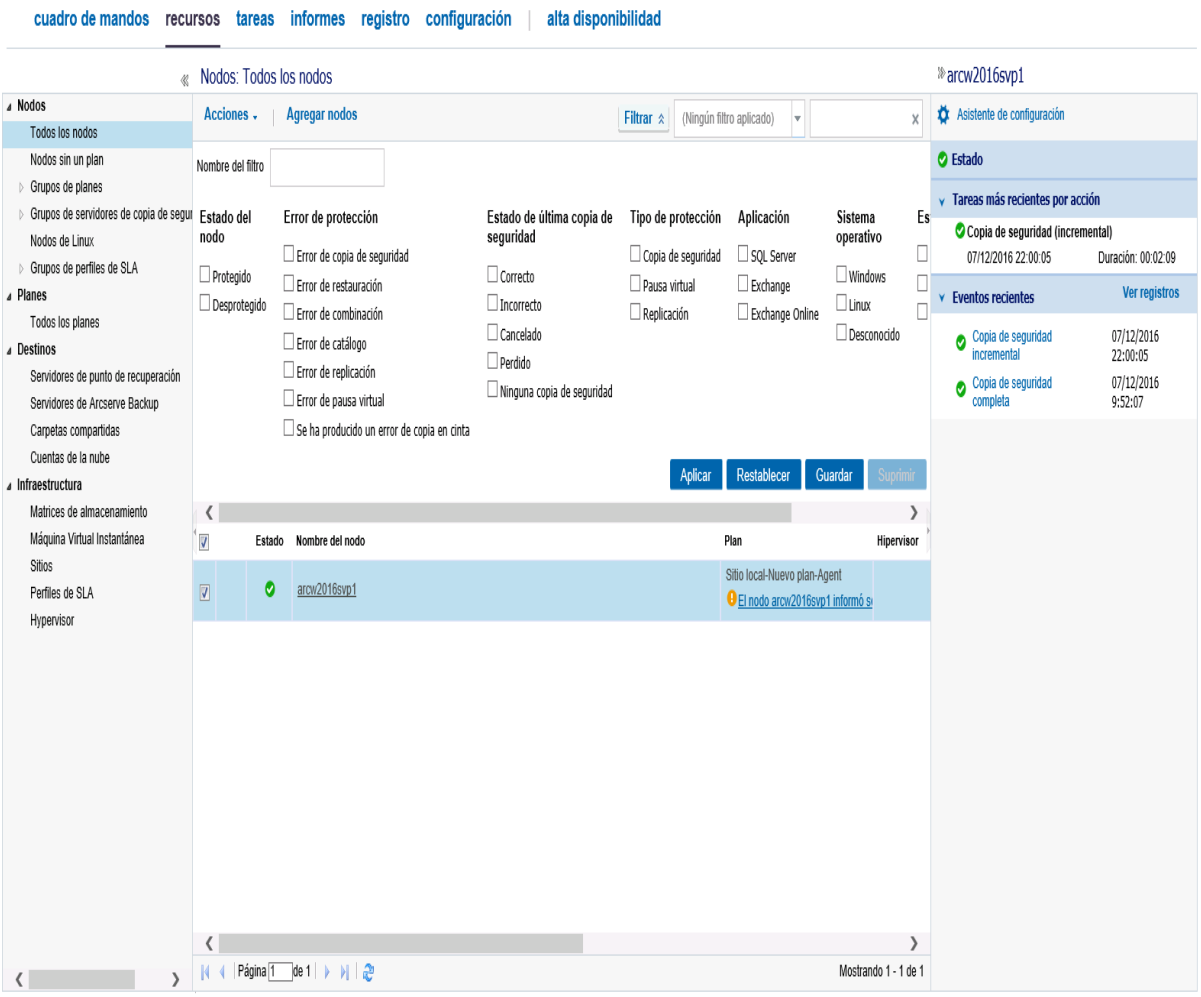
Gestión de nodos

La vista de gestión de nodos le permite gestionar todos los nodos y aplicar filtros para refinar la búsqueda de nodos. Cuando se selecciona un nodo específico en panel central, se pueden ver el estado y los eventos recientes sobre el nodo en panel derecho. Se pueden aplicar diversos filtros del panel central. Se pueden crear grupos de nodos en el panel izquierdo para agrupar nodos específicos.

Cuando se selecciona un nodo del panel central, se muestran el estado de nodo y los eventos recientes en el panel derecho.

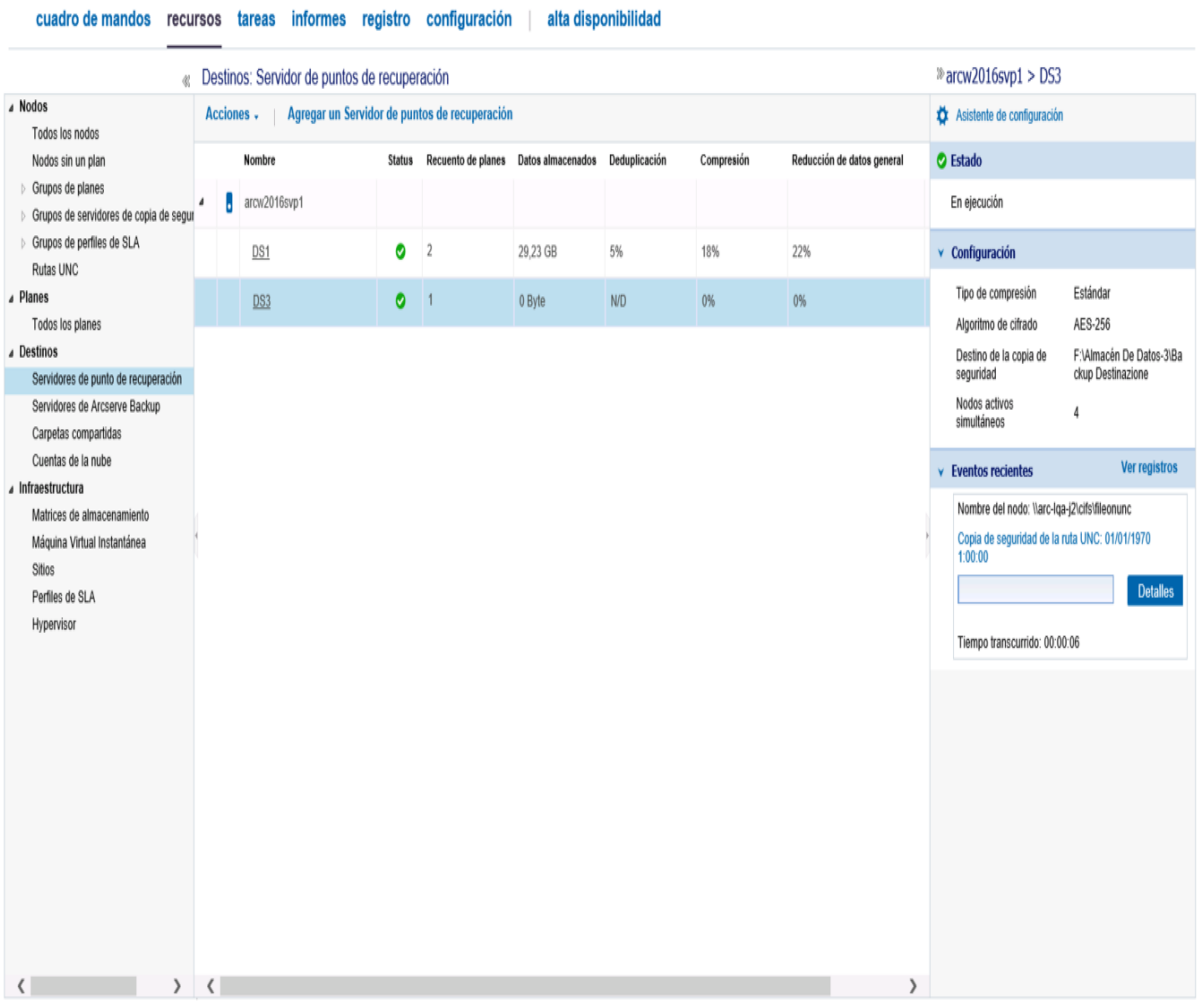
Se pueden realizar operaciones en los nodos haciendo clic en el menú desplegable Acciones del panel central. Aquellas operaciones que se pueden realizar mediante el menú Acciones del panel central se aplican a todos los nodos de origen. Aquellas operaciones que se pueden realizar mediante el menú Acciones del panel derecho se aplican solamente al nodo que se ha seleccionado en el panel central.

En la ficha Recursos, haga clic en **Todos los nodos** bajo el nodo en el panel izquierdo. A continuación, en el panel central, seleccione un nodo y haga clic en **Filtro** para ver las opciones de gestión de nodos. Puede seleccionar las casillas de verificación de las opciones que desea y hacer clic en **Aplicar**.


cuadro de mandos
recursos
tareas
informes
registro
configuración
alta disponibilidad
Nodos: Todos los nodos
arcw2016svp1
Nodos
Todos los nodos
Nodos sin un plan
Grupos de planes
Grupos de servidores de copia de segur
Nodos de Linux
Grupos de perfiles de SLA
Planes
Todos los planes
Destinos
Servidores de punto de recuperación
Servidores de Arcserve Backup
Carpetas compartidas
Cuentas de la nube
Infraestructura
Matrices de almacenamiento
Máquina Virtual Instantánea
Sitios
Perfiles de SLA
Hypervisor
Acciones
Agregar nodos
Filtrar
(Ningún filtro aplicado)
Nombre del filtro
Estado del nodo
Protegido
Desprotegido
Error de protección
Error de copia de seguridad
Error de restauración
Error de combinación
Error de catálogo
Error de replicación
Error de pausa virtual
Se ha producido un error de copia en cinta
Estado de última copia de seguridad
Correcto
Incorrecto
Cancelado
Perdido
Ninguna copia de seguridad
Tipo de protección
Copia de seguridad
Pausa virtual
Replicación
Aplicación
SQL Server
Exchange
Exchange Online
Sistema operativo
Windows
Linux
Desconocido
Aplicar
Restablecer
Guardar
Suprimir
Estado
Nombre del nodo
Plan
Hipervisor
arcw2016svp1
Sitio local-Nuevo plan-Agent
Página 1 de 1
Mostrando 1 - 1 de 1
Asistente de configuración
Estado
Tareas más recientes por acción
Copia de seguridad (incremental)
07/12/2016 22:00:05
Duración: 00:02:09
Eventos recientes
Ver registros
Copia de seguridad incremental
07/12/2016 22:00:05
Copia de seguridad completa
07/12/2016 9:52:07

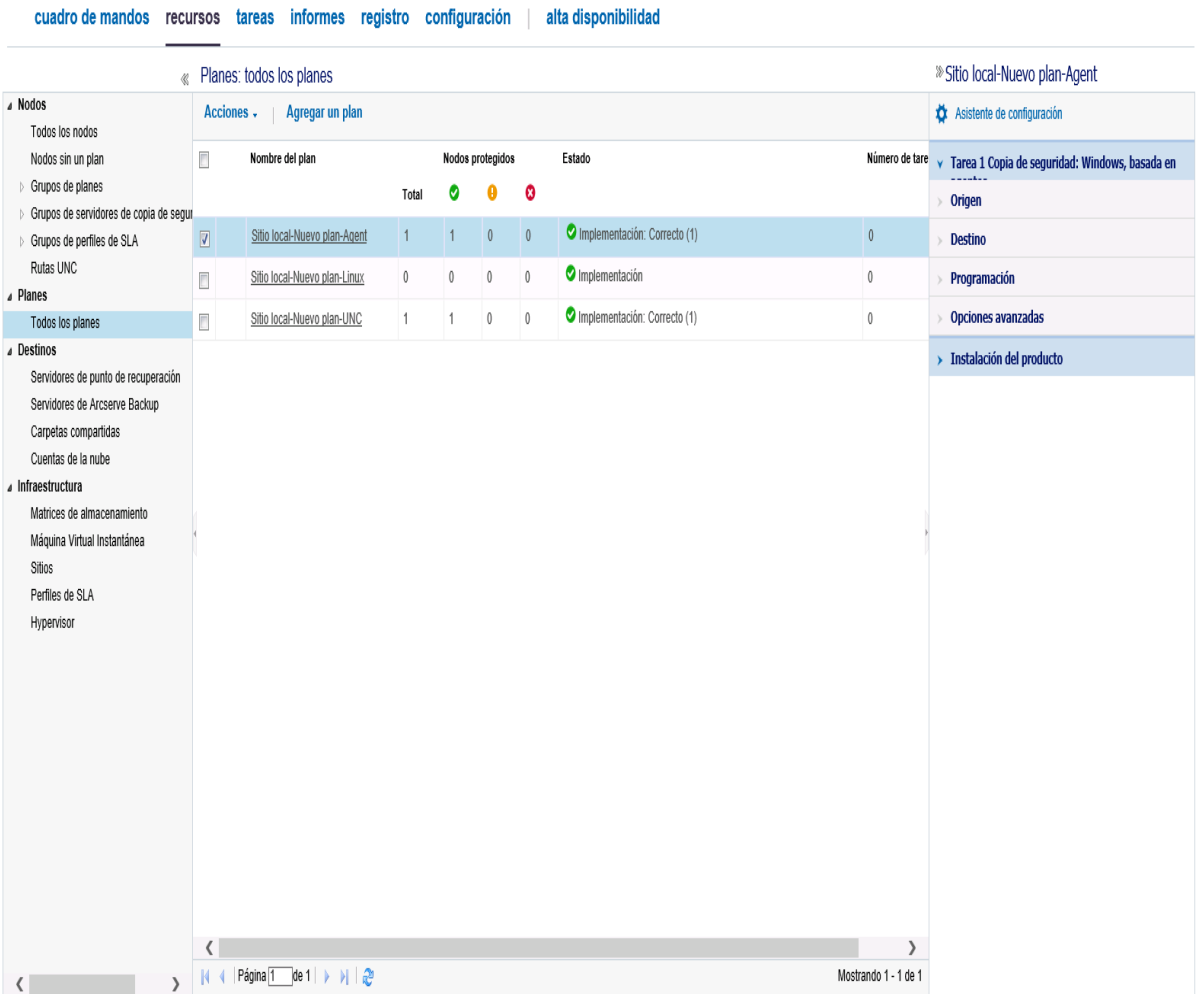
Gestión del destino

La vista de gestión del destino le permite gestionar los servidores de punto de recuperación de destino. Cuando se selecciona un servidor del panel central, sus eventos recientes se muestran en el panel derecho. Cuando se selecciona un almacén de datos, se muestra el estado y los valores de configuración en el panel derecho.



Gestión de planes

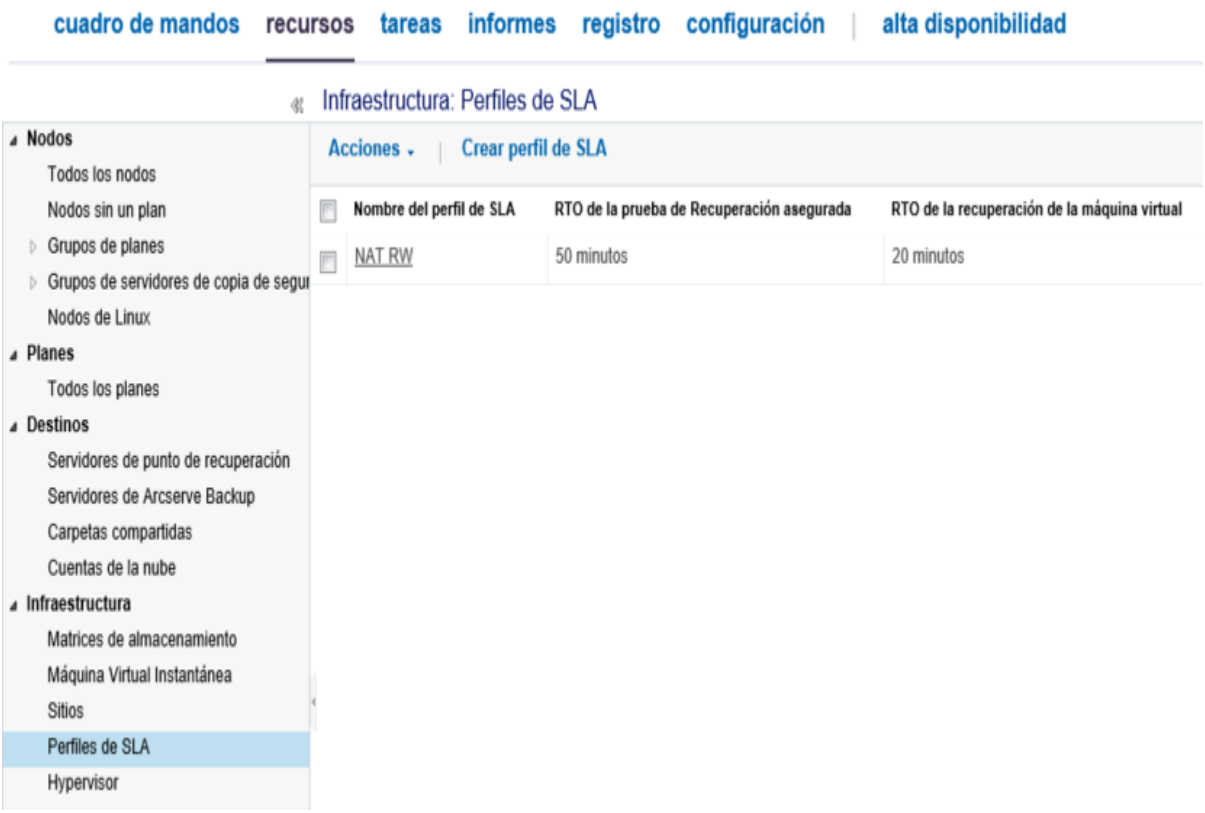
La vista de gestión de planes le permite gestionar todos los planes. Se pueden crear, modificar, suprimir, implementar, pausar y reanudar planes desde esta vista. Los detalles del plan aparecen en el panel derecho. Se puede hacer clic en los campos necesarios para ver los detalles y poder gestionarlos.



Gestión de la infraestructura

La vista de gestión de la infraestructura permite gestionar matrices de almacenamiento, máquinas virtuales instantáneas y sitios remotos.

La siguiente captura de pantalla destaca el panel de gestión de la infraestructura:



tareas

La ficha **tareas** muestra el estado de las tareas durante un período específico. Aplique filtros para clasificar los resultados o para agrupar las tareas por plan.

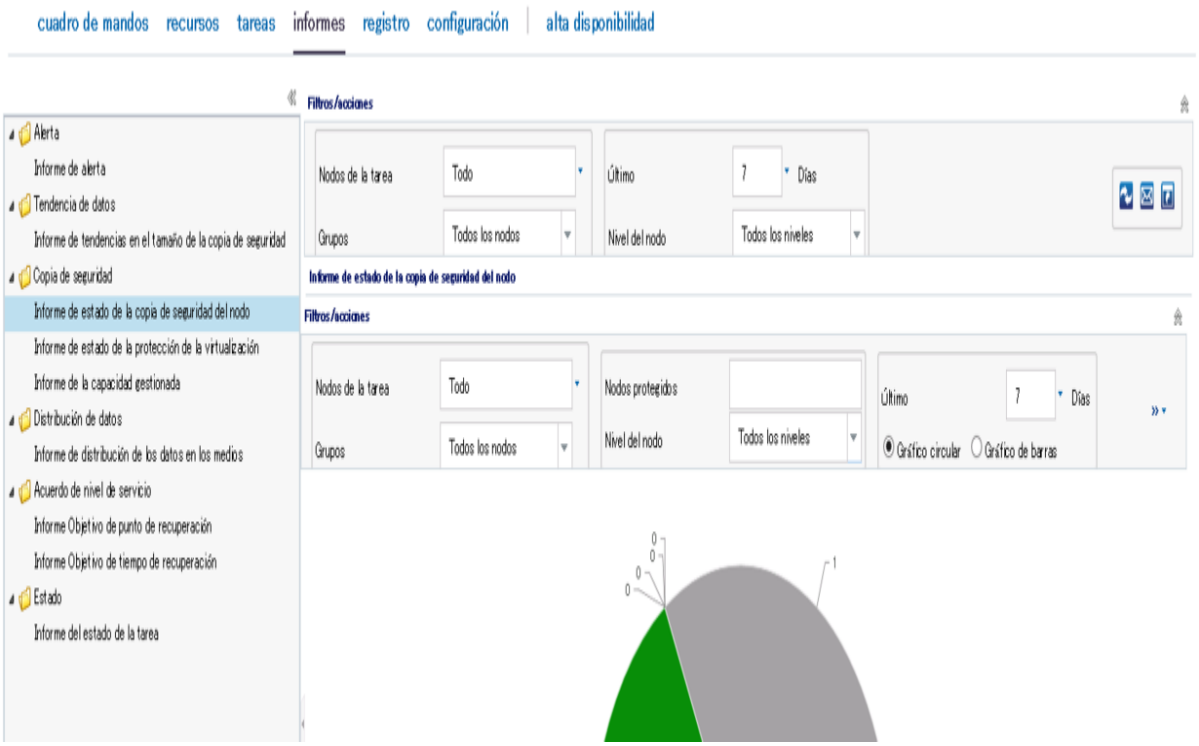


Cuando una tarea está en curso, el panel derecho muestra el controlador de tareas que contiene el progreso de la tarea. Haga clic en **Detalles de la tarea** en el panel derecho para abrir el controlador de tareas. Se puede ver que la tarea solo se monitoriza si la tarea está en curso.

Para cancelar una tarea, abra el controlador de tareas y haga clic en **Cancelar**.

informes

La ficha **Informes** muestra una lista de informes que se pueden generar. Se pueden aplicar filtros a los informes para obtener informes específicos. Los informes se generan en formatos CSV, PDF o HTML. Para obtener más información sobre estos informes, consulte Cómo generar Informes de Arcserve UDP.



registro

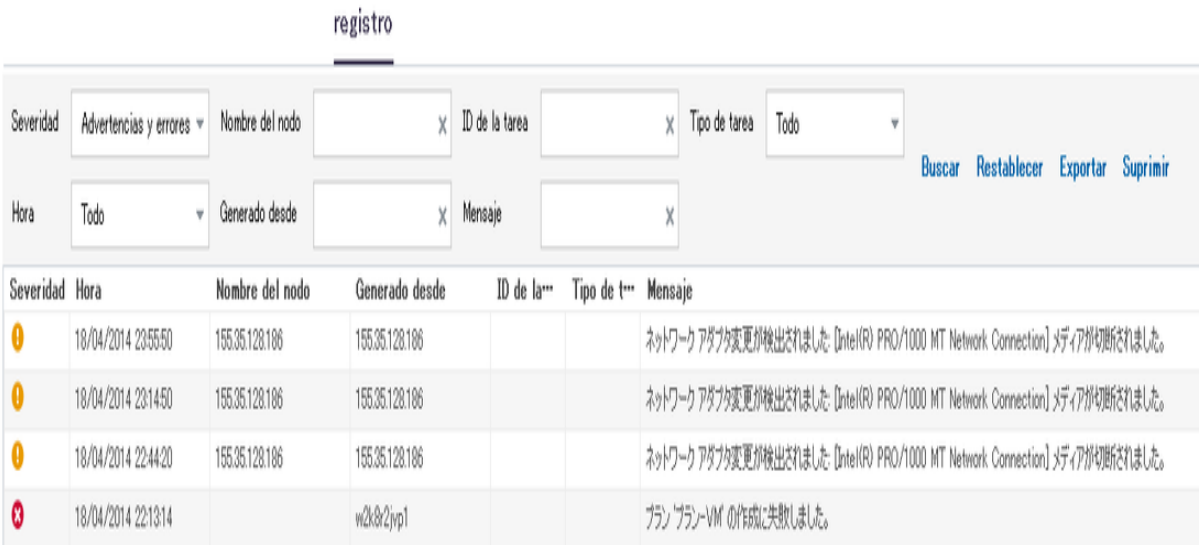
La ficha **registros** muestra todos los registros de actividades para los nodos protegidos, los servidores de destino, los almacenes de datos y los planes. Se pueden ver registros y aplicar diversos filtros como severidad, nodo específico, registros generados desde el equipo, los ID de tarea y el contenido de registro.

El ID de mensaje proporciona un hipervínculo para acceder a la documentación detallada. Haga clic en el hipervínculo de la columna del ID de mensaje para ver la descripción y una solución para ese mensaje.

Nota: Los registros de actividades generados por la Consola, el servidor de copia de seguridad de Linux, el Agente y la tarea de copia en cinta no tienen ID de mensaje.

Se pueden buscar los registros de actividades mediante una combinación de los filtros disponibles o mediante una de las opciones siguientes:

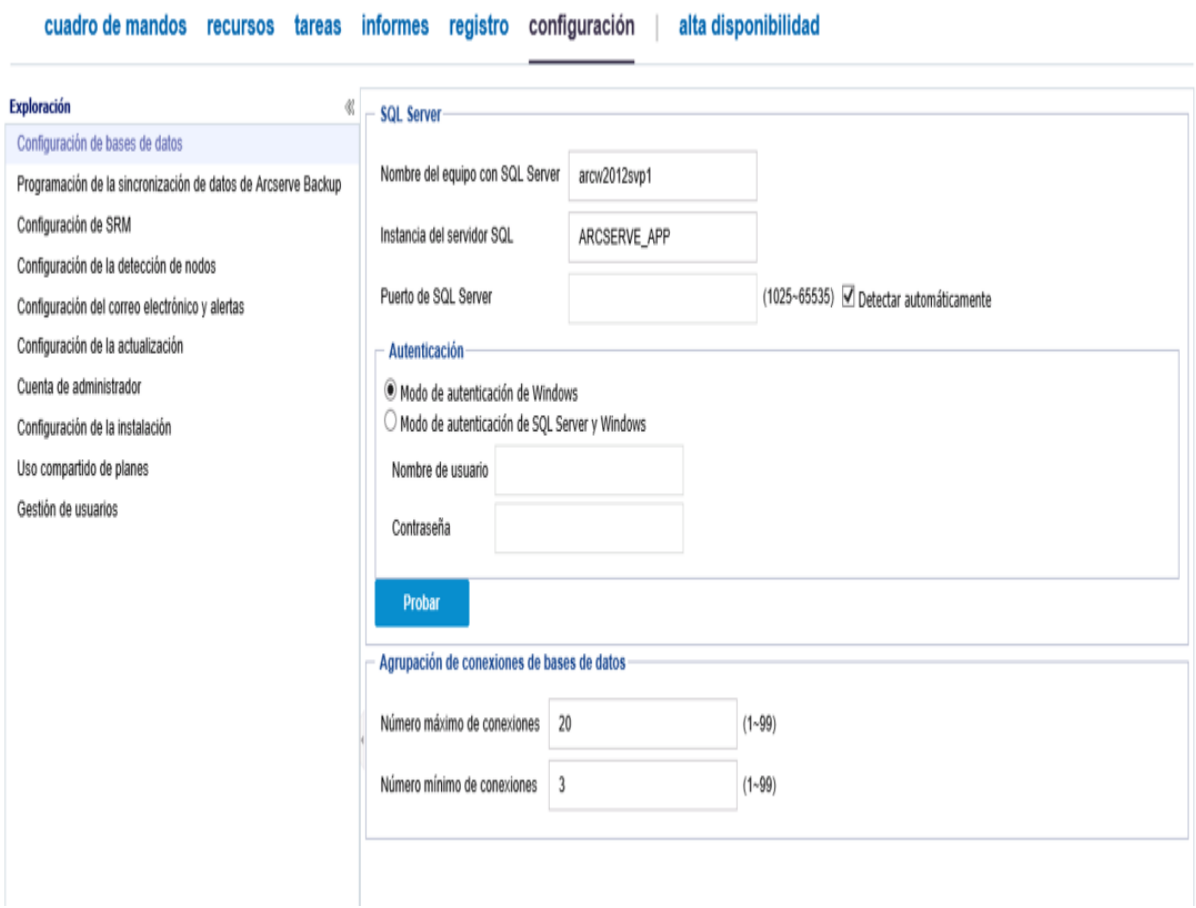
- Seleccione los tipos de severidad para ver todos los registros relacionados con el tipo seleccionado.
- Introduzca otros detalles (como el Nombre de nodo y el ID de tarea) y haga clic en **Búsqueda**.
- **Actualizar:** Muestra los registros más recientes disponibles según los filtros definidos.
- **Restablecer:** Solo utiliza los filtros predeterminados y solo muestra Advertencia y Error para todos los tipos de tareas.
- **Exportar:** Descarga el registro de la tarea actual como un archivo *.zip (es decir, activitylog_export_2017_10_12_15_02_27_586.zip) al directorio Descargas del sistema Windows.
- **Suprimir:** Elimina todos los registros o todos los registros anteriores a una fecha específica.


registro
Severidad
Advertencias y errores
Nombre del nodo
ID de la tarea
Tipo de tarea
Todo
Buscar
Restablecer
Exportar
Suprimir
Hora
Todo
Generado desde
Mensaje
Severidad
Hora
Nombre del nodo
Generado desde
ID de la...
Tipo de t...
Mensaje
18/04/2014 23:55:50
155.35.128.186
155.35.128.186
ネットワーク アダプタ変更が検出されました: [Intel(R) PRO/1000 MT Network Connection] メディアが切断されました。
18/04/2014 23:14:50
155.35.128.186
155.35.128.186
ネットワーク アダプタ変更が検出されました: [Intel(R) PRO/1000 MT Network Connection] メディアが切断されました。
18/04/2014 22:44:20
155.35.128.186
155.35.128.186
ネットワーク アダプタ変更が検出されました: [Intel(R) PRO/1000 MT Network Connection] メディアが切断されました。
18/04/2014 22:13:14
w2k8r2jvp1
プラン 'プラン-VM' の作成に失敗しました。

configuración

La ficha **configuración** le permite configurar ciertas preferencias como, por ejemplo, qué servidor de correo electrónico usar, configurar el ID de usuario de administrador y la contraseña, y definir la ruta de implementación de nodos predeterminada.

Para obtener más información sobre la ficha **configuración,** vea Cómo configurar Arcserve UDP.



High Availability

La ficha **High Availability** permite gestionar y controlar las funciones de Arcserve High Availability. En caso necesario, especifique las credenciales en el cuadro de diálogo **Agregar servicio de control** y consulte los detalles.

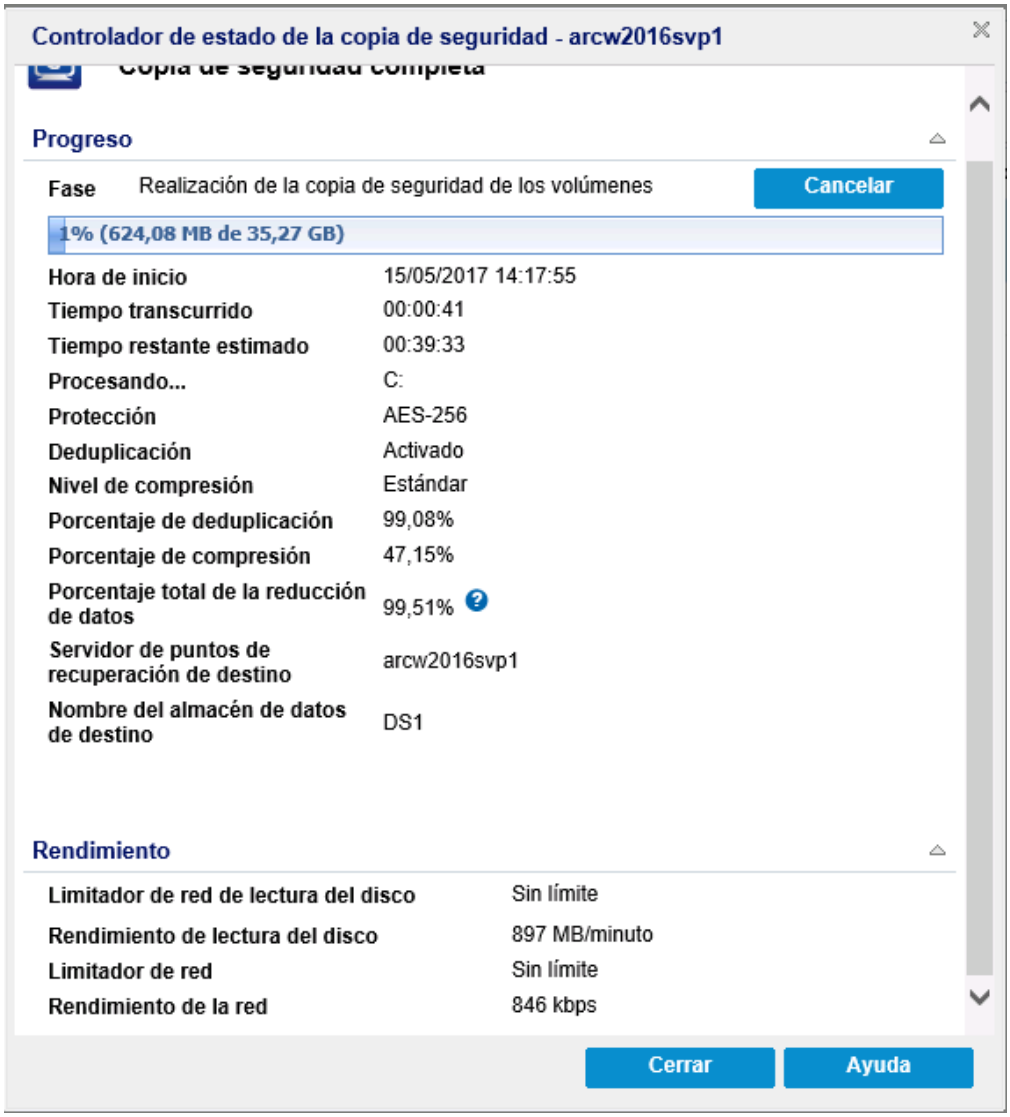


Cuadro de diálogo Controlador de tareas

El cuadro de diálogo Controlador de tareas le permite ver el estado de una tarea. Cuando se está ejecutando una tarea, este panel se expande y muestra información sobre el evento en curso, como por ejemplo el tiempo estimado que falta para completar la tarea, el porcentaje y tamaño de la tarea que ya se ha completado y el tamaño total de la tarea una vez completada.

Cuando se está ejecutando una tarea, en el panel derecho expanda **Eventos recientes** y haga clic en el botón **Detalles** para abrir los controladores del estado y mostrar información más detallada acerca de la tarea que se está ejecutando actualmente.

Haga clic en el botón **Cancelar** para detener la tarea actual.



Cómo configurar Arcserve UDP

Mediante Arcserve Unified Data Protection, se pueden especificar los siguientes valores de configuración de Arcserve Unified Data Protection.

- Protocolo de comunicaciones del servidor
- Configuración de la base de datos
- Sincronización de datos de Arcserve Backup
- Configuración SRM
- Configuración de la detección de nodos
- Configuración del correo electrónico y alertas
- Configuración del proxy
- Actualización de la configuración
- Cuenta del administrador
- Configuración de la implementación remota
- Compartir plan
- Gestión de usuarios
- Configuración de la duración del tiempo de espera de la Consola

Configuración del protocolo de comunicaciones del servidor

La solución Arcserve Unified Data Protection utiliza el Protocolo de transferencia de hipertexto (HTTP) para la comunicación entre todos los componentes. Si está preocupado por la seguridad de las contraseñas que se comunican entre los componentes, se puede cambiar el protocolo HTTP al Protocolo seguro de transferencia de hipertexto (HTTPS). Cuando no necesite este nivel extra de seguridad, puede cambiar el protocolo a HTTP.

Nota: Cuando se cambie el protocolo a HTTPS, se muestra una advertencia en el explorador web. La advertencia aparece a causa de un certificado de seguridad autofirmado en el que se indica que se puede ignorar la advertencia y continuar o bien agregar ese certificado al explorador para evitar que esta advertencia se muestre en el futuro.

Siga estos pasos:

1. Inicie sesión en el equipo donde está instalada la Consola de Arcserve Unified Data Protection mediante una cuenta administrativa o una cuenta con privilegios administrativos.

   Nota: Si no inicia sesión mediante una cuenta administrativa o una cuenta con privilegios administrativos, configure la línea de comandos para que se ejecute usando el privilegio Ejecutar como administrador.
2. Abra la línea de comandos de Windows.
3. Realice una de las tareas siguientes:
   - Para cambiar el protocolo de HTTP a HTTPS:

     Inicie la herramienta de utilidad changeToHttps.bat desde la ubicación predeterminada siguiente.

     Nota: La ubicación de la carpeta BIN puede variar dependiendo de donde se haya instalado la Consola de Arcserve Unified Data Protection.

     C:\Archivos de programa\Arcserve\Unified Data Protection\Management\BIN

     Cuando se haya cambiado el protocolo correctamente, aparecerá el siguiente mensaje:

     El protocolo de comunicación se ha cambiado a HTTPS.
   - Para cambiar el protocolo de HTTPS a HTTP:

     Inicie la herramienta de utilidad changeToHttp.bat desde la ubicación predeterminada siguiente

Nota: La ubicación de la carpeta BIN puede variar dependiendo de donde se haya instalado la Consola de Arcserve Unified Data Protection.

C:\Archivos de programa\Arcserve\Unified Data Protection\Management\BIN

Cuando se haya cambiado el protocolo correctamente, aparecerá el siguiente mensaje:

El protocolo de comunicación se ha cambiado a HTTP.

4. Reinicie el explorador y vuelva a conectarse a la Consola de Arcserve Unified Data Protection.

   Nota: Para actualizar el protocolo de comunicación utilizado por el servidor de puntos de recuperación de Arcserve Unified Data Protection y el Agente de Arcserve Unified Data Protection para comunicarse con la Consola de Arcserve Unified Data Protection, se debe actualizar el nodo directamente desde la Consola.

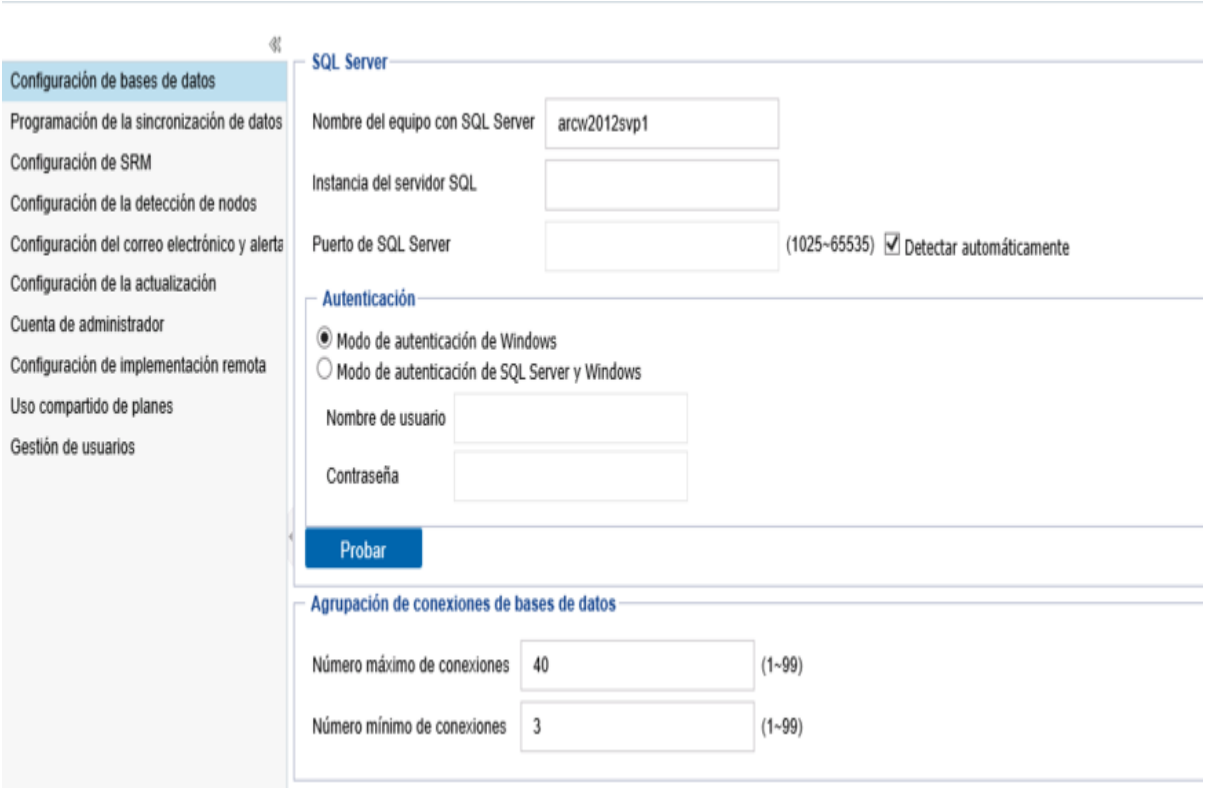
Configuración de bases de datos

La página **Configuración de bases de datos** le permite introducir detalles sobre la base de datos. La configuración de la base de datos requiere detalles sobre SQL Server, el número de conexiones y el modo de autenticación.

Nota: Se puede volver a crear la base de datos antes de configurarla. Suprima la base de datos de Arcserve Unified Data Protection mediante el procedimiento descrito en Como volver a crear la base de datos de Arcserve Unified Data Protection y, a continuación, configure la base de datos.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **configuración**.
2. En el panel izquierdo, haga clic en **Configuración de bases de datos**.



Para llevar a cabo la configuración, rellene los campos siguientes en el panel de configuración y haga clic en **Guardar**.

Nombre del equipo de SQL Server

Especifica el nombre del servidor que hospeda la instancia de SQL Server.

Instancia de SQL Server

Especifica el nombre de la instancia de SQL Server.

Puerto de SQL Server

Especifica el número de puerto para esta instancia o active la opción **Detección automática.** El intervalo de opciones para el número de puerto va del 1025 al 65535.

Detección automática

Al seleccionar la casilla de verificación se permite que la aplicación encuentre el número de puerto.

Autentificación

Seleccione uno de los modos de autenticación de las opciones siguientes:

Modo de autenticación de Windows: Modo predeterminado:

(Opcional) **Probar**: Haga clic en Probar para verificar que la aplicación puede comunicar con la instancia de Microsoft SQL Server.

SQL Server y modo de autenticación de Windows:

Seleccione la opción e introduzca los detalles en el nombre de usuario y la contraseña.

Valores de la agrupación de conexiones de bases de datos

Para el número máximo y mínimo de conexiones, introduzca un valor del 1 al 99.

Se establece la configuración del servidor de base de datos.

Haga clic en **Restablecer** para borrar todos los valores especificados y cargar los datos originales.

Recreación de la base de datos de Arcserve Unified Data Protection

Es posible que se deba volver a crear la base de datos de Arcserve Unified Data Protection por motivos diversos. Por ejemplo, puede que la base de datos actual consuma más de 10 GB de datos. Para volver a crear la base de datos, primero se debe suprimir la base de datos de Arcserve Unified Data Protection existente y, a continuación, configurar una nueva base de datos para sustituir la base de datos suprimida. El procedimiento sirve tanto para bases de datos de Microsoft SQL Server como de Microsoft SQL Server Express Edition.

Importante: Al suprimir la base de datos de Arcserve Unified Data Protection, se pierden todos los datos actuales.

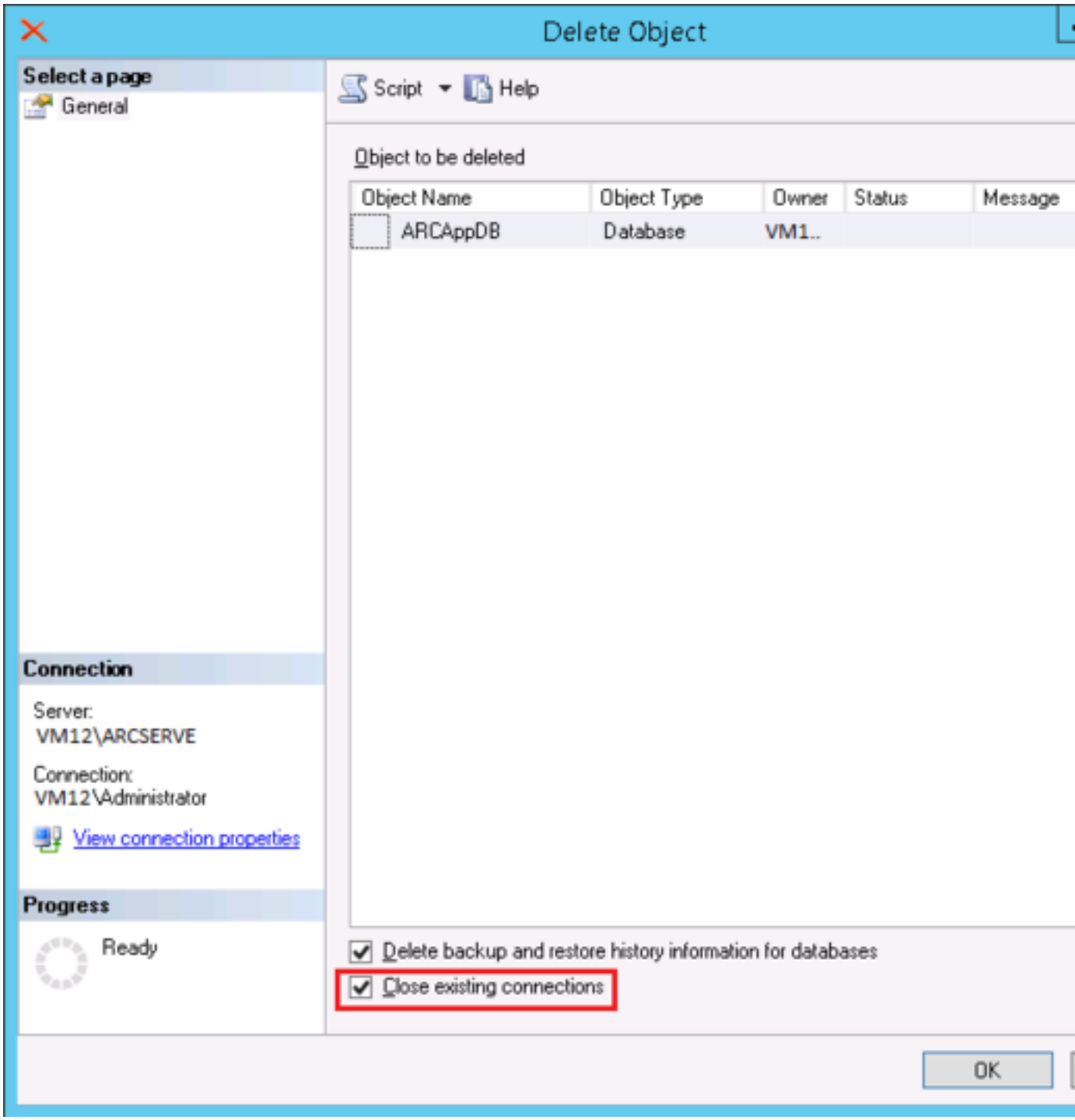
Para volver a crear la base de datos de Arcserve Unified Data Protection

1. Abra Microsoft SQL Server Management Studio Express e inicie sesión en la instancia ARCSERVE_APP.

   Nota: Si Microsoft SQL Server Management Studio Express no está instalado en el servidor de Arcserve Unified Data Protection, es posible descargar la utilidad del Centro de descarga de Microsoft.

2. Haga clic con el botón secundario del ratón en arcserveUDP y haga clic en **Suprimir** en el cuadro de diálogo emergente.

   Se abrirá el cuadro de diálogo **Eliminar objeto**.



3. En el cuadro de diálogo **Eliminar objeto**, haga clic en la opción **Cerrar conexiones existentes** y haga clic en **Aceptar**.

   La base de datos de Arcserve Unified Data Protection existente se ha suprimido.

4. Configure la nueva base de datos. Para obtener más información, consulte Configuración de base de datos.

   La solución Arcserve Unified Data Protection vuelve a crear la base de datos. El nombre de la instancia de la base de datos es **ARCSERVE_APP**.

Configuración de la sincronización de datos de copia de seguridad de Arcserve

Se puede configurar la **Programación de la sincronización de datos deArcserve Backup** .

Siga estos pasos:

1. En la Consola, haga clic en la ficha **configuración**.
2. En el panel de la izquierda, haga clic en **Programación de la sincronización de datos de Arcserve Backup**.
3. En el panel de la derecha, haga clic en **Activar**.

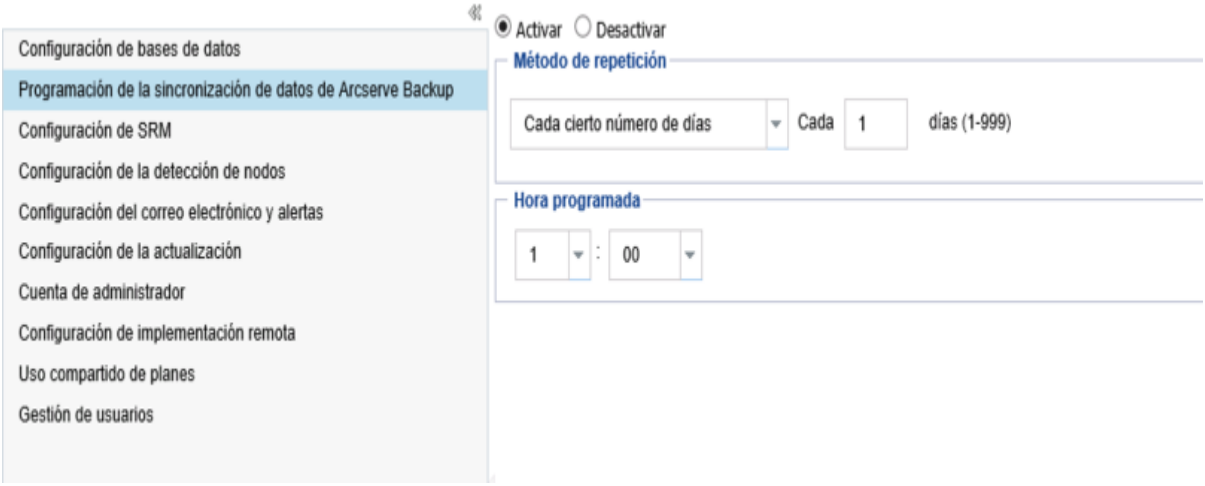
   De forma predeterminada, se activa configuración de **Sincronización de datos de Arcserve Backup**.

   Nota: Al hacer clic en **Desactivar** se detiene la programación.
4. Especifique los parámetros siguientes para programar la sincronización de datos de Arcserve Backup:
   - **Método de repetición**
   - **Hora programada**
5. Haga clic en **Guardar**.

   Se aplicará la programación para la sincronización de datos de Arcserve Backup.

   Nota: No haga clic en **Guardar** si se desea ejecutar la sincronización inmediatamente.
6. (Opcional) Para ejecutar el proceso inmediatamente, haga clic en **Ejecutar ahora**.

   El cuadro de diálogo **Nodo** se muestra con la lista de nodos disponibles para la sincronización.



7. Seleccione los nodos que se desea ejecutar para la sincronización y haga clic en **Aceptar**.

Configuración de SRM

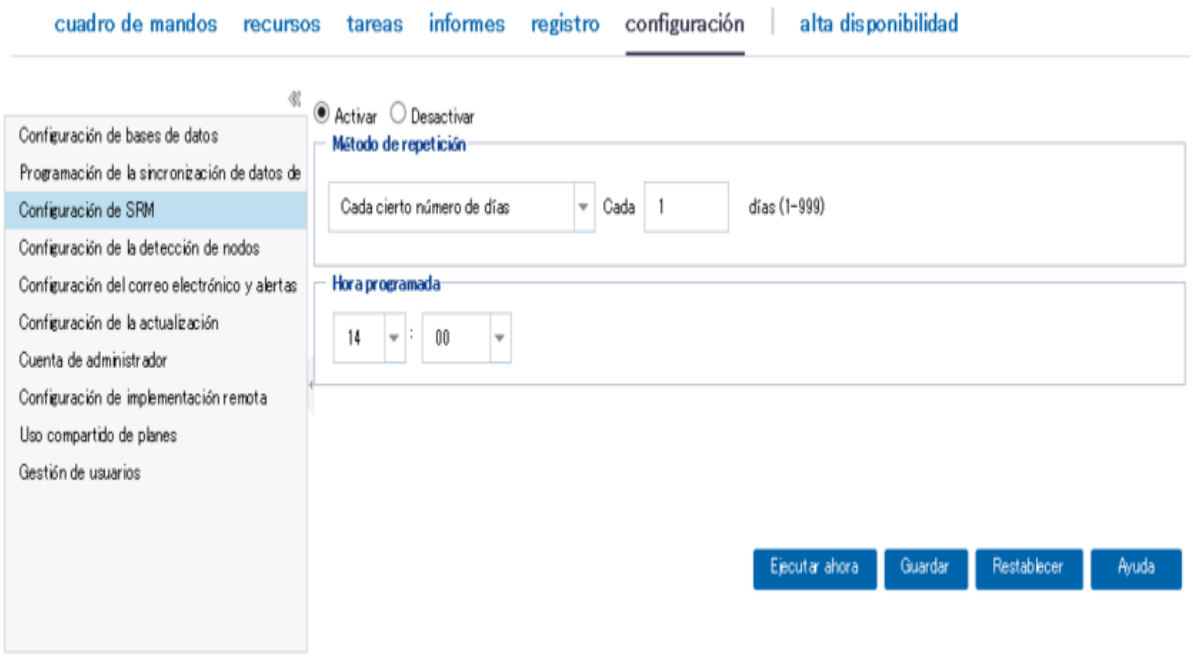
La página Configuración de SRM le permite configurar una programación de SRM para los nodos que defina cuándo y con qué frecuencia se deben recopilar datos de SRM. SRM (Gestión de los recursos de almacenamiento) es una funcionalidad que recopila información sobre los siguientes datos:

- Hardware, software y datos de la aplicación para las implementaciones de Microsoft SQL Server y Microsoft Exchange Server.
- Datos de los Indicadores clave del rendimiento (PKI) desde nodos.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **configuración**.
2. En el panel izquierdo, haga clic en **Configuración del usuario de SRM**.
3. En el panel de la derecha, haga clic en **Activar**.

   De forma predeterminada, la **Configuración de SRM** está activada.



   Nota: Al hacer clic en **Desactivar** se detiene la programación.

4. Especifique los parámetros siguientes para programar SRM:
   - **Método de repetición**
   - **Hora programada**
5. Haga clic en **Guardar**.

   Se aplica la programación para SRM.

Nota: No haga clic en **Guardar** si se desea recopilar los datos de SRM inmediatamente.

6. (Opcional) Para ejecutar el proceso inmediatamente, haga clic en **Ejecutar ahora**.

   El cuadro de diálogo **Nodo** se muestra con la lista de nodos disponibles para la sincronización.



	Nombre del nodo	Aplicaciones	Productos	Sistema operativo
	155.35.128.72			Windows Server 2008 R2 Enterprise
	g11n-senhi05-v8			Windows Server 2008 R2 Enterprise
	g11n-senhi06-v1			Windows 7 Enterprise
	W2012Jhv1			Windows Server 2012 Standard
	W7Ux64Jvp1			Windows 7 Ultimate

7. Seleccione los nodos que se desea ejecutar para la sincronización y haga clic en **Aceptar**.

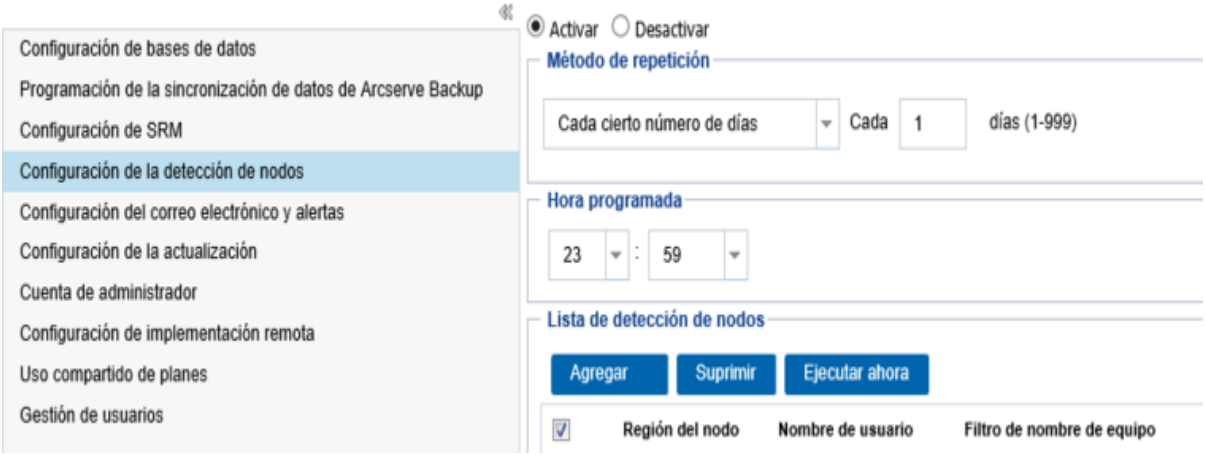
Configuración de la detección de nodos

La página **Configuración de la detección de nodos** permite configurar la programación de detección de nodos de Active Directory, VMware vSphere y Microsoft Hyper-V varias veces y en un tiempo programado. Cuando se detectan nuevos nodos, se envía una alerta de correo electrónico al administrador para que pueda agregar manualmente los nodos nuevos. De forma predeterminada, la opción **Configuración de la detección** está desactivada.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **configuración**.
2. En el panel de la izquierda, seleccione **Configuración de la detección de nodos**.

   Para activar la configuración, haga clic en la opción **Activar** a fin de especificar el tipo de método de repetición que desea y establecer una hora programada para el inicio de la detección de nodos.



Se pueden especificar los siguientes parámetros para configurar la programación de detección:

- **Cada cierto número de días:** permite repetir este método después del número de días especificado. (Valor predeterminado)
- **Cada día seleccionado de la semana:** permite repetir este método los días especificados. De forma predeterminada, los días de la semana son lunes, martes, miércoles, jueves y viernes.
- **Cada día seleccionado del mes:** permite repetir este método el día de mes especificado. 1 es la opción predeterminada para el día del mes.
- **Tiempo programado:** permite especificar cuando se va a ejecutar la detección según la programación de repetición.

- **Lista de detección de nodos>Agregar:** seleccione desde dónde desea agregar los nodos. A continuación, especifique las credenciales según sea necesario.

  Nota: Opcionalmente, haga clic en **Ejecutar ahora** para ejecutar la detección de manera instantánea.

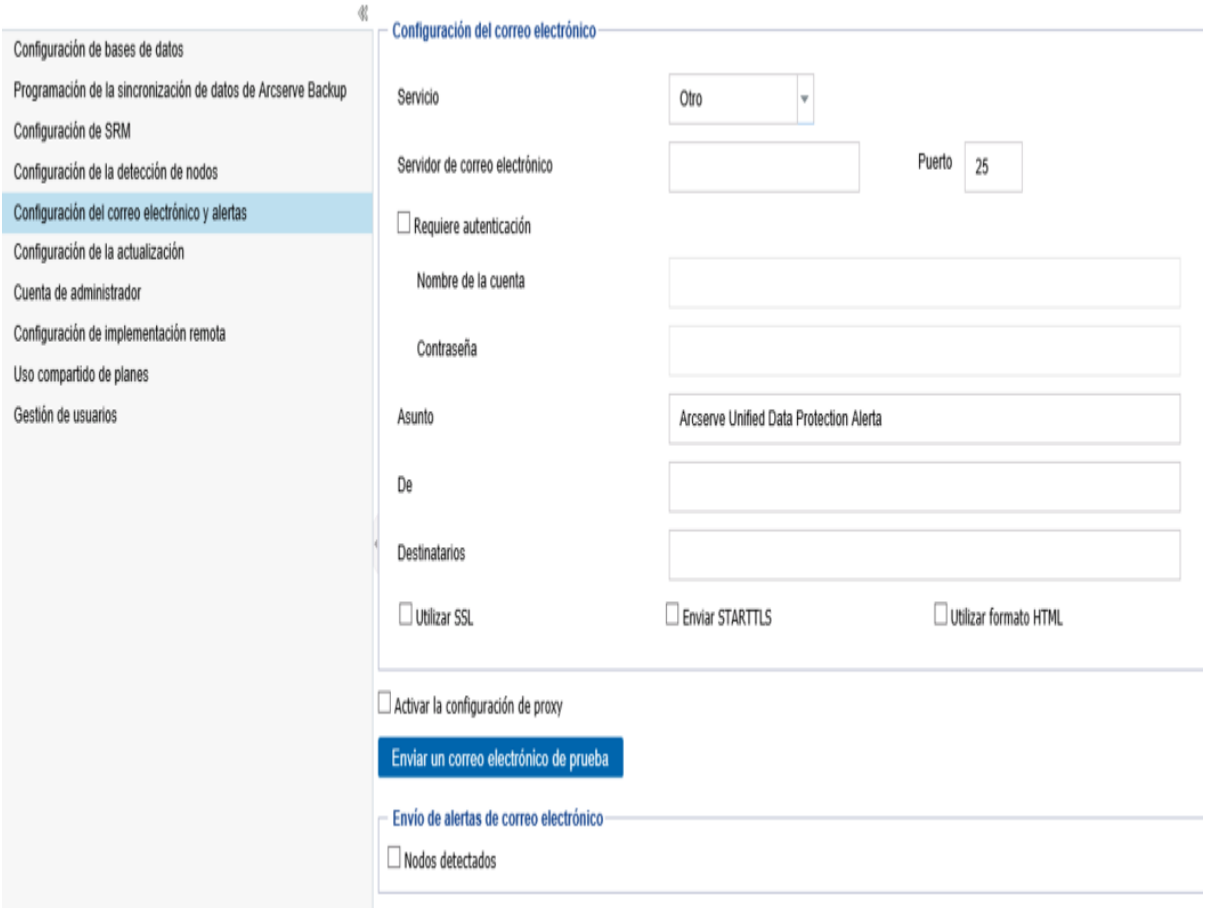
Configuración del correo electrónico y alertas

La página **Configuración del correo electrónico y alertas** le permite proporcionar la configuración del correo electrónico y la configuración de alertas del correo electrónico.

Nota: Como requisito previo, instale Microsoft .NET Framework (versión 2.0 o posterior) en el equipo en el que se ha instalado la Consola para que la función de exportación de los gráficos de informe pueda exportar las imágenes a un informe correctamente.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **configuración**.
2. En el panel de la izquierda, haga clic en **Configuración del correo electrónico y alertas**.
3. Introduzca detalles para establecer los valores de configuración predeterminados.



Servicio

Seleccione los servicios de correo electrónico de las opciones disponibles.

Servidor de correo electrónico

Especifique el nombre de host del servidor de correo de SMTP que se puede utilizar para enviar alertas de correo electrónico.

Puerto

Especifique el número de puerto relacionado con el servidor de correo electrónico.

Requiere autenticación

Seleccione la casilla de verificación para introducir las credenciales.

Utilizar SSL/Enviar STARTTLS/Utilizar formato HTML

Seleccione la opción deseada para especificar los requisitos.

Activar la configuración de proxy

Seleccione la casilla de verificación para introducir los detalles del **Servidor proxy** y de la autenticación.

Correo electrónico de prueba

Haga clic para verificar los detalles que se han introducido en la sección Configuración del correo electrónico.

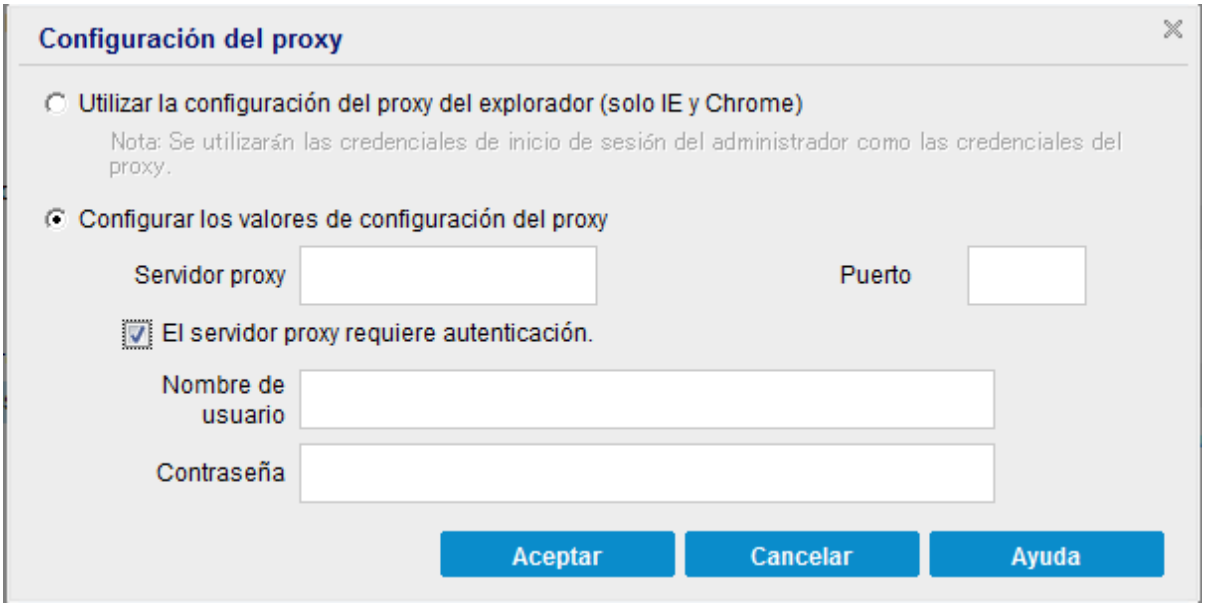
Enviar alertas de correo electrónico

Seleccione **Nodos detectados** para configurar nodos de **Active Directory** que se pueden encontrar utilizando la función Detectar disponible para los nodos en la ficha **recursos**.

Configuración del proxy

Seleccione **Configuración del proxy** para indicar si desea que Arcserve UDP se comunique mediante el servidor proxy. Un servidor proxy actúa como intermediario entre su servidor y el servidor de Arcserve para garantizar la seguridad, mejorar el rendimiento y tener el controla administrativo. Funciona como la conexión al servidor de Arcserve desde el que el servidor de descargas obtiene las actualizaciones.

Cuando se selecciona el servidor de Arcserve como servidor de descarga, se abre el cuadro de diálogo **Configuración del proxy**.



- **Utilizar la configuración de proxy del explorador**

  Esta selección es solamente aplicable a Windows Internet Explorer (IE) y Google Chrome.

  Cuando se selecciona, se indica a Arcserve UDP que detecte y utilice automáticamente los mismos valores de configuración del proxy que se aplican al explorador para conectarse al servidor de Arcserve para obtener la información de actualización de Arcserve UDP.

- **Configuración del proxy**

  Cuando se selecciona, permite al servidor proxy especificado conectarse al servidor de Arcserve para obtener la información de actualización de Arcserve UDP. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet.

Además, se puede especificar también si su servidor proxy requiere autenticación. Si se selecciona, especifica que la información de autenticación es necesaria (ID de usuario y contraseña) para utilizar el servidor proxy.

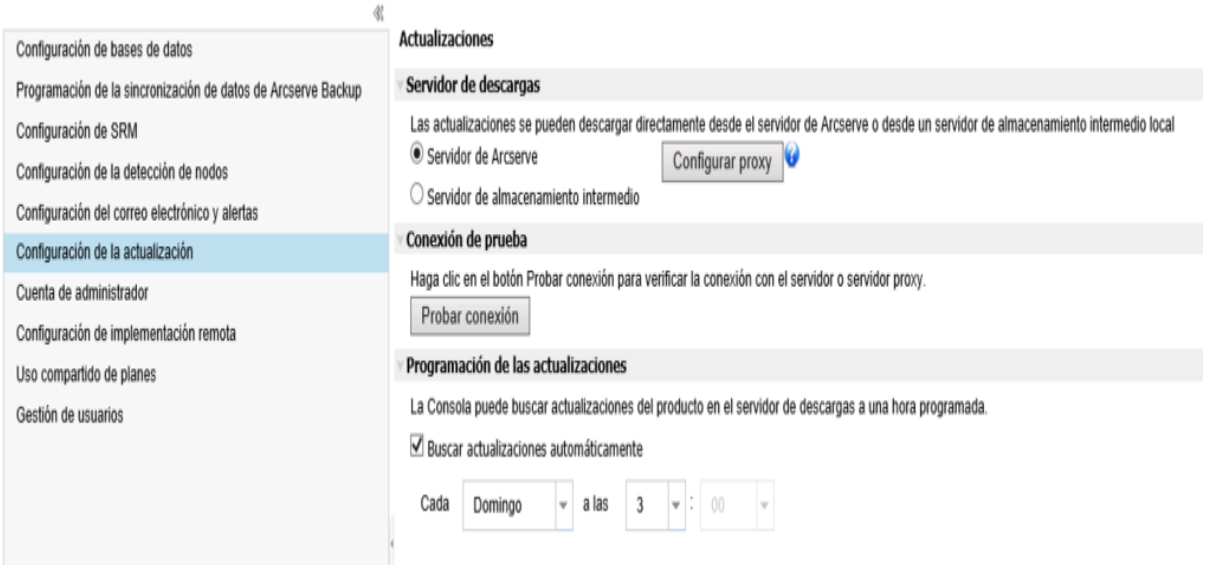
Nota: El formato para el nombre de usuario debe ser un nombre de usuario del dominio completamente calificado con la forma <nombre del dominio>\<nombre de usuario>.

Actualización de la configuración

La página Actualización de la configuración le permite establecer el servidor de descargas y la programación de la actualización para configurar actualizaciones. Se pueden proporcionar detalles sobre los valores de configuración de proxy del servidor de Arcserve o del servidor de almacenamiento intermedio para la opción Servidor de descargas.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **configuración**.
2. En el panel de la izquierda, haga clic en **Actualizar configuración**.



Proporcione los detalles sobre el tipo de Servidor de actualización y Programación de actualización. El servidor de actualización es el servidor de Arcserve o el servidor de almacenamiento intermedio.

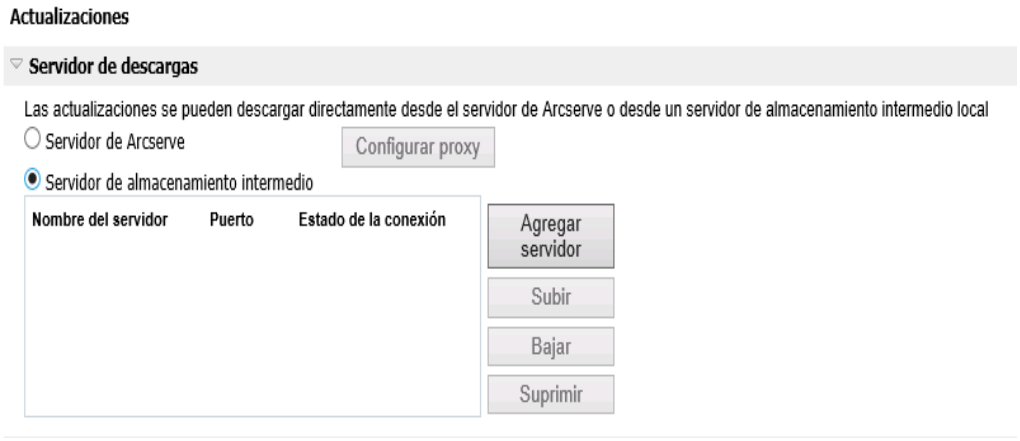
3. Para el **Servidor de descarga**, seleccione una de las opciones siguientes:
   - Para el **servidor de Arcserve**, haga clic en **Configuración proxy** para completar la configuración del proxy.
   - Para **Servidor de almacenamiento intermedio**, haga clic en **Agregar servidor** para proporcionar detalles del servidor de almacenamiento intermedio.

     Para crear un servidor de almacenamiento intermedio, consulte Cómo crear un servidor de almacenamiento intermedio.

     Si el servidor de almacenamiento está detrás de un cortafuegos, prepare un equipo que pueda acceder a Internet, tenga instalado el producto UDP y

obtenga las últimas actualizaciones del servidor de Arcserve. A continuación, copie las carpetas **EngineUpdates** y **FullUpdates** desde la ubicación siguiente al equipo del servidor de almacenamiento intermedio:

<ruta de instalación de UDP>\ Arcserve\Unified Data Protection\Update Manager



Notas:

- Como la función de actualización automática no necesita una licencia, no es necesario activar la licencia en el servidor de almacenamiento intermedio.
- Para obtener más información sobre los puertos, consulte Puertos de comunicación usados por Arcserve UDP.

Se pueden agregar varios servidores de almacenamiento intermedio.

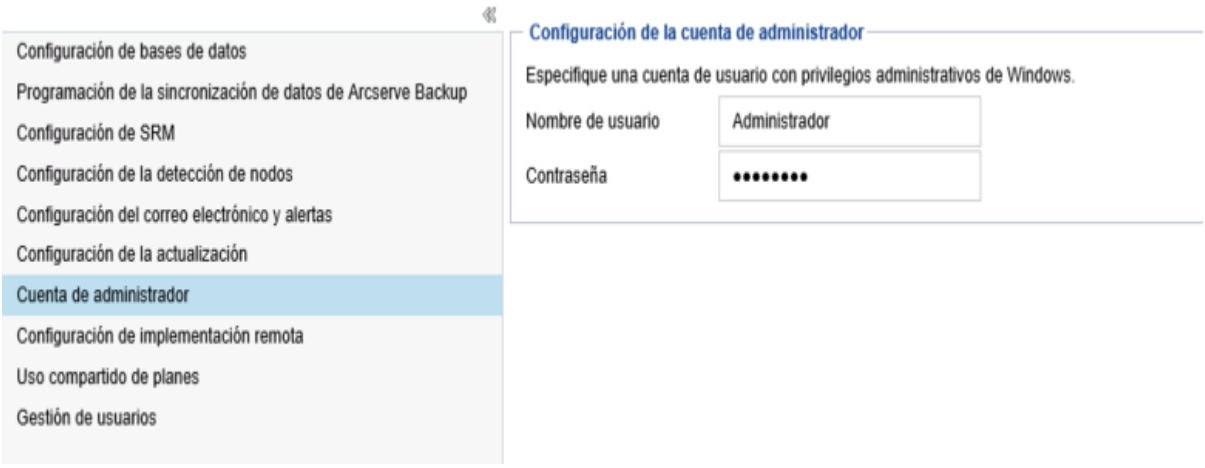
4. Haga clic en **Conexión de prueba** para verificar los detalles del **Servidor de descargas**.
5. Introduzca detalles para la **Programación de la actualización**.
6. Seleccione **Buscar actualizaciones automáticamente**.
7. Haga clic en **Guardar** para completar la actualización.

Configuración de la cuenta del administrador

La página **Cuenta del administrador** le permite crear una cuenta de usuario proporcionando un **nombre del usuario** y una **contraseña**.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **configuración**.
2. En el panel de la izquierda, haga clic en **Cuenta del administrador**.



3. Proporcione las credenciales de la cuenta de administrador y haga clic en **Guardar**.

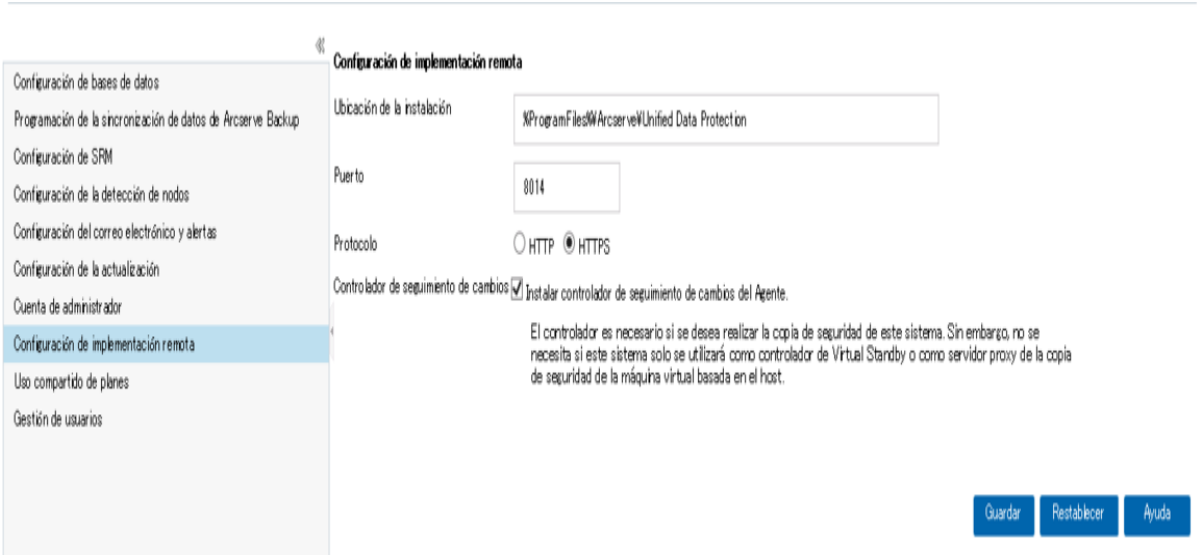
Configuración de la implementación remota

La página **Configuración de implementación remota** permite especificar valores de configuración predeterminados para instalar el Agente de Arcserve Unified Data Protection y el Servidor de puntos de recuperación de Arcserve Unified Data Protection. Especifique los valores de configuración predeterminados de la instalación para proporcionar la ubicación de la instalación.

Introduzca los detalles para la **ruta de instalación**, el **protocolo** y el **puerto**, y haga clic en **Guardar**.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **configuración**.
2. En el panel izquierdo, haga clic en **Configuración de implementación remota**.



3. Introduzca detalles como sea necesario y haga clic en **Guardar**.

Asignación del plan a la cuenta de usuario

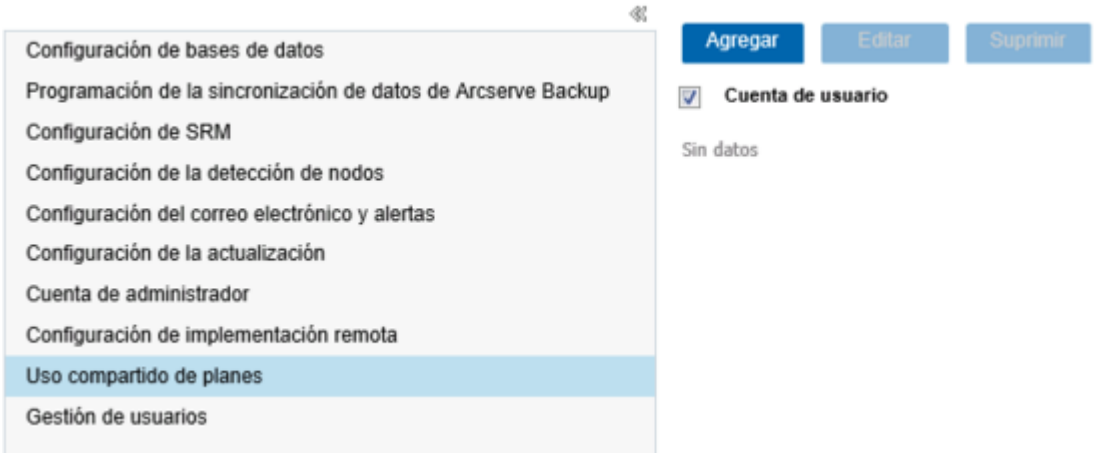
Administrador de destino

Ya se ha creado una cuenta de usuario y un plan para una consola de origen. Para identificar y gestionar datos replicados, debe asignarse el plan a la cuenta de usuario.

Nota: Se puede asignar más de un plan a una cuenta de usuario, pero dos cuentas diferentes no pueden compartir un plan. Sin embargo, se recomienda asignar un solo plan a una cuenta de usuario para que se puedan identificar y gestionar los datos replicados fácilmente.

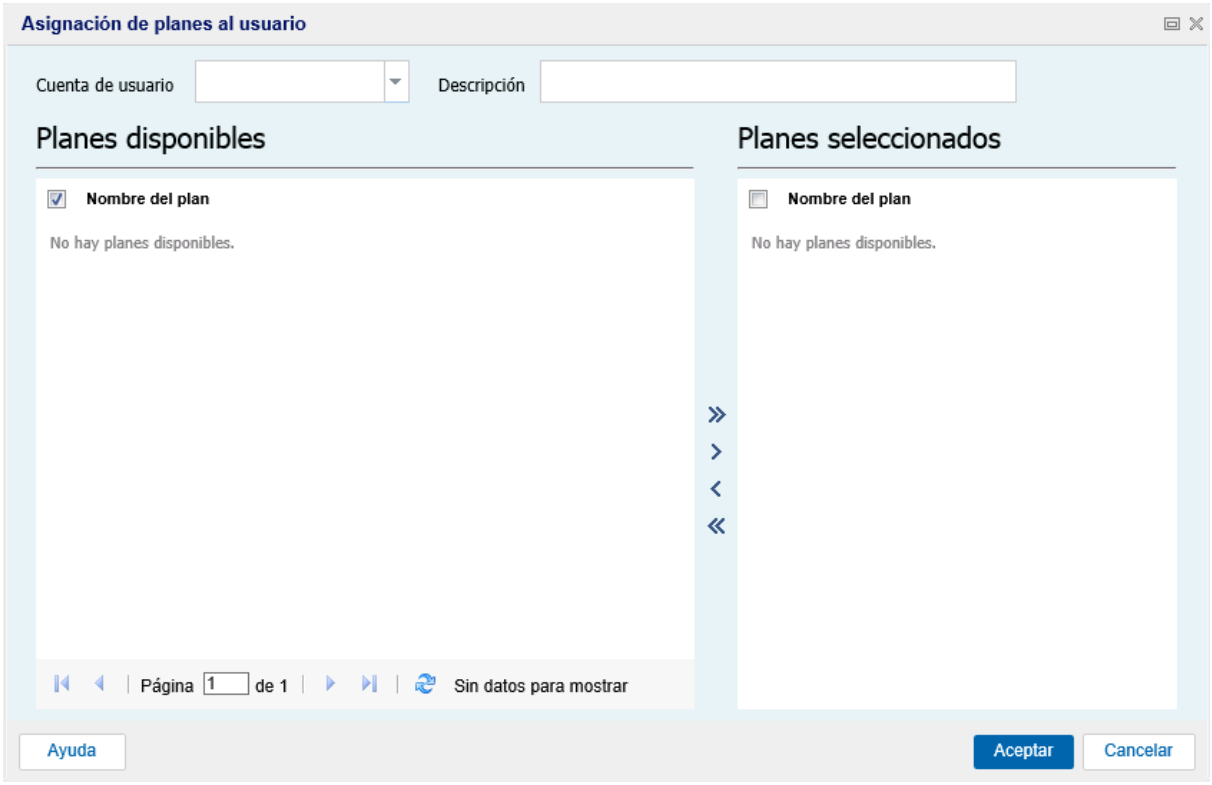
Siga estos pasos:

1. En la Consola, haga clic en la ficha **configuración**.
2. En el panel izquierdo, haga clic en **Compartir plan**.



3. En el panel central, haga clic en **Agregar**.

   Se abre el cuadro de diálogo **Asignar plan al usuario**.



4. Seleccione la **Cuenta de usuario**.
5. Seleccione un plan en la columna **Planes disponibles**.

   Nota: Si un plan ya se ha agregado a un nombre de usuario, ese plan no se muestra en la columna **Planes disponibles**.
6. Haga clic en **Agregar todos los planes** o en **Agregar planes seleccionados** para agregar los planes de la columna **Planes seleccionados**.
7. Haga clic en **Aceptar**.

   Se cierra el cuadro de diálogo **Asignar plan al usuario.** El nombre de usuario y los planes asociados se muestran en la página **Compartir plan**.

   La cuenta de usuario se asigna al plan creado para la consola de origen.

   Se puede utilizar **Editar** para modificar la configuración del usuario o **Suprimir** para eliminar la cuenta de usuario de la lista.

Gestión de usuarios

La página Gestión de usuarios le permite hacer lo siguiente:

- Iniciar sesión en la Consola de gestión de usuarios (Consola del servicio de identidad) desde la Consola de Arcserve UDP. Para obtener más información, consulte Inicio de la Consola de gestión de usuarios de Arcserve UDP.
- Activar y configurar la autenticación multifactor (MFA) para todos los usuarios. Para obtener más información, consulte Configuración de la autenticación multifactor.

Configuración de la duración del tiempo de espera de la Consola

Si la Consola está inactiva durante un tiempo determinado, se cierra automáticamente la sesión de la Consola. Se puede cambiar el valor del tiempo de espera predeterminado en el archivo ConsoleConfiguration.xml.

Siga estos pasos:

1. Inicie sesión en el equipo en el que haya instalado la Consola.
2. Abra el archivo ConsoleConfiguration.xml de la siguiente ubicación:

   <Directorio_principal_UDP>\Management\Configuration\ConsoleConfiguration.xml
3. Cambie el valor de consolaUISessionTimeout.

   El valor está en segundos.

   Por ejemplo:

   <consoleUISessionTimeout> 3600 </consoleUISessionTimeout> (el valor predeterminado es 1 hora, el valor está en segundos)

   El número 3600 indica que la duración del tiempo de espera para la Consola es de 3600 segundos.
4. Guarde el archivo ConsoleConfiguration.xml.

Cómo migrar los puntos de recuperación de Arcserve r16.5 a Arcserve UDP

Importante: Si va a replicar desde una carpeta compartida a un almacén de datos seleccionado en el servidor de puntos de recuperación, consulte Cómo realizar una replicación de datos sin conexión mediante el servidor de puntos de recuperación JumpStart.

Para migrar los puntos de recuperación de Arcserve r16.5 a Arcserve UDP, realice los pasos siguientes:

1. Creación de un almacén de datos para replicar los datos de Arcserve r16.5
2. Replicación de los datos de Arcserve r16.5 al almacén de datos de UDP

Creación de un almacén de datos para replicar los datos de un punto de recuperación de Arcserve r16.5

Para replicar los datos de un punto de recuperación existente de Arcserve D2D r16.5 , primero se debe crear un almacén de datos de la Consola donde se replicarán los datos.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Vaya a **Destinos**, **Servidor de punto de recuperación**.
3. Seleccione el servidor de punto de recuperación.
4. Haga clic con el botón secundario del ratón y seleccione **Agregar un almacén de datos**.
5. Introduzca los detalles en la página **Adición de almacenes de datos**.
6. Guarde el almacén de datos.

   El almacén de datos se crea.

Replicación de los datos de Arcserve r16.5 al almacén de datos de UDP

Después de crear el almacén de datos, se pueden replicar los datos del punto de recuperación de Arcserve r16.5 el servidor de puntos de recuperación JumpStart.

Siga estos pasos:

1. Haga clic en **Acciones** y, a continuación, haga clic en **Servidor de puntos de recuperación JumpStart**.

   Se abrirá el **Asistente del servidor de punto de recuperación Jumpstart**.

2. Seleccione Desde una carpeta compartida a un almacén de datos en un servidor de punto de recuperación seleccionado..

3. Especifique que la carpeta compartida de origen.

   Aparecerán los detalles del punto de recuperación.

   Nota: Si ni la sesión ni el almacén de datos de destino están cifrados, la contraseña de sesión es opcional. Si la sesión no está cifrada pero el almacén de datos de destino sí está cifrado, se deberá proporcionar una contraseña de sesión en la página **Selección del almacén de datos de destino**.

4. Haga clic en **Siguiente**.

   Se abre la página **Selección del almacén de datos de destino.** Si se cifran los datos de origen, solamente aparecerán los almacenes de datos cifrados en la lista desplegable.

5. (Opcional) Especifique la contraseña de la sesión si la sesión no se cifra en el Paso 3.

6. Haga clic en **Siguiente**.

7. Haga clic en **Finalizar**.

   Los datos del punto de recuperación de Arcserve r16.5 se replican en el almacén de datos de Arcserve UDP.

Configuración del asistente de configuración

Con el asistente de configuración, configure el entorno de protección de los datos tan pronto como inicie sesión en la Consola. Si se utiliza Arcserve UDP por primera vez, el Asistente de configuración es una forma ideal para crear el primer plan de copia de seguridad. El asistente crea planes para definir cómo proteger los datos. Un plan está formado por una o varias tareas para definir el origen, el destino, la programación y los parámetros avanzados. Con el primer inicio de sesión en la Consola, se abrirá el asistente de configuración. Se puede ocultar la página de bienvenida del asistente seleccionando **No mostrar esta página la próxima vez**.

Se puede crear un plan para proteger los nodos físicos como, por ejemplo, los nodos de Windows y de Linux, y máquinas virtuales como, por ejemplo, VMware e Hyper-V.

Los siguientes pasos describen una descripción genérica sobre cómo crear un plan basado en el Agente de Windows mediante el Asistente de configuración.

1. Inicie sesión en la Consola.

   Si se está iniciando sesión por primera vez, se abrirá el Asistente de configuración.

2. Si no se abre el asistente, haga clic en la ficha **recursos** y, a continuación, haga clic en **Asistente de configuración** en el panel derecho.

   Se abre la página de bienvenida del asistente.

3. Haga clic en **Siguiente**.

   Se abre la página **Crear un plan**.

4. Especifique el nombre del plan.

5. Seleccione un tipo de nodo que se deberá proteger.

   Por ejemplo, seleccione **Copia de seguridad: Windows, basada en agentes**.

6. Haga clic en **Siguiente**.

   Se abre el cuadro de diálogo **Agregar nodos para proteger.** Los campos son opcionales en la página **Agregar nodos para proteger**.

7. Seleccione el método para agregar nodos de la lista desplegable.

   Los campos varían en función de la selección.

8. Proporcione los detalles del nodo, haga clic en **Agregar a la lista** y, a continuación, haga clic en **Siguiente**.

   Se abre la página **Destino de copia de seguridad**.

9. Especifique el tipo de destino en la lista desplegable.

Los campos restantes de la página **Destino de la copia de seguridad** varían en función del tipo de destino. También se puede activar la contraseña de sesión.

Para crear un almacén de datos, consulte Agregar un almacén de datos.

10. Especifique los detalles restantes del destino y haga clic en **Aceptar**.

    Se abre la página **Programación de la copia de seguridad**.

11. Especifique la programación de la copia de seguridad y haga clic en **Siguiente**.

    Se abre la página **Confirmación del plan**.

12. Verifique el plan.
13. (Opcional) Haga clic en **Crear un plan** para agregar otro plan.
14. Haga clic en **Siguiente**

    La configuración del recurso se ha completado.

15. Haga clic en **Finalizar**.

    Se cierra el asistente y se crea un nuevo plan.

    Se puede ver el plan en **recursos**, **Planes**, **Todos los planes**.

Capítulo 6: Funcionamiento de las funciones clave de Arcserve UDP

Esta sección incluye los siguientes temas:

Funcionamiento de la función Nutanix en Arcserve UDP

Para explorar las funciones disponibles para la función Nutanix en Arcserve UDP, consulte Cómo funcionan Nutanix con Arcserve UDP.

Funcionamiento de la función OneDrive en Arcserve UDP

Explore las funciones disponibles para la función OneDrive en Arcserve UDP.

- Gestión de los nodos de OneDrive
- Cómo crear un plan de copia de seguridad de Microsoft Office 365 OneDrive
- Cómo restaurar los datos de OneDrive

Funcionamiento de la función Exchange Online en Arcserve UDP

Exchange Online es una aplicación de correo electrónico que se aloja en la nube de Microsoft. Para proteger los elementos de correo de Exchange Online (correos, elementos del calendario, contactos, etc.) desde la nube de Microsoft, es necesario crear un plan en Arcserve UDP. Explore las funciones disponibles para la función Exchange Online en Arcserve UDP.

- Privilegios de usuario para Exchange Online en Arcserve UDP
- Adición de un nodo de Exchange Online
- Gestión de los nodos de Exchange Online
- Adición del rol y del grupo necesarios a la cuenta de copia de seguridad de Exchange Online para realizar la copia de seguridad y la restauración
- Cómo crear un plan de copia de seguridad de Exchange Online
- Cómo restaurar los datos del buzón de correo de Exchange Online
- Aplicación de prácticas recomendadas

Funcionamiento de la función de instantánea de hardware en UDP

Arcserve UDP puede utilizar las instantáneas de almacenamiento de hardware para realizar copias de seguridad. Se puede especificar si se desea usar una instantánea de hardware durante la creación de una tarea de copia de seguridad. Si se selecciona la instantánea de hardware, Arcserve UDP intenta crear una instantánea de hardware en primer lugar. Si se produce un error en la instantánea de hardware, Arcserve UDP volverá automáticamente a la instantánea de software sin que se produzca un error en la tarea de copia de seguridad.

- Cómo utilizar la instantánea de hardware para copias de seguridad
- Matriz de almacenamiento compatible en Arcserve UDP
- Utilización de la instantánea de hardware para la copia de seguridad sin agente de VMware
- Utilización de la instantánea de hardware para la copia de seguridad sin agente de Hyper-V
- Utilización de la instantánea de hardware para la copia de seguridad basada en el agente
- Verificación del uso de la instantánea de hardware por parte de la copia de seguridad

Nimble

- Adición de una matriz de almacenamiento de
- Consideraciones sobre el almacenamiento de Nimble cuando la autenticación CHAP está activada
- Utilización de la instantánea de hardware para la copia de seguridad sin agente de VMware

HPE 3PAR StoreServe

- Adición de una matriz de almacenamiento de
- Utilización de la instantánea de hardware para la copia de seguridad sin agente de VMware

NetApp

- Adición de una matriz de almacenamiento de
- Consideraciones para la compatibilidad de NetApp iSCSI/FC con VMware

- Condiciones aplicadas a la instantánea de hardware de VMware de NFS de NetApp
- Utilización de la instantánea de hardware para la copia de seguridad sin agente de VMware

Funcionamiento de la función de la nube en UDP

La función de la nube de Arcserve UDP garantiza que se han protegido los datos en la nube en caso de una supresión accidental. Con el uso de la función de la nube de Arcserve UDP se pueden copiar los archivos especificados, los puntos de recuperación, crear instancias utilizando puntos de recuperación, crear máquinas virtuales de Virtual Standby en la nube, etc.

Consulte los vínculos para utilizar la nube en Arcserve UDP:

- Adición de una cuenta de la nube
- Gestión de los nodos para la nube
  - Descarga de un punto de recuperación de la nube
  - Carga de un punto de recuperación a la nube
  - Copia de un punto de recuperación en el disco local o recurso compartido de red
- Cómo configurar un servidor de puntos de recuperación en la nube
  - Cómo especificar la configuración de la nube para restaurar desde una ubicación de la nube de la copia de archivos
  - Cómo especificar la configuración de la nube para restaurar desde una ubicación de la nube del archivo de archivado
- Cómo realizar la copia de seguridad de los datos en la nube
  - Cómo crear un plan de Virtual Standby a AWS EC2
  - Cómo crear y gestionar una máquina virtual instantánea en Amazon EC2
  - Cómo crear un plan de copia de puntos de recuperación
- Nube para Linux
  - Instalación del Agente de Arcserve UDP (Linux) en la nube de AWS
  - Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux en la nube de AWS
  - Cómo realizar una reconstrucción completa (BMR) de la migración para los equipos de Linux desde Amazon EC2 al equipo local
  - Cómo realizar la migración de la máquina virtual instantánea desde la nube al recurso local
- Plan de copia de seguridad de Microsoft Office 365

- Cómo crear un plan de copia de seguridad de Exchange Online
- Cómo restaurar los datos del buzón de correo de Exchange Online
- Cómo crear un plan de copia de seguridad de Microsoft Office 365 OneDrive
- Cómo restaurar los datos de OneDrive
- Creación de un plan de copia de seguridad de SharePoint Online (Vídeo)
- Cómo restaurar los datos de recopilación de sitios de SharePoint Online

- Microsoft Azure
  - Cómo crear un plan de Virtual Standby a Microsoft Azure
  - Cómo crear y gestionar una máquina virtual instantánea en Microsoft Azure
- Solución de problemas
  - Cómo agregar la contraseña de cifrado para un destino cifrado existente
  - Configuración del registro para la tarea de copia del punto de recuperación
  - Congestión del ancho de banda con las tareas de copia del punto de recuperación a la nube
  - No se puede conectar con la nube

Funcionamiento de la función de la ruta UNC/NFS en UDP

La ruta UNC/NFS se introduce como un nuevo tipo de nodo. Para utilizar la función, consulte las siguientes secciones:

- Privilegios de usuario para la ruta UNC/NFS en Arcserve UDP
- Cómo agregar y gestionar una ruta UNC/NFS
- Cómo crear un plan de copia de seguridad de la ruta UNC/NFS
- Cómo restaurar desde una ruta UNC/NFS

Funcionamiento de la función SharePoint Online en UDP

Arcserve UDP v6.5 Actualización 2 y versiones posteriores admite trabajar con el entorno de Microsoft SharePoint Online. Para utilizar la función, consulte las siguientes secciones:

- Requisitos previos
- Adición de un nodo de SharePoint
- Gestión de los nodos de SharePoint Online
- Creación de un plan de copia de seguridad de SharePoint Online
- Cómo restaurar los datos de recopilación de sitios de SharePoint Online

Requisitos previos

Arcserve UDP 8.0 tiene el siguiente requisito previo para trabajar con el entorno de Microsoft SharePoint Online:

Asegúrese de que tiene los privilegios de usuario apropiados para las funciones de Arcserve UDP. Para obtener más información, consulte Privilegios de usuario para SharePoint Online en Arcserve UDP.

Capítulo 7: Uso de la administración basada en roles de Arcserve UDP

Administración basada en roles (RBAC) permite a los administradores asignar distintos roles y permisos a usuarios diferentes para utilizar la Consola de Arcserve UDP. Cada rol puede tener sus propios permisos. Un rol de superadministrador puede crear roles personalizados y permisos para otros usuarios de la Consola de Arcserve UDP.

Mediante RBAC pueden asignarse niveles de seguridad variables para cada rol.

Esta sección incluye los siguientes temas:

Acceso a la Consola de gestión de usuarios

La página Gestión de usuarios le permite hacer lo siguiente:

- Iniciar sesión en la Consola de gestión de usuarios (Consola del servicio de identidad) desde la Consola de Arcserve UDP.
- Activar y configurar la autenticación multifactor (MFA) para todos los usuarios.

Esta sección incluye los siguientes temas:

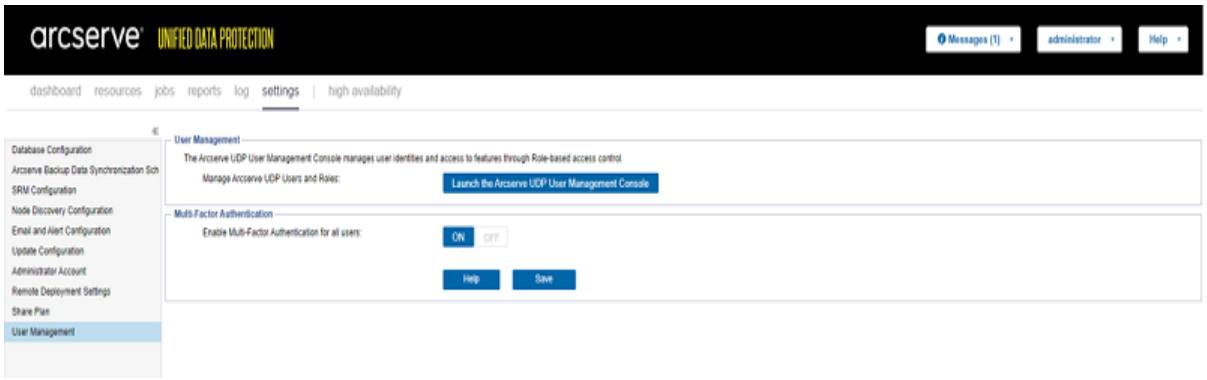
Inicio de la Consola de gestión de usuarios de Arcserve UDP

La Consola de gestión de usuarios de Arcserve UDP gestiona las identidades de usuario y controla el acceso a las funciones mediante el control de acceso basado en roles. Esta sección proporciona información sobre cómo iniciar la Consola de gestión de usuarios de Arcserve UDP.

Siga estos pasos:

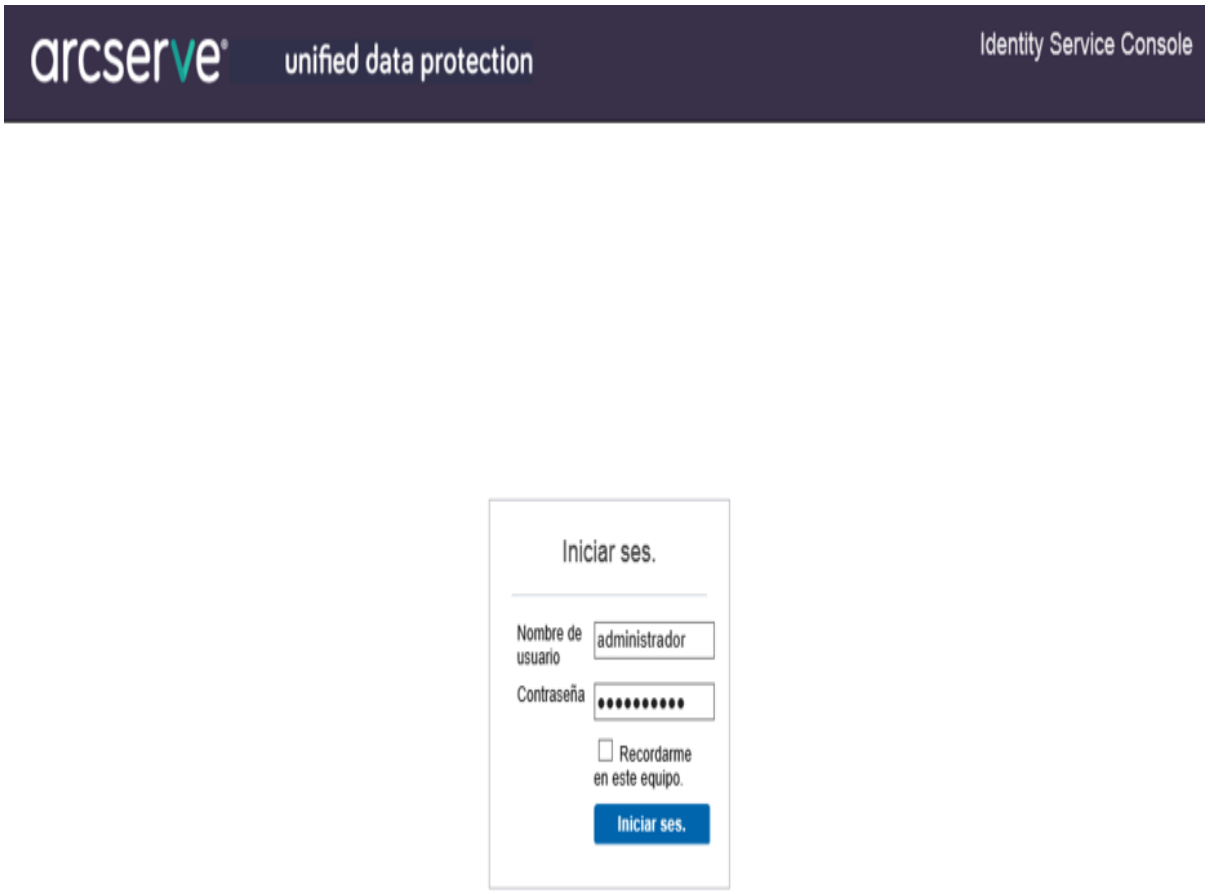
1. Inicie sesión en la Consola de Arcserve UDP.
2. Vaya a **Configuración** > **Gestión de usuarios**.

   Aparece la página Gestión de usuarios en el panel central.



3. Haga clic en **Iniciar la consola de gestión de usuarios de Arcserve UDP**.

   La Consola del servicio de identidad se abre en una ventana nueva.



4. Especifique el nombre de usuario y la contraseña, y, a continuación, haga clic en **Iniciar sesión**.

   Aparece la página principal de la Consola del servicio de identidad.

   Se ha obtenido acceso correctamente a la Consola de gestión de usuarios de Arcserve UDP.

   De forma alternativa, también se puede iniciar sesión en la Consola del servicio de identidad. Para iniciar sesión, introduzca la dirección con el siguiente formato en la nueva ventana:

   http (o https):///(dirección IP o nombre de host):(número de puerto de la Consola)/carbon

Configuración de la autenticación multifactor

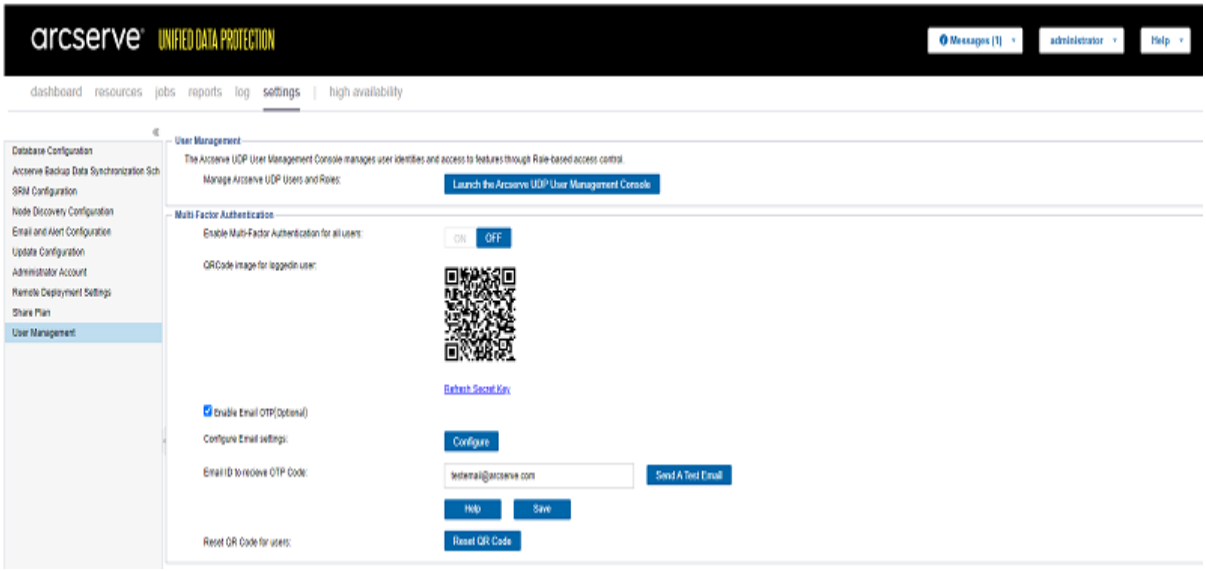
Esta sección proporciona los siguientes temas:

Configuración de la autenticación multifactor como usuario administrador

Esta sección proporciona información sobre cómo configurar la autenticación multi-factor para todos los usuarios.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP con las credenciales de administrador.
2. Vaya a **Configuración** > **Gestión de usuarios**.



3. Para activar la autenticación multifactor para todos los usuarios, en la sección Autenticación multifactor, **active** la configuración.

   Aparece la imagen del código QR para el usuario que ha iniciado sesión.

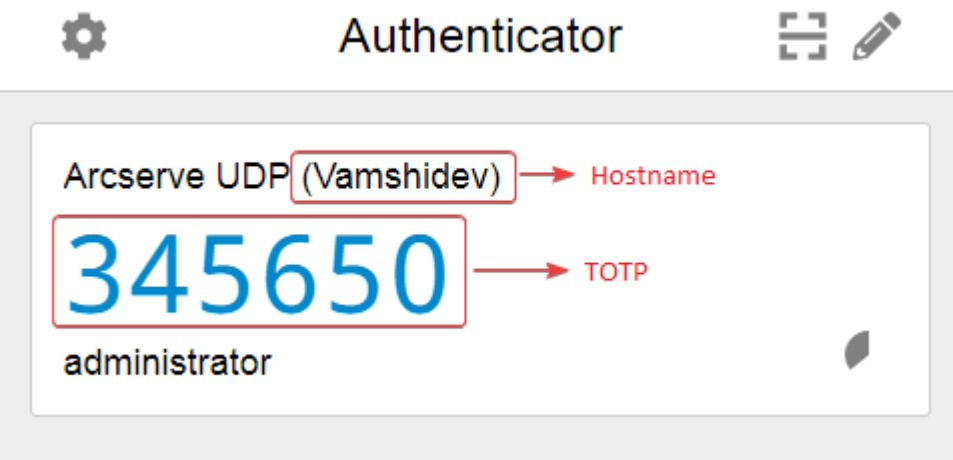
   Nota: Si desea desactivar la autenticación multifactor para todos los usuarios, **desactive** la opción.

4. Para generar el TOTP, escanee la imagen del código QR con una aplicación de autenticación.

   Notas:

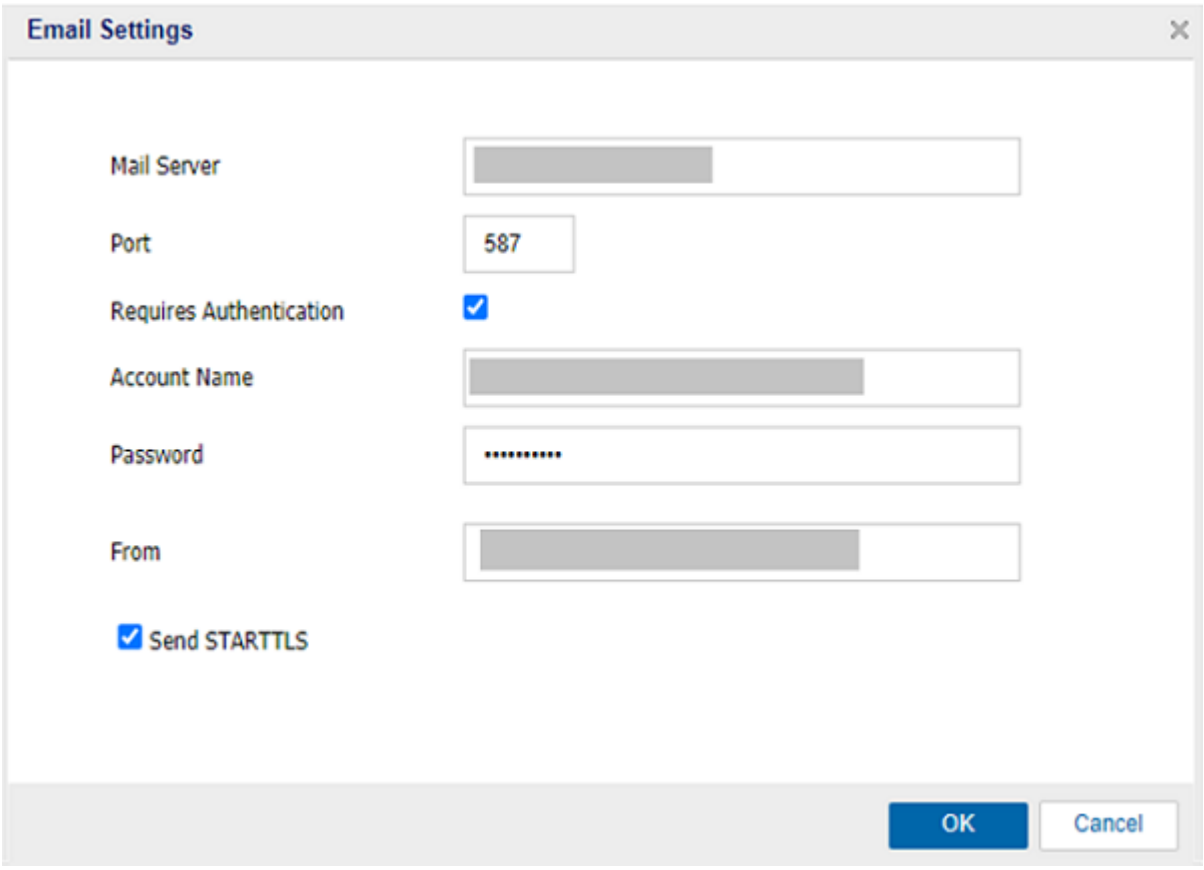
   - Se puede utilizar cualquiera de las aplicaciones de autenticación móvil como la aplicación Google Authenticator o la aplicación Microsoft Authenticator del dispositivo móvil. De forma alternativa, también se puede utilizar la extensión Authenticator en el explorador Chrome.

- Para generar un nuevo código TOTP, haga clic en el vínculo **Actualizar clave secreta** situado debajo de la imagen del código QR.
- Cuando se utiliza una aplicación de autenticación para varias cuentas de usuario, el nombre de host de la cuenta de usuario diferencia a los TOTP. En la aplicación de autenticación, se puede ver el nombre de host y su respectivo TOTP.



5. (Opcional) Si desea activar la OTP de correo electrónico, seleccione **Activar la OTP del correo electrónico (opcional)** y, a continuación, haga lo siguiente:
   a. Para configurar los valores de configuración del correo electrónico, haga clic en el botón **Configurar**.

      Aparece el cuadro de diálogo Configuración del correo electrónico.



b. En el cuadro de diálogo Configuración del correo electrónico, haga lo siguiente y, a continuación, haga clic en **Aceptar**:

- **Servidor de correo:** Escriba la dirección del servidor de correo electrónico.
- **Puerto:** Escriba el número de puerto para el servidor de correo electrónico.
- Si el servidor de correo electrónico especificado requiere autenticación, seleccione la casilla de verificación **Requiere autenticación**.
- **Nombre de cuenta:** Escriba el nombre de usuario o la dirección de correo electrónico del servidor de correo electrónico especificado.
- **Contraseña:** Escriba la contraseña para autenticar.
- **De:** Escriba la dirección de correo electrónico del remitente según sea necesario.

- Si el servidor de correo electrónico especificado requiere el comando de protocolo STARTLS, seleccione la casilla de verificación **Enviar STARTLS**.

c. Para que el *ID de correo electrónico para recibir el código de OTP*, escriba una o más direcciones de correo electrónico.

Nota: Debe proporcionar una dirección de correo electrónico para recibir la OTP durante el proceso de inicio de sesión. Si desea proporcionar varias direcciones de correo electrónico, utilice el punto y coma (;) para separarlas.



d. Para comprobar si las direcciones de correo electrónico configuradas están recibiendo la OTP, haga clic en **Enviar un correo electrónico de prueba**.

6. Haga clic en **Guardar**.

   Aparecerá un diálogo de confirmación.

   Nota: Aparece el cuadro de diálogo de confirmación para reiniciar el servicio de identidad solo cuando se configura, modifica o elimina la configuración del correo electrónico.

7. En el cuadro de diálogo de confirmación, para reiniciar el servicio de identidad, haga clic en **Sí**.

   Después de reiniciar el servicio de identidad, actualice el explorador. Esto es necesario para que se aplique la configuración del correo electrónico.

Para restablecer el código QR, consulte Cómo restablecer el código QR.

Cómo restablecer el código QR

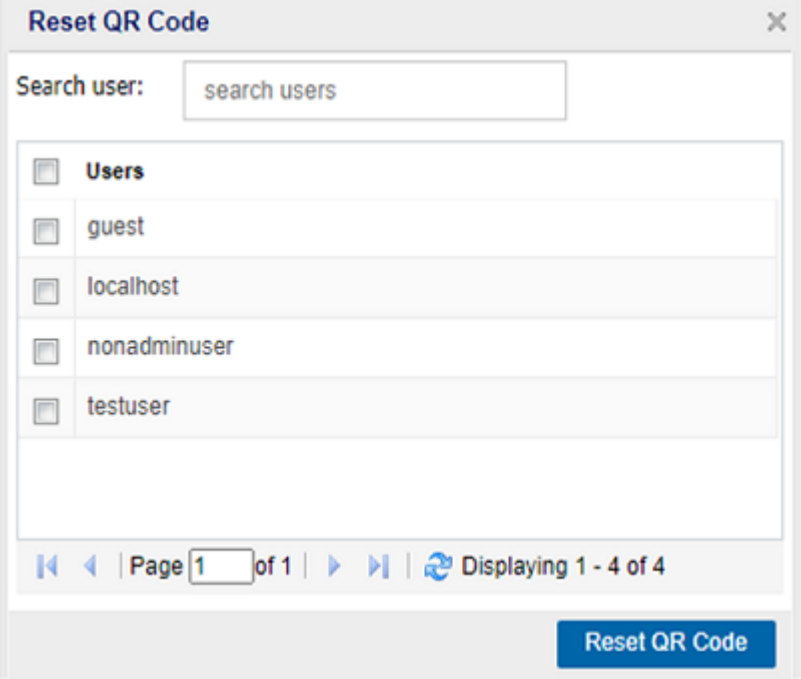
Esta sección proporciona información sobre cómo restablecer el código QR para los usuarios.

Nota: Un usuario administrador puede restablecer el código QR para todos los usuarios excepto el suyo.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP con las credenciales de administrador.
2. Vaya a **Configuración** > **Gestión de usuarios**.
3. Para *Restablecer el código QR para los usuarios*, haga clic en el botón **Restablecer código QR**.

   Aparecerá el cuadro de diálogo Restablecer código QR.



4. En el cuadro de diálogo Restablecer código QR, en la lista de usuarios, seleccione los usuarios para los que desea restablecer el código QR y, a continuación, haga clic en **Restablecer código QR**.

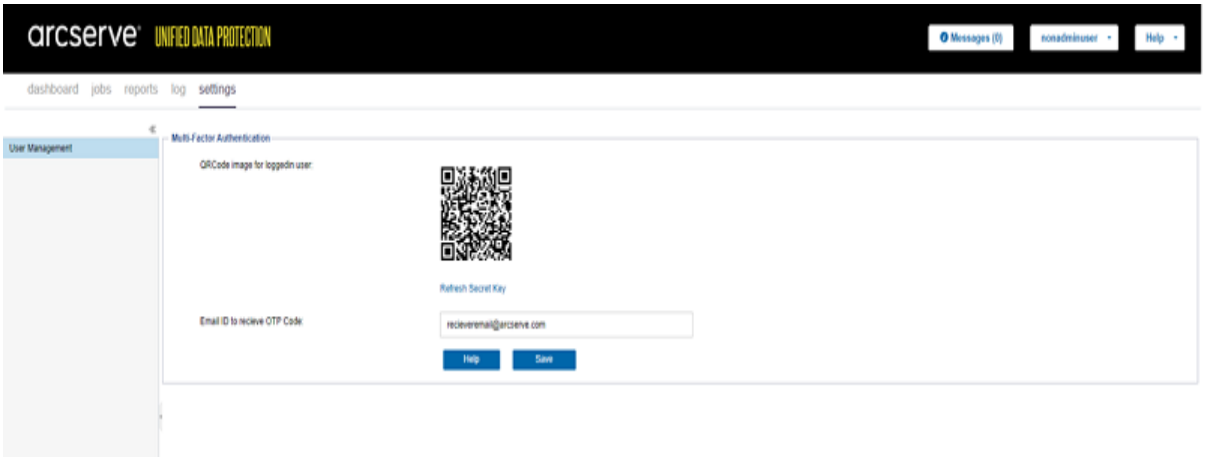
Nota: Después de restablecer el código QR, durante el siguiente inicio de sesión, los usuarios seleccionados deberán volver a escanear el código QR para obtener un nuevo TOPT y volver a registrarse.

Configuración de la autenticación multifactor como usuario no administrador

Esta sección proporciona información sobre cómo configurar la autenticación multifactor para su propio perfil de usuario.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP con credenciales que no sean de administrador.
2. Vaya a **Configuración** > **Gestión de usuarios**.



Nota: La página *Configuración > Gestión de usuarios* no está disponible para los usuarios que no tienen el permiso de Gestión de usuarios. Sin embargo, el administrador puede asignar este permiso a todos los usuarios que no sean administradores o a otros usuarios. Para obtener más información, consulte Asignación de roles predefinidos.

3. Para generar un nuevo código TOTP, haga clic en el vínculo **Actualizar clave secreta** situado debajo de la imagen del código QR.
4. Para que el *ID de correo electrónico para recibir el código de OTP*, escriba una o más direcciones de correo electrónico.

   Nota: Debe proporcionar una dirección de correo electrónico para recibir la OTP durante el proceso de inicio de sesión. Si desea proporcionar varias direcciones de correo electrónico, utilice el punto y coma (;) para separarlas.



5. Haga clic en **Guardar**.

   Se guardarán los nuevos valores de configuración.

Adición de usuarios, eliminación de usuarios y cambios de contraseña

Puede agregar o eliminar usuarios locales o de dominio desde el control de usuarios de Windows. La lista de gestión de usuarios en la consola de servicio de identidad se actualiza inmediatamente.

Utilice el Control de usuarios de Windows para cambiar la contraseña de usuario. Cuando se actualiza la contraseña de un usuario, el usuario debe iniciar sesión en la Consola de servicio de identidad utilizando la contraseña más reciente. El rol del usuario se mantiene.

Configuración de la gestión de usuarios

Se pueden asignar distintos roles a cada usuario y proporcionar permisos diferentes para cada rol. La configuración de la gestión de usuarios le ayuda a realizar las siguientes opciones:

- Roles predefinidos
- Asignación de roles predefinidos
- Visualización y cancelación de un rol
- Adición de un nuevo rol
- Búsqueda de usuarios y roles



Roles predefinidos

La función de un rol predefinido es proporcionan una referencia a algunas definiciones típicas de roles. Cada rol dispone de un conjunto predefinido de permisos asignados.

Para el rol de administrador, se seleccionan todas las opciones de los permisos. Un rol de administrador puede acceder a todas las funciones de Arcserve UDP.

Haga clic en los permisos para el rol de copia de seguridad y los siguientes permisos seleccionados se han predefinido:

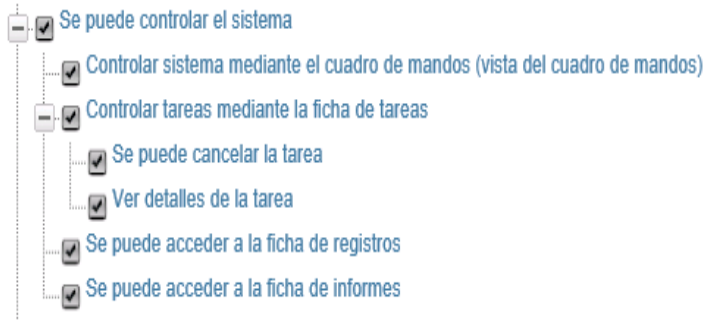

All Permissions
applications
ARCserve
Realizar copias de seguridad
Hacer copia de seguridad del nodo ahora
Verificar/aplicar actualizaciones
Se puede configurar el sistema
Administrator Account
Arcserve Backup Data Synchronization Schedule
Configuración de bases de datos
Configuración del correo electrónico y de alertas
Factory Reset
Installation Settings
Node Data Deletion Configuration
Node Discovery Configuration
Share Plan
SRM Configuration
Configuración de actualizaciones
User Management
Gestión de licencias
Gestionar máquina virtual instantánea
Gestionar recursos (crear, actualizar y suprimir)
Agregar hipervisores/configurar HBBU
Gestionar destinos/almacenes de datos
Create Arcserve backup servers
Delete Arcserve backup servers
Update Arcserve backup servers
View Arcserve backup servers
Create cloud accounts
Delete cloud accounts
Update cloud accounts
View cloud accounts
Crear
Suprimir
Importar almacén de datos
Servidor de puntos de recuperación JumpStart
Actualización
Ver
Delete recovery points

Los siguientes permisos se han predefinido para el rol de copia de seguridad:

- Realizar copia de seguridad
- Ver destino
- Gestionar nodos/planes/sitios
- Controlar la función del sistema

El rol de administrador tiene toda la flexibilidad necesaria para borrar los permisos seleccionados o para seleccionar un permiso nuevo. Cuando se haga clic en Actualizar, el permiso que se ha agregado recientemente se convertirá en el permiso predeterminado para el rol de copia de seguridad. También se puede cambiar el nombre del rol.

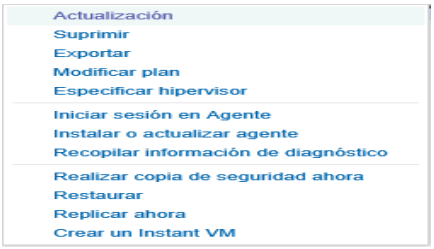
Para el rol de controlador, se seleccionan previamente el permiso de registro/generación de informes y el controlador de tareas del cuadro de mandos.



Para el rol de restauración, se seleccionan previamente los siguientes permisos:

- Gestionar máquina virtual instantánea
- Ver destino
- Ver nodo
- Ver plan
- Gestionar Virtual Standby
- Controlar tareas
- Registros de acceso
- Realizar la restauración

Si se asigna el rol de restauración a un usuario, el usuario podrá iniciar sesión y tendrá la autoridad correspondiente. Por ejemplo, para un usuario que tiene el rol de restauración, si se realiza la copia de seguridad de un nodo correctamente, se podrá crear una máquina virtual instantánea o una restauración para ir a la siguiente actividad.



Para el rol de _Admin, el permiso de administración de RHA tiene el acceso a la función de alta disponibilidad.

Asignación de roles predefinidos

Cuando un superadministrador asigna un rol a cualquier usuario, solo el usuario puede iniciar sesión en la Consola. El botón Usuarios muestra la lista completa de usuarios, incluidos los usuarios de dominio y locales.

Puede asignar los roles disponibles (predefinidos) o autodefinidos a cualquier usuario local o de dominio.

Nota: Solamente un superadministrador (es decir, un administrador que instala Arcserve UDP) puede asignar el rol de administrador a otros usuarios. Los administradores solo pueden asignar roles de no administrador a otros usuarios.

Siga estos pasos:

1. Haga clic en **Usuarios y roles** en la página **Configurar**.

   Se mostrarán los usuarios y los roles en la página Gestión de usuarios.

2. Haga clic en **Usuarios** en la página Gestión de usuarios.

   Aparecerá la lista de usuarios.

3. Haga clic en **Asignar rol** para un usuario.

   Se abrirá la página **Lista de roles de usuario**.

4. Seleccione uno o varios roles y haga clic en **Actualizar**.

   El rol del usuario se ha actualizado correctamente.

5. Haga clic en **Finalizar** para volver a la pantalla anterior.

   Se ha asignado un rol al usuario correctamente.

Visualización y cancelación de un rol

Se puede ver el rol actual que se ha asignado a un usuario. Se puede cancelar un rol asignado desactivando la casilla de verificación del rol.

Siga estos pasos:

1. Haga clic en **Usuarios y roles** en la página **Configurar**.

   Se mostrarán los usuarios y los roles en la página **Gestión de usuarios**.

2. Haga clic en Usuarios en la página Gestión de usuarios.

   Aparecerá la lista de usuarios.

3. Desactive la casilla de verificación para cancelar un rol y haga clic en **Actualizar**.

   Los roles se eliminan del usuario.

   Nota: Si no se le asigna ningún rol, un usuario no puede iniciar sesión en la Consola de Arcserve UDP.

4. Haga clic en **Finalizar** para volver a la página anterior.

   Ha visualizado y cancelado un rol.

Adición de un nuevo rol

Se puede crear un rol personalizado y seleccionar los permisos que tendrá.

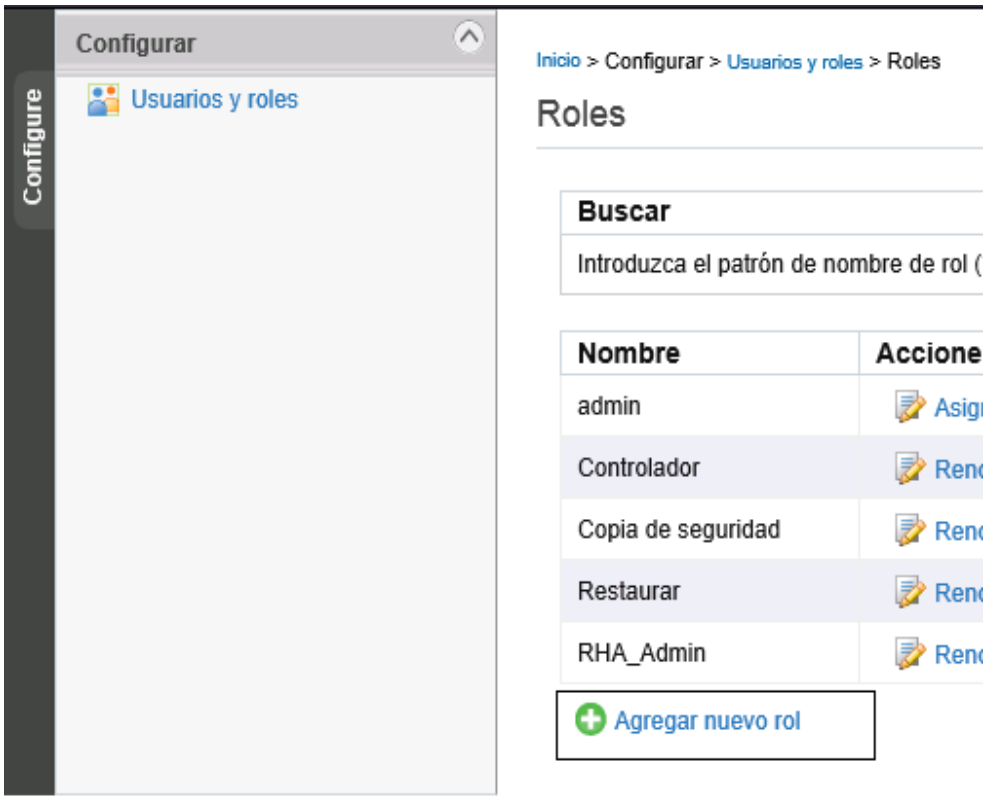
Siga estos pasos:

1. Haga clic en **Usuarios y roles** en la página **Configurar**.

   Se mostrarán los usuarios y los roles en la página **Gestión de usuarios**.

2. Haga clic en **Roles**.

   Se abrirá la página **Roles**, en la que se enumeran todos los roles disponibles.



3. Haga clic en **Agregar nuevo rol**.

   Se abrirá la página **Agregar rol**.

4. Escriba un nombre de rol y haga clic en **Siguiente**.

   Nota: No utilice caracteres especiales como **~!@# $% ^ & * ** y otros en el nombre de un rol.

5. Seleccione las casillas de verificación de los permisos necesarias y haga clic en **Siguiente**.

6. Seleccione usuarios para este rol.

7. Haga clic en **Finalizar**.

Se creará un nuevo rol, al que se le habrán asignado permisos.

Nota: Algunos permisos solo funcionan cuando también se seleccionan los permisos relacionados. Por ejemplo, para configurar un rol para gestionar Virtual Standby, se debe seleccionar el permiso para gestionar Virtual Standby y el permiso para ver nodos a fin de asegurarse de que el rol puede funcionar con normalidad.

Búsqueda de usuarios y roles

Se pueden filtrar usuarios y roles para encontrar el usuario o rol requerido. Introduzca el signo asterisco (*) para buscar todos los usuarios y roles.

Para buscar un rol, siga estos pasos:

1. Haga clic en **Usuarios y roles** en la página **Configurar**.

   Se mostrarán los usuarios y los roles en la página **Gestión de usuarios**.

2. Haga clic en **Roles**.

   Se abre la página **Roles**.



3. Especifique el patrón del nombre de rol y haga clic en **Buscar**.

   Aparecen los resultados filtrados.

Para buscar un usuario, siga estos pasos:

1. Haga clic en **Usuarios y roles** en la página **Configurar**.

   Se mostrarán los usuarios y los roles en la página **Gestión de usuarios**.

2. Haga clic en **Usuarios**.

   Se abre la página **Usuarios**.

3. Especifique el patrón del nombre de usuario y haga clic en **Buscar**.

   Aparecen los resultados filtrados.

Integración de Arcserve UDP con Active Directory

Arcserve UDP es compatible con la integración de Active Directory (AD) utilizando los grupos de Windows y de Active Directory.

Esta sección incluye los siguientes temas:

- Cómo se integra Arcserve UDP 8.0 con Active Directory utilizando grupos de Windows
- Cómo se integra Arcserve UDP 8.0 con Active Directory utilizando grupos de Active Directory

Cómo integrar Arcserve UDP 8.0 con Active Directory utilizando grupos de Windows

La función existente Administración basada en roles (UDP-RBA) permite la gestión de permisos de UDP basados en grupos de Active Directory (AD). En la versión anterior de UDP-RBA, solo se admitían las cuentas individuales de usuarios de Active Directory. Ahora, los grupos de Active Directory pueden servir como roles de RBA.

El almacén de usuarios secundarios de solo lectura de LDAP se agrega automáticamente al ejecutar una utilidad.

Siga estos pasos:

1. Inicie el símbolo del sistema y ejecute *C:\Archivos de programa\Arcserve\Unified Data Protection\Management\BIN*.
2. Ejecute la utilidad *DomainAuthTool.bat*.

   La siguiente información aparece en la pantalla:

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>DomainAuthTool.bat
log4j:WARN No appenders could be found for logger (com.ca.arcserve.edge.app.base.util.CommonUtil).
log4j:WARN Please initialize the log4j system properly.


Uso: DomainAuthTool.bat <operación> <requisitos> [opciones]

        Operación (no distingue mayúsculas de minúsculas):
                Create          Crear o actualizar el valor de configuración del almacén de usuarios
LDAP
                Remove          Eliminar configuración del almacén de usuarios de solo lectura de LDA

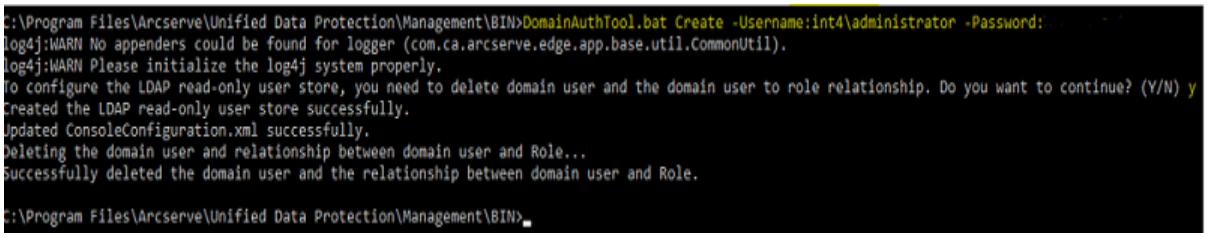
        Parámetro necesario (no distingue mayúsculas de minúsculas):
                -Username:<username>    El formato del nombre de usuario o administrador de la Consol
s dominio\usuario o nombreusuario@dominio.com
                -Password:<password>    Contraseña de administrador de la Consola de Arcserve UDP

        Parámetro opcional (no distingue mayúsculas de minúsculas):
                -DCName:<DC name>       El nombre o la dirección IP del controlador del dominio. Este
za para crear o modificar.
                -Protocol:<protocol>    El protocolo para AD, LDAP o LDAPS, este parámetro se utiliza
 modificación
                -Port:<port>            Puerto para AD (valor predeterminado: 389). Este parámetro se
 o modificar.

Ejemplos:
        DomainAuthTool.bat Create -Username:administrator -Password:1234
        DomainAuthTool.bat Create -Username:administrator -Password:1234 -DCName:10.57.1.2 -Protocol:
        DomainAuthTool.bat Remove -Username:administrator -Password:1234

C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>_
```

3. Cree un almacén de usuarios secundarios de solo lectura de LDAP y, al mismo tiempo, modifique los parámetros opcionales. Por ejemplo: Haga referencia al comando marcado en amarillo en la captura de pantalla siguiente.



4. Asigne el rol de usuario local.

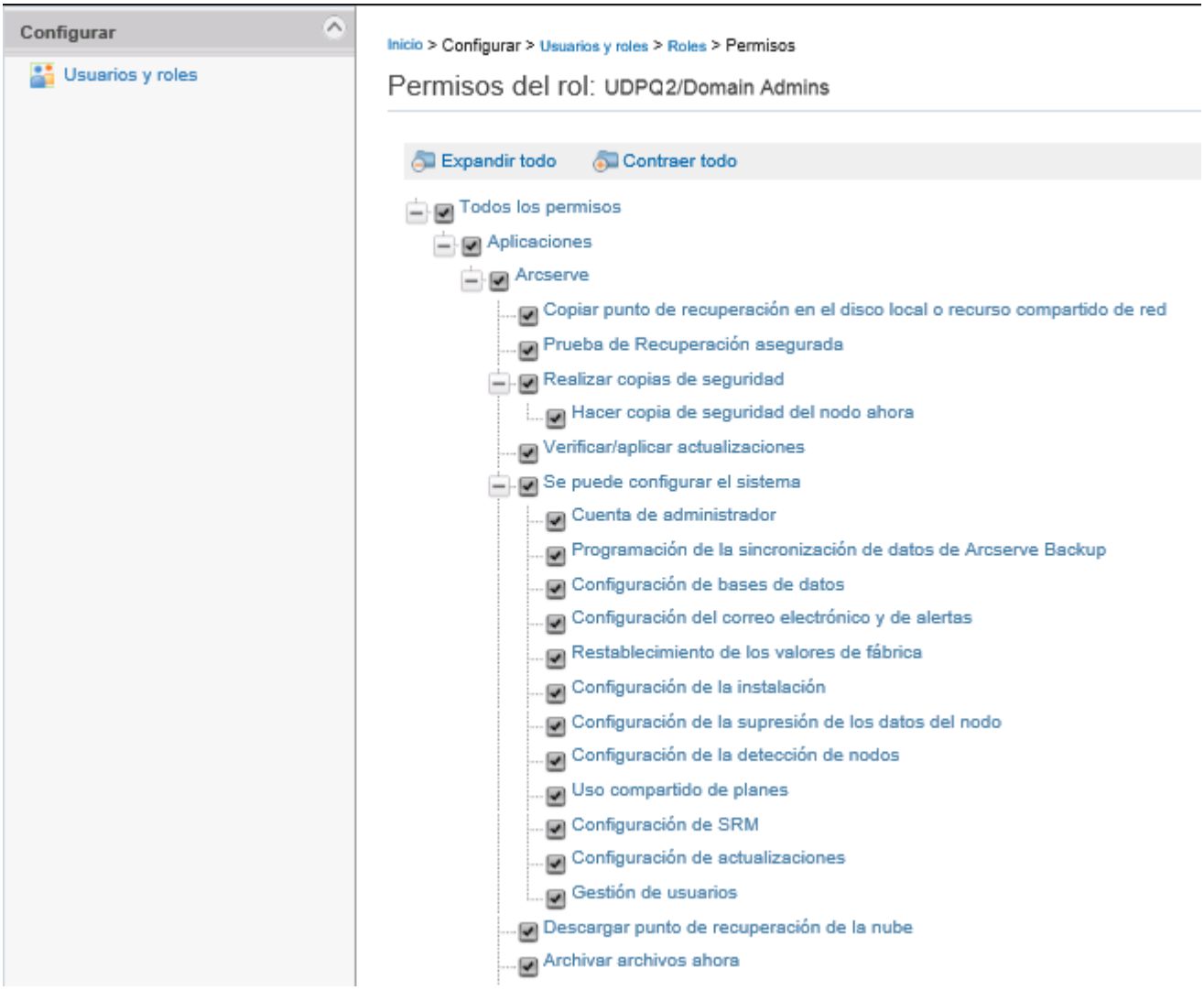
   Para obtener más información, consulte Asignación de roles predefinidos.

5. Para agregar permisos para los usuarios del dominio de solo lectura de LDAP, realice los pasos siguientes:

   a. Únase al grupo del controlador del dominio.

   b. Agregue el permiso de Arcserve UDP para el grupo correspondiente tal y como se muestra en la captura de pantalla siguiente.

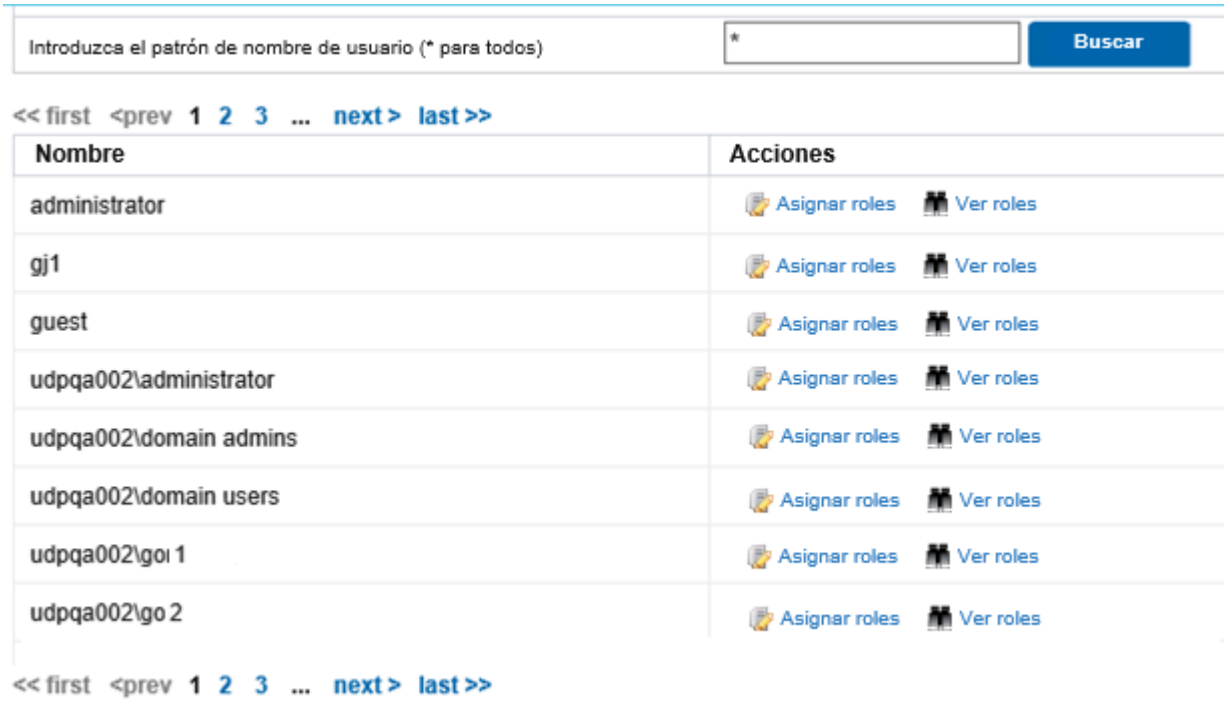
   Nota: No es posible asignar el rol predeterminado local directamente a los usuarios del dominio de solo lectura.



Ahora, el usuario puede iniciar sesión en la Consola de Arcserve UDP con el permiso específico.

6. (Opcional) Elimine el almacén de usuarios de LDAP con la utilidad.

   Ejecute la utilidad para eliminar el almacén de usuarios de LDAP. A continuación, reinicie el servicio de gestión y el usuario del dominio anterior aparecerá como se muestra a continuación.


Introduzca el patrón de nombre de usuario (* para todos)
*
Buscar
<< first <prev 1 2 3 ... next > last >>
Nombre
Acciones
administrator
gj1
guest
udpqa002\administrator
udpqa002\domain admins
udpqa002\domain users
udpqa002\go 1
udpqa002\go 2
Asignar roles
Ver roles
<< first <prev 1 2 3 ... next > last >>

Cómo integrar Arcserve UDP 8.0 con Active Directory utilizando grupos de Active Directory

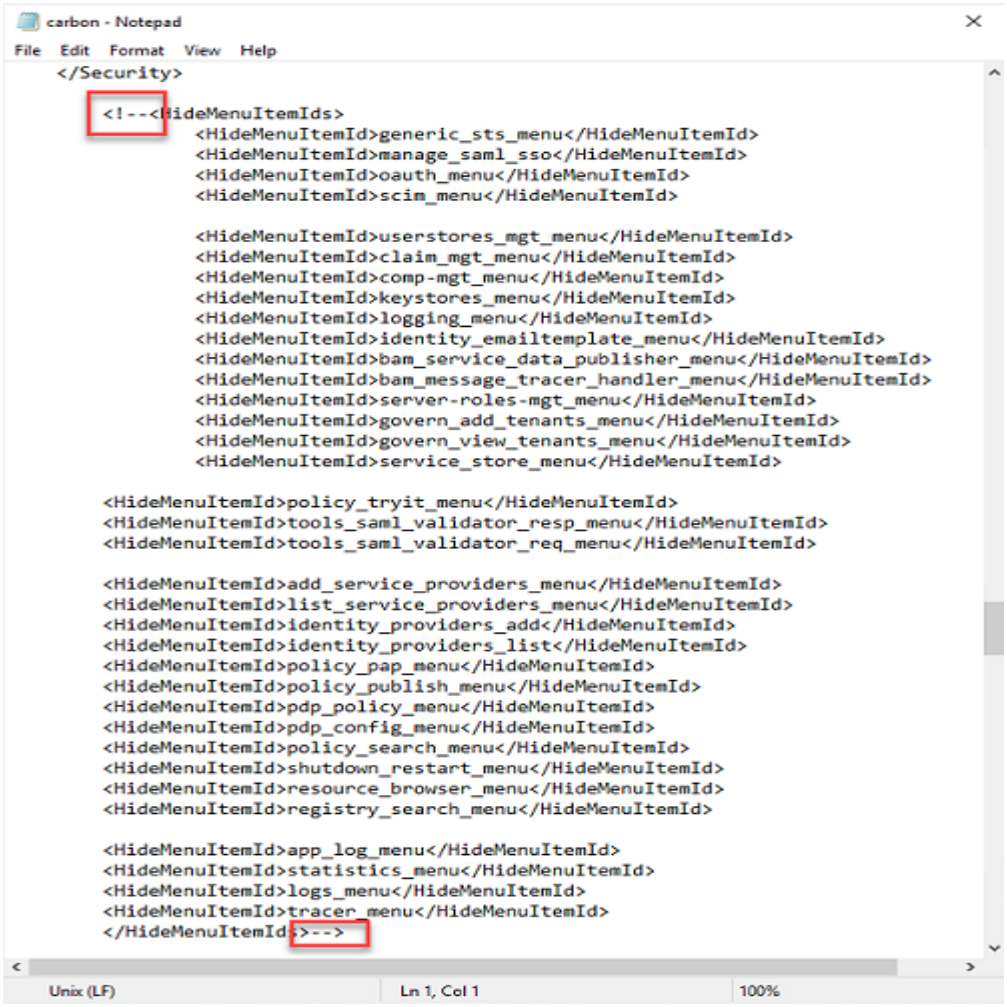
La administración basada en roles de Arcserve UDP 8.0 permite los permisos a nivel del usuario donde la función de Active Directory (AD) no está activada de forma predeterminada. Sin embargo, la plataforma de WSO2 Carbon en Arcserve UDP 8.0 no es compatible con los grupos de Active Directory que tienen el almacén de usuarios secundarios. Se puede activar la extensión para Arcserve UDP 8.0 que configura los grupos de Active Directory como roles de Arcserve UDP y ayuda a asignar los permisos de forma automática para los miembros del grupo de Active Directory.

Siga estos pasos:

1. Vaya a la siguiente ruta de instalación de Arcserve UDP y abra el archivo *carbon.xml*:

   …\Archivos de programa\Arcserve\Unified Data Protection\Management\IdentityServer\repository\conf\carbon.xml

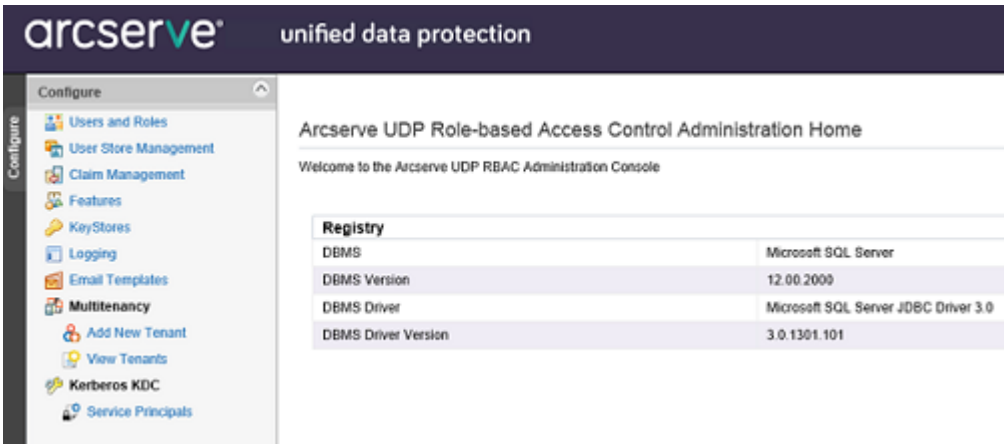
2. En el archivo *carbon.xml*, desactive el contenido de HideMenuItemIds utilizando <!-- and --> tal y como se muestra en la siguiente pantalla.



3. Guarde el archivo *carbon.xml* y reinicie el servicio de gestión de Arcserve UDP.
4. Abra la consola de gestión del usuario utilizando el vínculo siguiente:

   https://localhost:8015/carbon

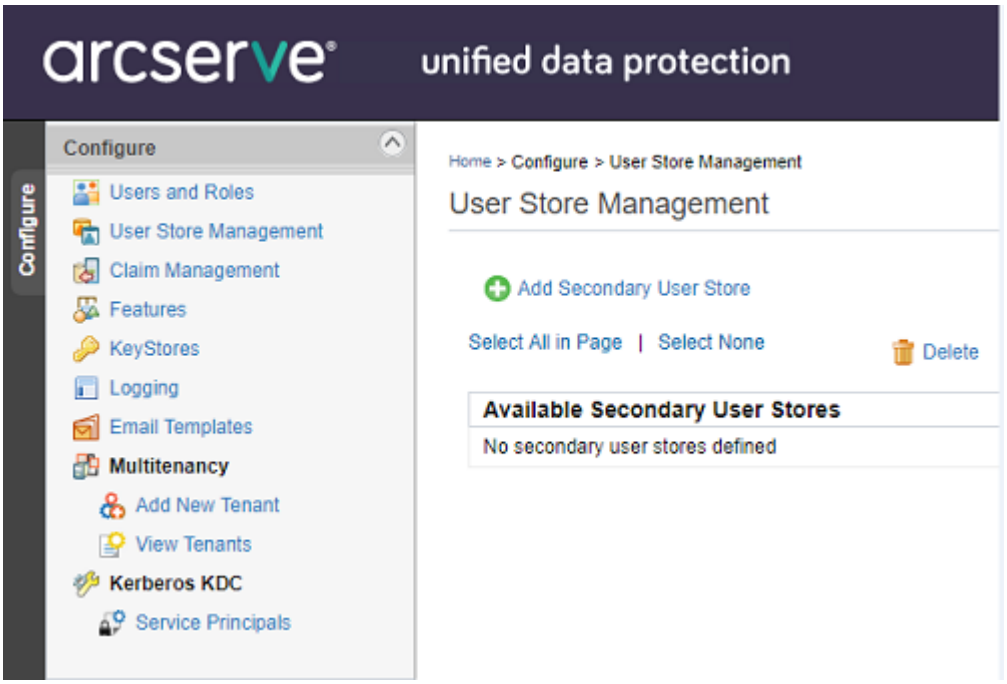
   Aparece la página principal de la administración del control de acceso basado en roles de *Arcserve UDP*.



5. Haga clic en la opción **Gestión del almacén de usuarios** disponible en el panel izquierdo.

   Aparece la página **Gestión del almacén de usuarios**.

6. Haga clic en **Agregar almacén de usuarios secundarios**.

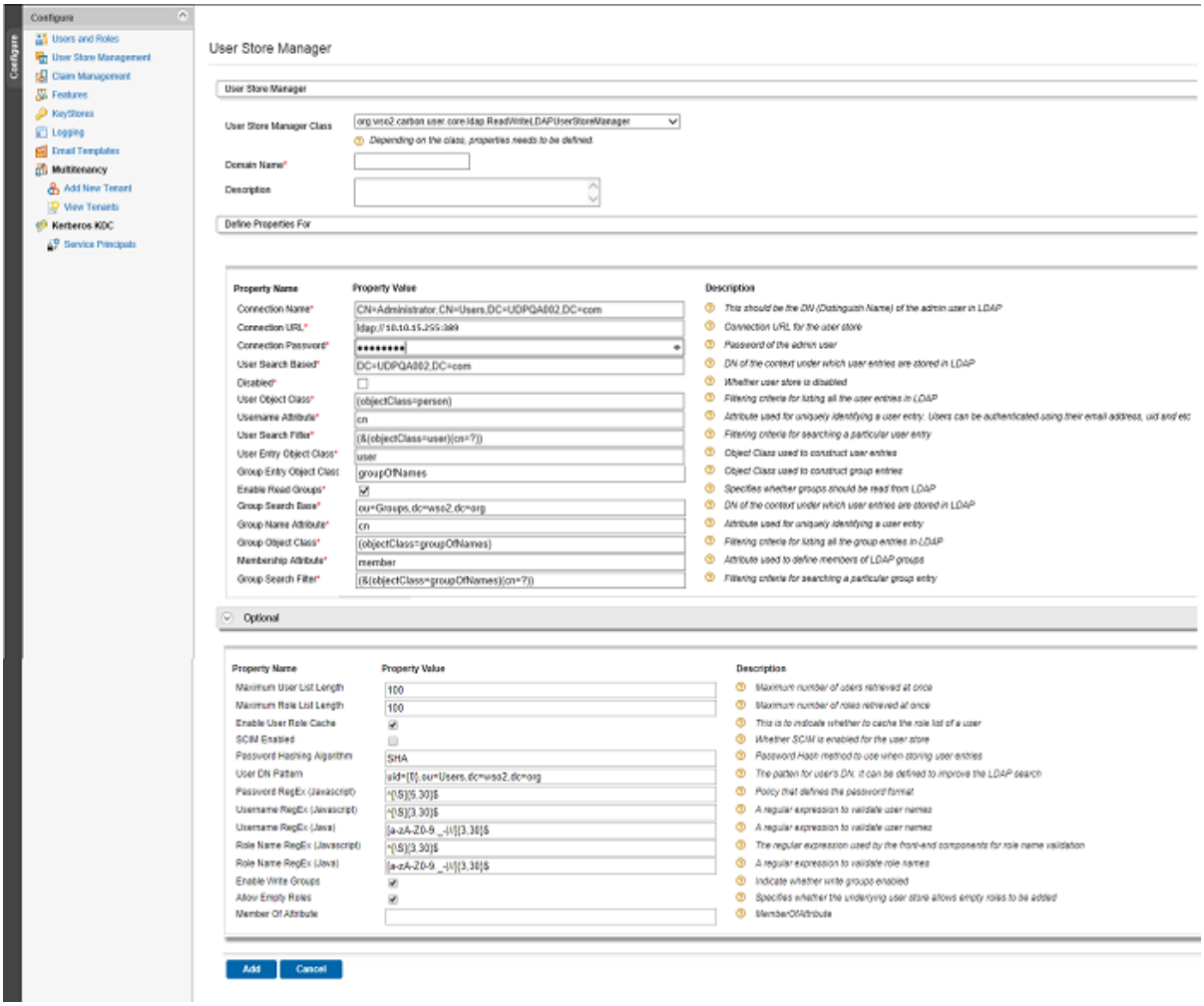


   Aparece la página **Gestor del almacén de usuarios**.

7. Seleccione la opción **Clase del gestor del almacén de usuarios** en la lista desplegable e introduzca el nombre del dominio en el campo **Nombre de dominio**.

8. Introduzca los detalles en los campos según sea necesario en **Definir propiedades** y **Grupos opcionales**.

La siguiente captura de pantalla es un ejemplo de la página Gestor del almacén de usuarios después de introducir los detalles.



9. Haga clic en **Agregar**.

   Aparece el cuadro de diálogo **Gestión de usuarios de UDP**.

10. Haga clic en **Aceptar**.

    La página Gestión del almacén de usuarios aparece y muestra el almacén de usuarios secundarios agregado.



Nota: Si no se muestra el almacén de usuarios secundarios, actualice el explorador.

11. (Opcional) Haga clic en la opción **Usuarios y roles** en el panel izquierdo para ver la lista de usuarios y roles.

    Nota: Se deben definir los roles en el dominio utilizando Active Directory.

12. Ahora, realice los pasos siguientes para agregar los permisos de rol de UDP:

    a. Seleccione un usuario de AD o un grupo de AD.

    b. Asigne un rol de la lista de roles disponibles.

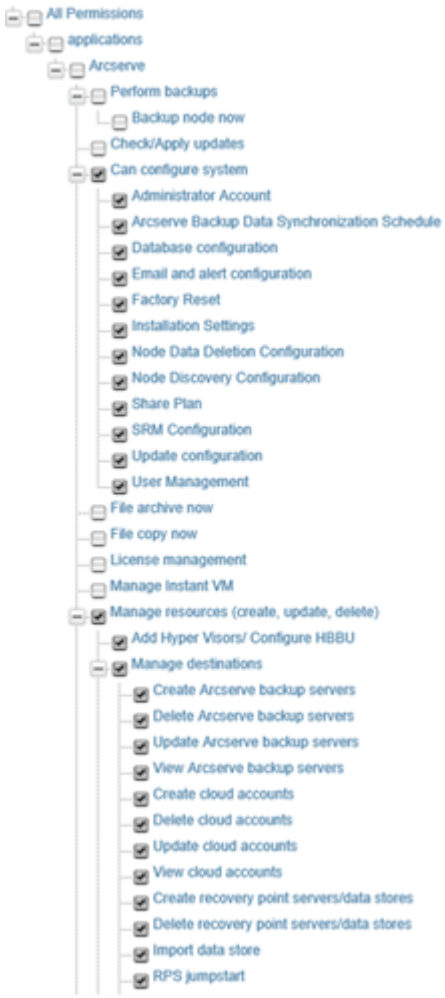
    c. Haga clic en **Ver rol**.

    Aparece la página **Lista de roles de usuario**.



    d. Haga clic en **Permisos**.

    Aparecerá la lista de permisos.



e. Seleccione los permisos como sea necesario.

Ahora, el usuario secundario puede iniciar sesión en la Consola de Arcserve UDP con los permisos asignados.

Acceso a Arcserve UDP utilizando la autenticación integrada de Windows

Los usuarios de Arcserve UDP ahora también pueden iniciar sesión mediante la autenticación integrada de Windows (IWA). La autenticación integrada de Windows facilita el inicio de sesión basado en el explorador. Si se ha autenticado una vez, la autenticación integrada de Windows permite al explorador web guardar las credenciales del usuario que ha iniciado sesión utilizando Windows. Solo será necesario introducir la dirección URL de la aplicación web protegida en el explorador. El explorador y el servidor se autentican y el usuario inicia sesión automáticamente.

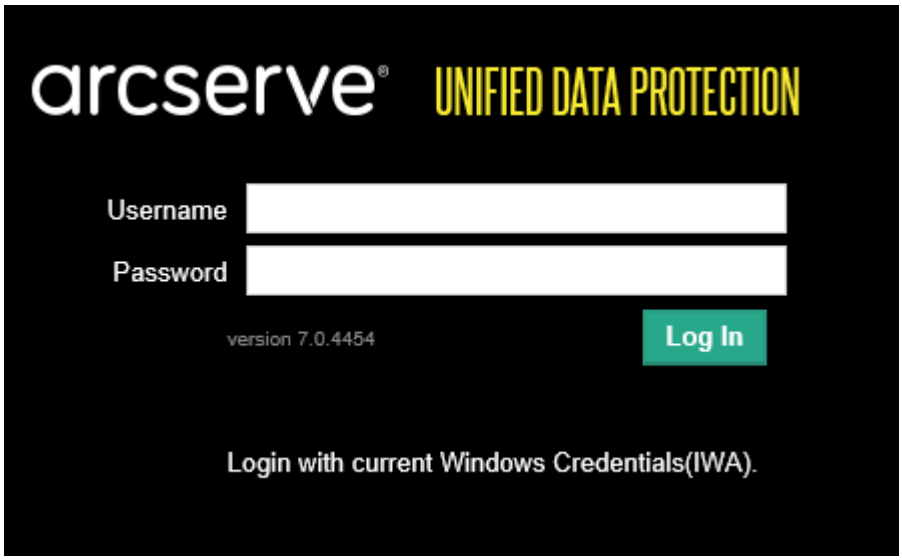
Nota: La Consola de Arcserve UDP no es compatible con IWA si la conexión de la base de datos de la Consola utiliza el modo de autenticación de Windows. Para obtener una solución alternativa, consulte el vínculo sobre la solución de problemas.

Con la introducción de la autenticación integrada de Windows, se puede utilizar la misma función y acceder a Arcserve UDP.

Siga estos pasos:

1. Abra la página de inicio de sesión de la Consola de Arcserve UDP.

   El vínculo de la autenticación integrada de Windows es visible en la página de inicio de sesión.



2. Haga clic en el vínculo: **Iniciar sesión con las credenciales de Windows actuales (IWA)**.

   Se abre la página principal.

   Para solucionar cualquier problema, consulte Solución de problemas.

Solución de problemas para la autenticación integrada de Windows (IWA)

Si el vínculo de la autenticación integrada de Windows no abre la página de la Consola, se pueden realizar los siguientes pasos para solucionar el problema:

1. Compruebe si se está utilizando la autenticación integrada de Windows en el equipo local en vez de en un equipo remoto.
2. Si aparece una pantalla en blanco después de hacer clic en el vínculo de la autenticación integrada de Windows, compruebe si se ha asignado el rol al usuario en la Consola de administración de RBAC.

   Nota: Si la conexión de la base de datos de la Consola utiliza el modo de autenticación de Windows, consulte el vínculo.
3. Configure utilizando los pasos indicados a continuación si se produce cualquier problema durante el inicio de sesión de IWA utilizando Firefox para abrir la dirección URL de la Consola.

   Siga estos pasos:

   a. En el campo de ubicación del explorador, introduzca about:config.

   b. Haga clic en **I'll be careful, I promise!** para continuar con la página about:config.

   c. Establezca los valores para las opciones siguientes para que el explorador confíe en el dispositivo ProxySG y negocie la autenticación:

      network.automatic-ntlm-auth.trusted-uris, network.negotiate.auth.delegation-uris, network.negotiate-auth.trusted-uris

      Para cada opción, realice los siguientes pasos:

      - Busque la opción que se desea establecer desplazándose o especificando el nombre de la opción en el campo de filtro.
      - Haga doble clic en la opción para abrir el cuadro de diálogo para especificar el valor de la cadena.
      - Introduzca la dirección URL virtual (para las implementaciones transparentes).

        Si dispone de más de un dispositivo ProxySG que solicitará las credenciales de autenticación, separe las entradas con comas. Por ejemplo, si la dirección URL abierta para la Consola es https://localhost:8015, se puede introducir localhost como el valor

de la cadena. O si la dirección URL abierta es https://10.57.60.9:8015, introduzca 10.57.60.9 como el valor de la cadena.

- Haga clic en **Aceptar**.

4. Mientras se utiliza Internet Explorer para abrir la Consola con IWA en el equipo remoto cuyas credenciales de Windows sean exactamente iguales a las credenciales del equipo local que ha instalado UDP, es posible que se deba configurar utilizando los pasos siguientes:
   a. Seleccione Herramientas > Opciones de Internet.
   b. Seleccione la ficha Seguridad.
   c. Seleccione la zona de Intranet local y haga clic en Sitios > **Opciones avanzadas**.
   d. Escriba el nombre de dominio completo del dispositivo ProxySG (para implementaciones explícitas) o la dirección URL virtual (para implementaciones transparentes) en el campo Agregar este sitio web a la zona y, a continuación, haga clic en Agregar > Cerrar > Aceptar.
   e. Seleccione la ficha Opciones avanzadas y asegúrese de que la opción Seguridad > Activar autenticación integrada de Windows está seleccionada.
   f. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo Opciones de Internet.

La Consola de Arcserve UDP no es compatible con IWA si la conexión de la base de datos de la Consola utiliza el modo de autenticación de Windows

Para utilizar la autenticación integrada de Windows (IWA), se debe cambiar el modo de autenticación de la configuración de la base de datos de la Consola a SQL Server y al modo de autenticación de Windows.

Siga estos pasos:

1. En la herramienta de gestión de SQL Server, compruebe si la base de datos de la Consola es compatible con SQL Server y con el modo de autenticación de Windows. Si la base de datos de la Consola no es compatible, cambie al modo de autenticación de Windows y a SQL Server y, a continuación, reinicie SQL Server.
2. Realice los pasos siguientes para crear la cuenta de Arcserve UDP en SQL Server:
    a. En la carpeta siguiente, haga clic con el botón secundario del ratón en **DBAccountUpdate.bat** y haga clic en la opción **Ejecutar como administrador**:

    <Carpeta de instalación de UDP>\Management\BIN

    Se abre la interfaz de comandos.

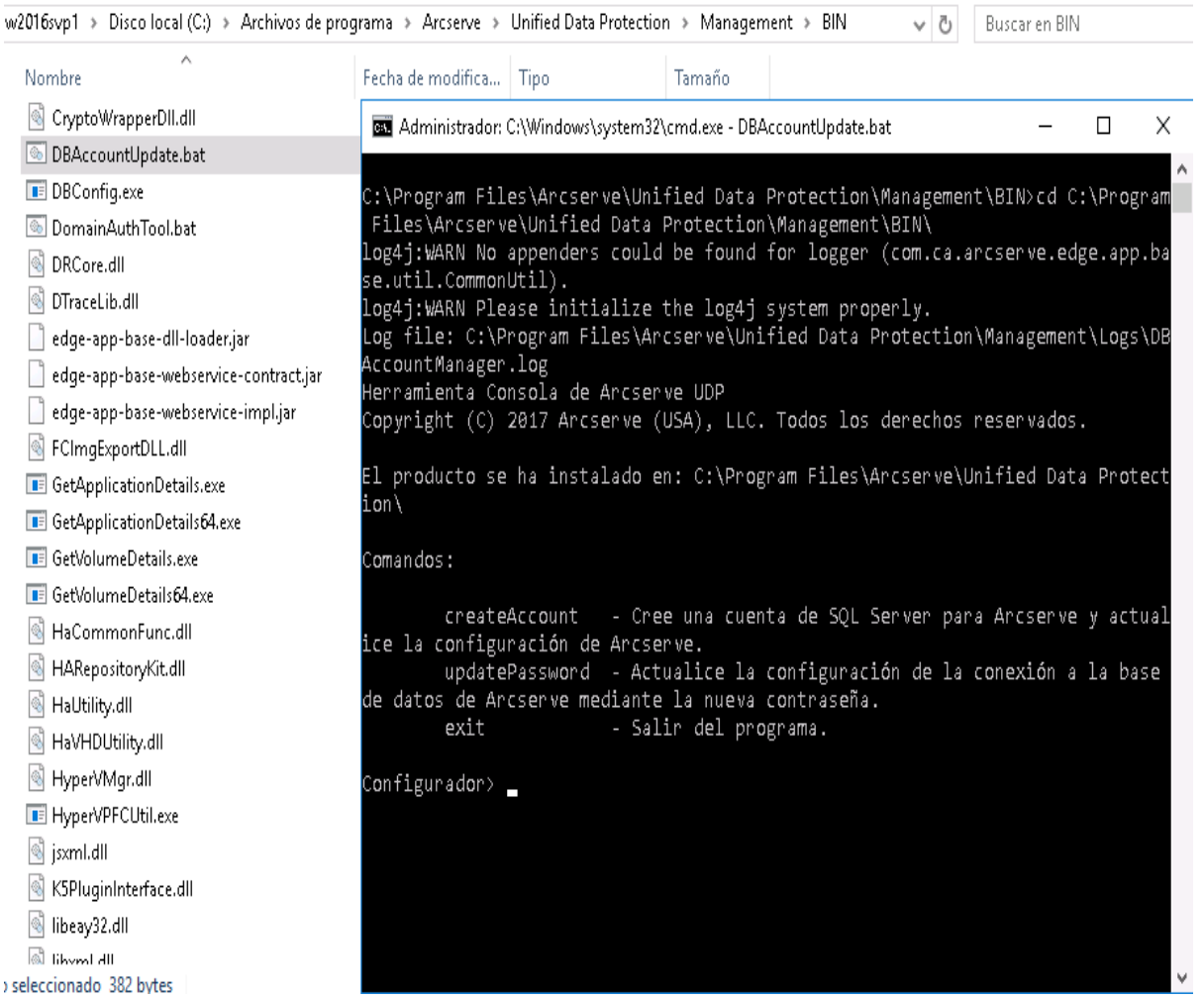
    b. En la interfaz de comandos, escriba *createAccount* y pulse la tecla Intro.

    La interfaz de línea de comandos le pedirá que proporcione una contraseña.

    c. Especifique la contraseña deseada para la cuenta *arcserve_udp* y pulse Intro.

    La Consola de Arcserve UDP crea la cuenta SQL Server llamada *arcserve_udp*.

    d. Escriba *exit* para cerrar la interfaz de línea de comandos.



3. Reinicie el servicio de gestión de Arcserve UDP.

Solución de problemas

La lista siguiente proporciona la posible solución para los errores que pueden aparecer con la Consola de gestión de usuarios:

- **Síntoma**

  Se ha producido un error al iniciar sesión en la consola de gestión de usuarios.

  Solución

  Verifique que se ha iniciado sesión como administrador. Los usuarios que no sean administradores no tienen permiso para acceder a la consola de gestión de usuarios. Compruebe que el nombre de usuario y la contraseña sean correctos.

- **Síntoma**

  Error de autenticación: El usuario no puede iniciar sesión en la consola.

  Solución

  Compruebe si se ha asignado algún rol al usuario. Si no se le asigna ningún rol, un usuario no puede iniciar sesión en la Consola de Arcserve UDP.

- **Síntoma**

  Se ha agotado el tiempo de espera de la consola de gestión de usuarios.

  Solución

  La duración de la sesión en la página de gestión de usuarios es de 15 minutos. Si la consola no detecta ninguna actividad en la página durante 15 minutos, se cierra la sesión del usuario automáticamente.

Capítulo 8: Adición y gestión de nodos de origen

Esta sección incluye los siguientes temas:

Cómo agregar nodos a la consola

Un nodo hace referencia a un equipo de origen físico o virtual en los hipervisores que se desea proteger. Se puede proteger un nodo realizando la copia de seguridad de los datos en un destino. El Arcserve Unified Data Protection permite agregar los tipos de nodo siguientes:

- Windows
- Linux
- Máquinas virtuales en VMware ESX/vCenter y servidores Microsoft Hyper-V

Puede agregar nodos especificando manualmente los detalles de estos, realizando la detección desde un directorio de Active Directory o importando desde un archivo e hipervisores.

Nota: También se pueden agregar nodos durante la creación de un plan.

¿Qué hacer a continuación?

- Revisión de los requisitos previos
- Adición de nodos
- Detección de nodos
- Importación de nodos

Revisión de los requisitos previos

Antes de empezar a agregar un nodo, complete las siguientes tareas de los requisitos previos:

1. Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.
2. Inicie sesión en la Consola.
3. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: Todos los nodos**.
4. En el panel central, haga clic en **Agregar nodos**.

   Se abre el cuadro de diálogo **Agregar nodos a la Consola de Arcserve UDP**.

   El cuadro de diálogo proporciona varias opciones para agregar un nodo.

Adición de nodos

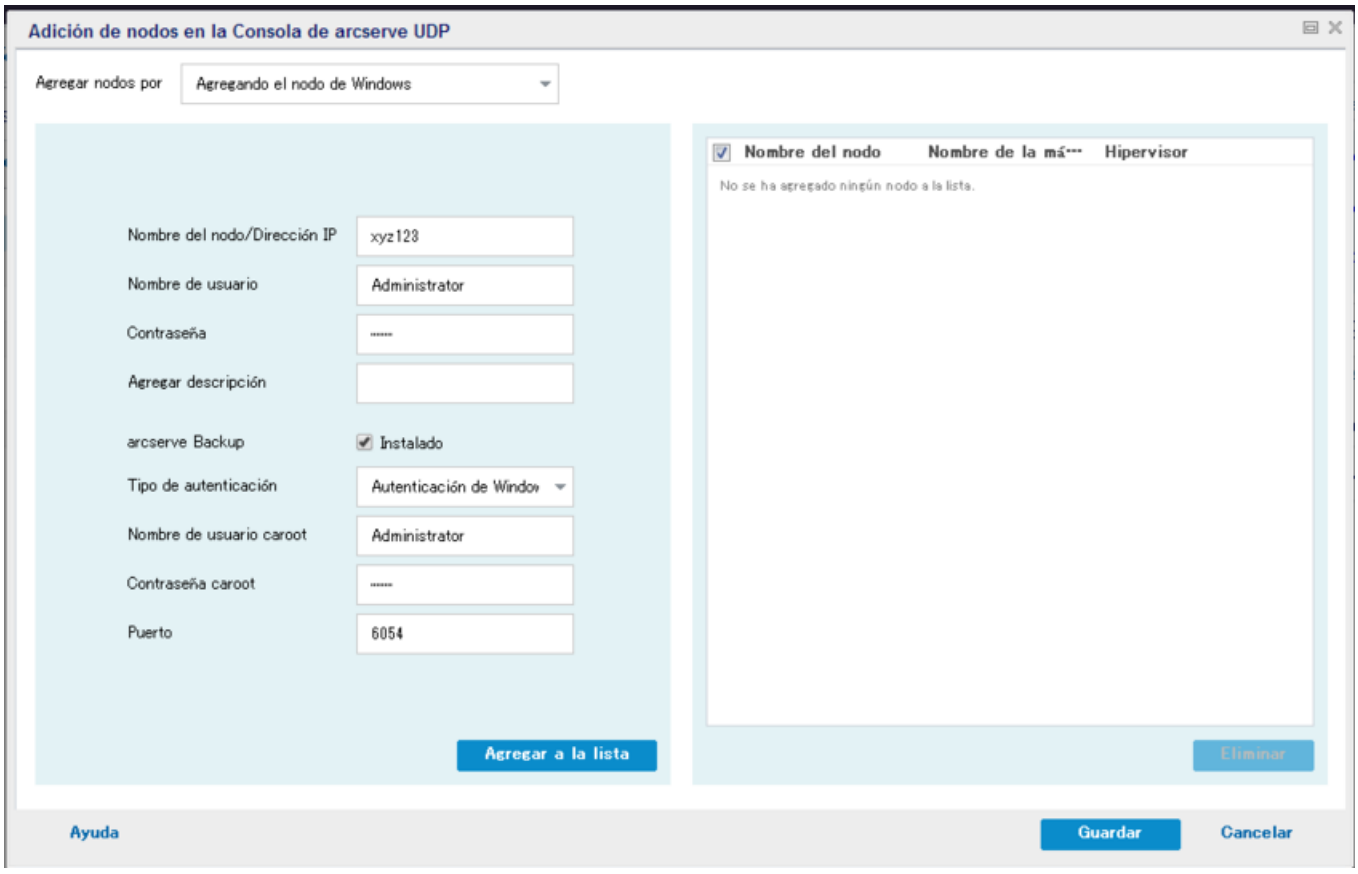
Cuando se tiene la dirección IP o el nombre de un nodo o de un conjunto de nodos, se pueden agregar a la consola especificando los detalles manualmente. Se puede agregar los siguientes tipos de nodos:

- **Windows:** nodos de origen de Windows que se desean proteger. Cuando el nodo de origen de Windows con el puerto de SMB está bloqueado, el Agente de Arcserve UDP (Windows) se instala en este nodo.
- **Linux:** nodos de origen de Linux que se desean proteger. El Agente de Arcserve Unified Data Protection para Linux se instala en el servidor de copia de seguridad de Linux y no en los nodos de origen de Linux.
- **Servidor de copia de seguridad de Linux:** servidor de Linux que gestiona los nodos de origen de Linux. El Agente de Arcserve Unified Data Protection para Linux se instala en este servidor.

Siga estos pasos:

1. En la lista desplegable **Agregar nodos por**, seleccione una de las opciones siguientes:

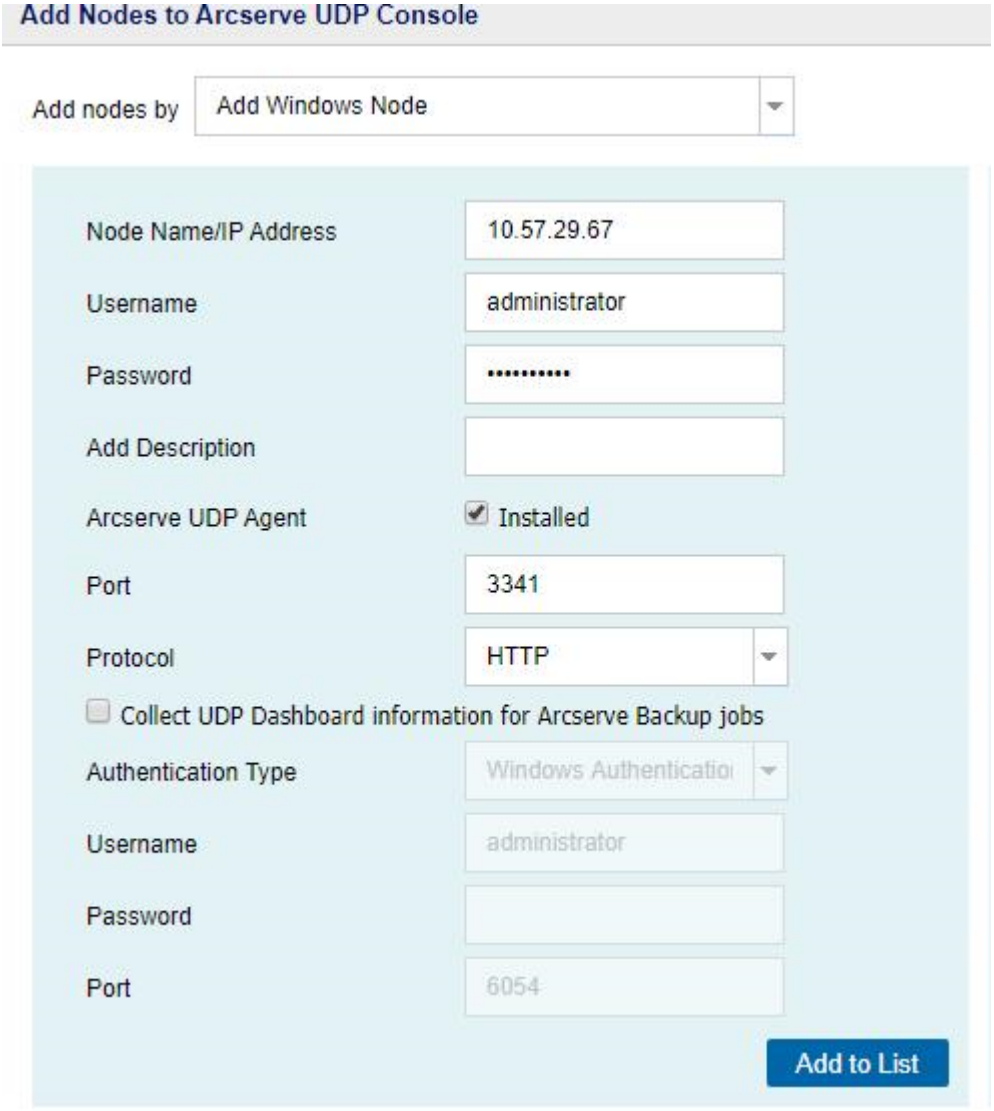
Agregando el nodo de Windows



Nota: Para activar los detalles de Arcserve Backup, seleccione **Instalado**.

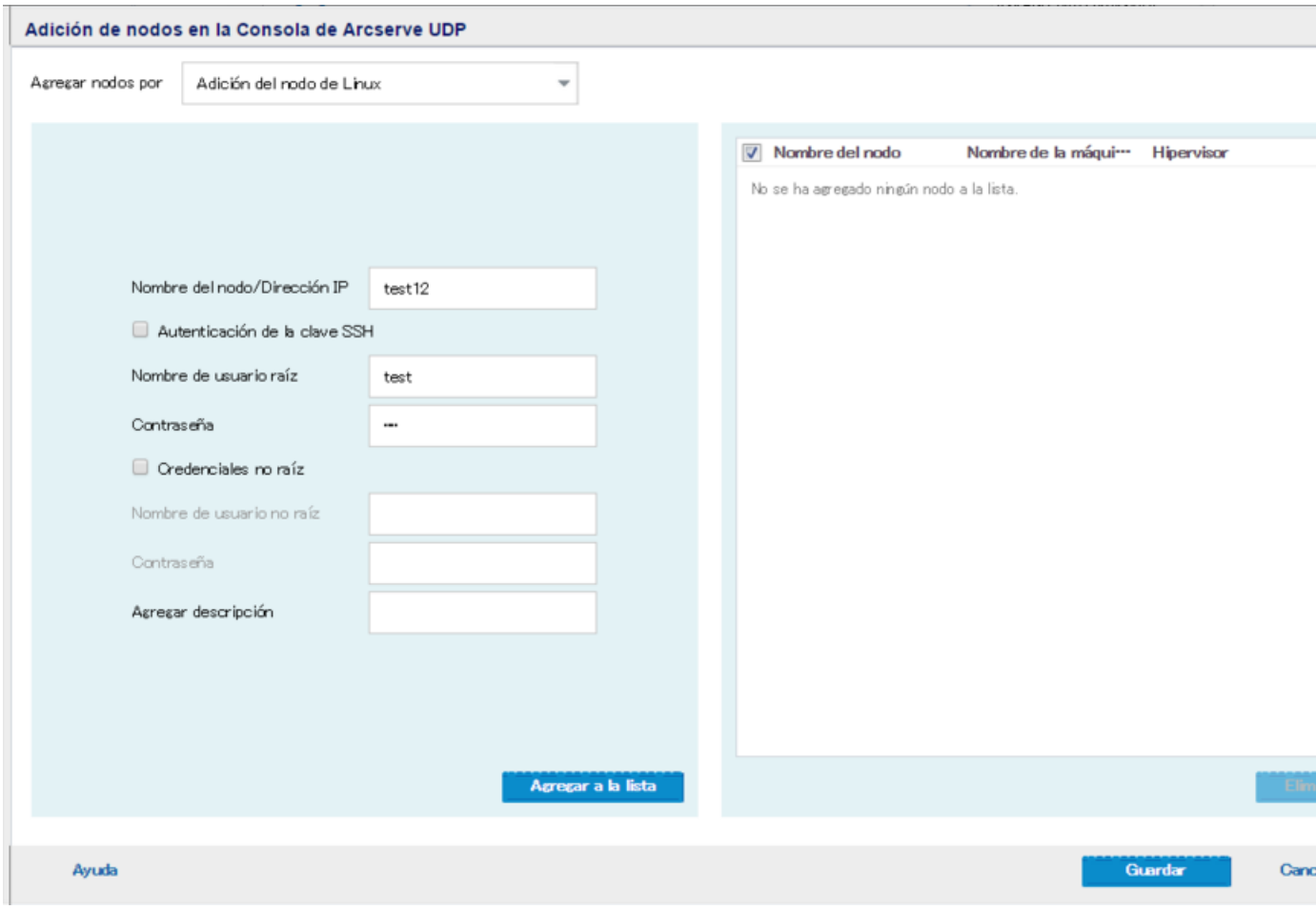
2. Para agregar un nodo bloqueado del puerto de SMB, vaya a la lista desplegable **Agregar nodos por** y seleccione una de las opciones siguientes:

Agregando el nodo de Windows



Nota: Proporcione los detalles del protocolo y del puerto personalizados y, a continuación, seleccione instalado.

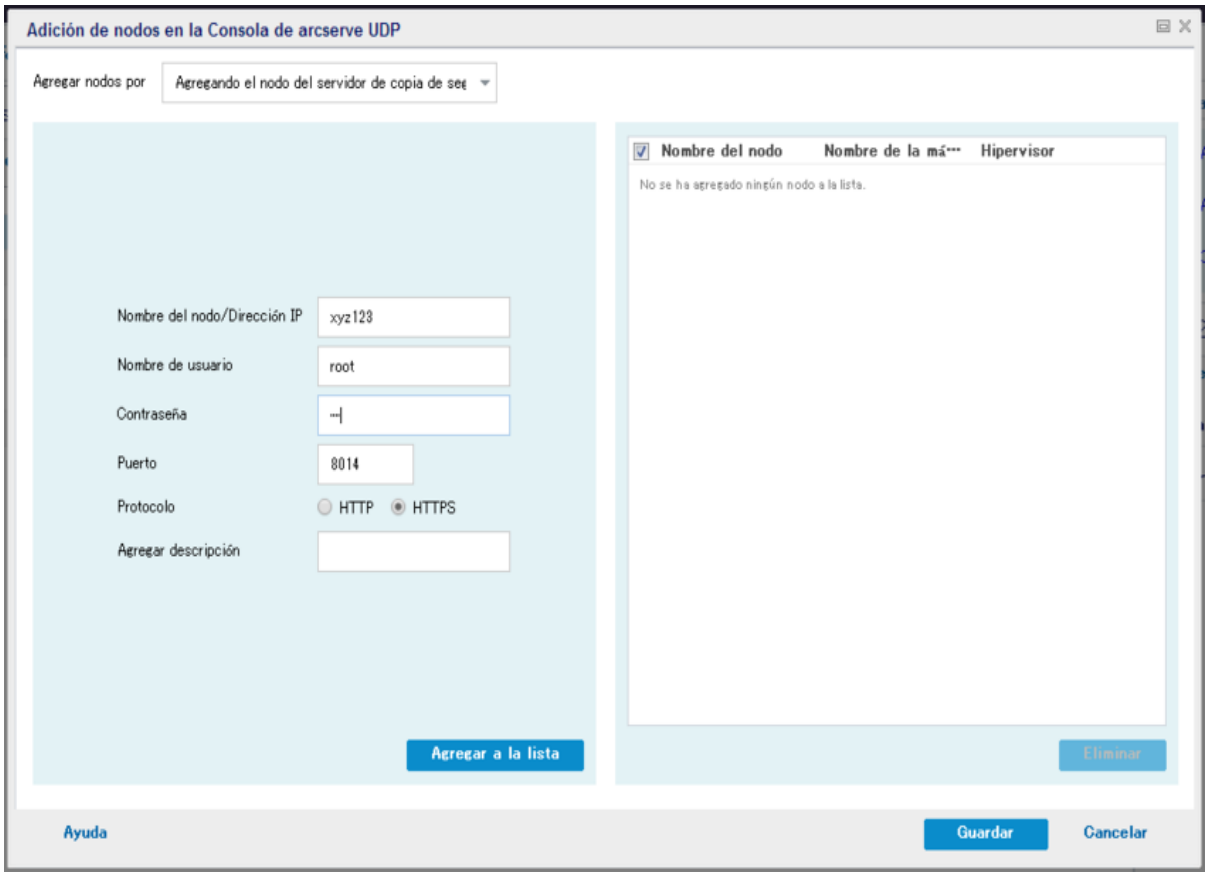
Agregando el nodo de Linux



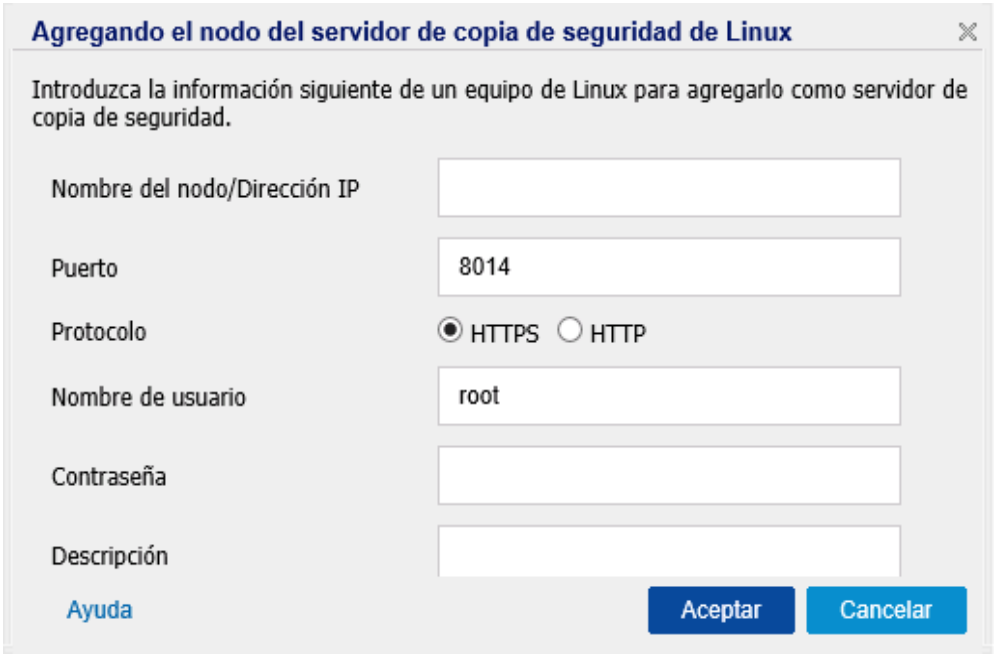
Notas:

- Para Linux, al seleccionar **Autenticación de la clave SSH**, no es necesario introducir los detalles de la contraseña, pero se requiere el nombre de usuario. Para obtener más información sobre cómo configurar la clave SSH, consulte la sección Configurar la autenticación de clave privada y clave pública.
- Antes de agregar un nodo de Linux, se debe agregar un **Servidor de copia de seguridad de Linux** que gestiona los nodos de Linux.
- Para el nodo de Debian Linux, no se admiten credenciales que no son root. Para agregar Debian Linux con usuario no root, utilice sudoers. Para obtener más información sobre cómo configurar Sudo, consulte Configuración de sudo en Debian.
- Cuando se realiza una restauración, solamente se puede iniciar sesión en el servidor de copia de seguridad de Linux desde la Consola de Arcserve UDP.

Agregando el nodo del servidor de copia de seguridad de Linux



El siguiente cuadro de diálogo aparece cuando se agrega el nodo del servidor de copia de seguridad de Linux desde la tarea **Copia de seguridad: Linux, basada en el Agente**:



Se muestran los detalles de la opción seleccionada.

3. Especifique los detalles del nodo y haga clic en **Agregar a lista**.

   El nodo se agrega al panel derecho. Para agregar más nodos, siga los pasos otra vez. Todos los nodos agregados se muestran en el panel derecho.

4. (Opcional) Para eliminar los nodos agregados de la lista situada en el panel derecho, seleccione los nodos y haga clic en **Eliminar**.

5. Seleccione los nodos que se deben agregar y haga clic en **Guardar**.

   Los nodos se agregan y se muestran en la página **Nodos: Todos los nodos**.

   Si el servidor de copia de seguridad de Linux se encuentra en el entorno NAT, realice los pasos siguientes antes de agregarlo a la Consola de Arcserve UDP:

   1. Cree un archivo *server.cfg* en la carpeta del servidor de copia de seguridad de Linux siguiente:

      /opt/Arcserve/d2dserver/configfiles/.

   2. Agregue la siguiente línea al archivo server.cfg:

      nat_enable = true

   3. Reinicie el Agente de Linux utilizando la línea de comandos siguiente:

      /opt/Arcserve/d2dserver/bin/d2dserver restart

   Nota: Si este servidor de copia de seguridad de Linux ya está agregado, actualice el servidor de copia de seguridad de Linux en la Consola de UDP.

Detección de nodos

Para agregar nodos que están en un directorio de Active Directory, se pueden detectar primero los nodos proporcionando los detalles de Active Directory y, a continuación, se pueden agregar los nodos a la consola.

Siga estos pasos:

1. En la lista desplegable **Agregar nodos por**, seleccione **Detección de nodos desde Active Directory**.
2. Especifique las credenciales del usuario y haga clic en **Agregar.**

   Nombre de usuario

   Especifica el dominio y el nombre de usuario con el formato dominio\nombre de usuario.

   Contraseña

   Especifica la contraseña del usuario.

   Filtro de nombre del equipo

   Especifica el filtro para detectar nombres de nodo.

   Después de la validación, el nombre de usuario se agrega a la lista.
3. Seleccione el nombre de usuario agregado y haga clic en **Examinar**.

   La detección correcta del nodo abre el cuadro de diálogo **Confirmar** que pregunta si se desean agregar los nodos del resultado de la **Detección**.

   Nota: El proceso de detección puede tardar un rato dependiendo de factores como la red y el número de equipos en la red.
4. Haga clic en **Sí**.

   Se muestran los nodos detectados.
5. Seleccione el nodo, introduzca el nombre del usuario y la contraseña y, a continuación, haga clic en **Aplicar**.

   Nota: Cuando se hace clic en Aplicar, las credenciales se verifican. Se debe verificar cada nodo antes de agregarlo a la lista.

   Las marcas de verificación verdes se muestran para los nodos verificados.
6. Haga clic en **Agregar a la lista**.

   El nodo seleccionado se muestra en el panel derecho.

7. Para agregar los nodos a la Consola, en el panel derecho seleccione el nodo y haga clic en **Guardar**. Para agregar todos los nodos, seleccione la casilla de verificación **Nombre de nodo**.

   Los nodos verificados se agregan y están disponibles en la página **Nodos: Todos los nodos**.

Solución de problemas: El dominio especificado no existe o no se ha podido establecer la conexión con el mismo

Síntoma

Cuando se agregan nodos al realizar la detección desde Active Directory, se obtiene el siguiente mensaje de error:

El dominio especificado no existe o no se ha podido establecer la conexión con el mismo. Verifique que el servidor de la consola pueda acceder al controlador de dominios a través de la red.

Solución

Se debe comprobar primero la conectividad entre el controlador de dominios y Arcserve UDP. Si la conectividad es correcta, utilice el siguiente comando con el argumento dsgetdc para comprobar si Windows puede encontrar el controlador de dominios en el nombre del dominio:

nltest.exe

Por ejemplo, nltest /dsgetdc:sample_domain, donde sample_domain es el nombre del dominio.

Si se produce un error en el comando, puede haber un problema de DNS en el entorno.

Nota: Se debe ejecutar el comando anterior en el equipo UDP. Para obtener más detalles, consulte el artículo de Microsoft.

Importación de nodos

Arcserve Unified Data Protection permite agregar varios nodos físicos y virtuales mediante el método de importación. En función del requisito, se puede utilizar uno de los siguientes métodos de importación:

- Importación de nodos desde un archivo CSV o TXT
- Importación de nodos desde el servidor de vCenter/ESX
- Importación de nodos desde el servidor Hyper-V

Importación de nodos desde el servidor vCenter/ESX

Mediante este método de importación, se pueden importar nodos de máquina virtual desde el servidor ESX o vCenter. Esta opción enumera todas las máquinas virtuales detectadas en el servidor especificado, incluso si Arcserve Unified Data Protection ya la gestiona.

Siga estos pasos:

1. En la lista desplegable **Agregar nodos por**, seleccione la opción **Importación desde vCenter/ESX**.
2. Especifique los detalles del servidor vCenter o ESX y haga clic en **Conectar**.

   En el panel izquierdo, se muestra un árbol de nodos.

   Nota: VMware Virtual Disk Development Kit (VDDK) 6.x.x está incluido en el paquete de Arcserve UDP versión 7.0, pero VDDK 6.x.x no es compatible con HTTP. Además, vCenter y ESX normalmente son compatibles con la conexión HTTPS solo de forma predeterminada. Seleccione HTTPS, a menos que se reemplace manualmente la versión integrada de VDDK 6.x.x por otra versión de VDDK y que se configure manualmente vCenter/ESX para permitir la conexión HTTP.
3. Expanda el árbol de nodos.

   (Opcional) Se puede escribir el nombre de nodo en el campo de filtro para encontrar el nodo en el árbol.
4. Seleccione los nodos que se desean migrar.

   Nota: Arcserve UDP le permite realizar las siguientes opciones:

   - Agregar y proteger los objetos del contenedor en la infraestructura de vSphere (como el centro de datos y la agrupación de recursos).
   - Agregue y proteja la plantilla de máquina virtual y proteja la máquina virtual por etiqueta.

   Sin embargo, actualmente se puede realizar esta acción mediante el asistente del plan. Para obtener más detalles, consulte *Adición de nodos desde vCenter/ESX* en la Especificación del origen detema.
5. Seleccione la casilla de verificación **Proporcione credenciales para los nodos seleccionados** y proporcione las credenciales de usuario.

   Nota: Las credenciales de usuario son necesarias para las funciones, tales como, la comprobación previa (PFC), el truncamiento del registro de aplicaciones y los comandos previos o posteriores a la copia de seguridad.
6. Haga clic en **Agregar a la lista**.

Los nodos seleccionados se agregan al panel derecho.

7. Seleccione los nodos y haga clic en **Guardar**.

   Los nodos se agregan y se muestran en la página **Nodos: Todos los nodos**.

Importación de nodos desde el servidor Hyper-V

Mediante este método de importación se pueden importar los nodos de máquina virtual desde los servidores de Microsoft Hyper-V.

Siga estos pasos:

1. En la lista desplegable **Agregar por nodos**, seleccione **Importación desde Hyper-V**.
2. Rellene los campos siguientes y haga clic en **Conectar**.

   Hyper-V

   Especifica el nombre del servidor Hyper-V o la dirección IP. Para importar las máquinas virtuales que se encuentran en clústeres de Hyper-V, especifique el nombre de nodo del clúster o el nombre de host de Hyper-V.

   Nombre de usuario

   Especifica el nombre de usuario de Hyper-V que tiene los derechos de administrador.

   Nota: Para los clústeres de Hyper-V, utilice una cuenta de dominio con privilegios administrativos del clúster. Para los hosts de Hyper-V independientes, se recomienda utilizar una cuenta de dominio.

   Contraseña

   Especifica la contraseña del nombre de usuario.

   La solución Arcserve Unified Data Protection busca y muestra un árbol de nodos en el panel izquierdo.
3. Expanda el árbol de nodos.

   (Opcional) Se puede escribir el nombre de nodo en el campo de filtro para encontrar el nodo en el árbol.

   Nota: Las máquinas virtuales configuradas como rol de clúster aparecen directamente en el nombre de nodo del clúster situado en el árbol. Las máquinas virtuales que no forman parte del clúster aparecerán situadas en el nombre de host del host individual de Hyper-V.
4. Seleccione los nodos que se desean migrar.
5. Seleccione la casilla de verificación **Proporcione credenciales para los nodos seleccionados** y proporcione las credenciales de usuario.

   Nota: Las credenciales de usuario son necesarias para las funciones, tales como, la comprobación previa (PFC), el truncamiento del registro de aplicaciones y los comandos previos o posteriores a la copia de seguridad. Sin credenciales de

usuario, se produce un error en la comprobación previa para los nodos seleccionados.

6. Haga clic en **Agregar a la lista**.

   Los nodos seleccionados se agregan al panel derecho.

7. Seleccione los nodos y haga clic en **Guardar**.

   Los nodos se agregan y se muestran en la página **Nodos: Todos los nodos**.

Importación de la máquina virtual utilizando una cuenta administrativa adicional

La cuenta administrativa adicional hace referencia a esas cuentas que no son administradores predeterminados. También se hace referencia a tales cuentas como cuentas administrativas no integradas. Para importar una máquina virtual de un host de Hyper-V, utilice la cuenta del administrador integrada del host de Hyper-V o una cuenta del dominio que está en el grupo de administradores local del host de Hyper-V o un usuario administrativo no integrado.

El usuario con la cuenta administrativa adicional puede utilizar los procedimientos que se mencionan a continuación para desactivar el acceso remoto del UAC.

Notas:

- Este procedimiento no es similar a la desactivación del UAC. Mediante este procedimiento se pueden desactivar algunas de las funciones del UAC.
- Considerando que se utiliza la tecnología del servicio remoto de Windows Management Instrumentation (WMI) para importar, compruebe que el cortafuegos no bloquea WMI.

Siga estos pasos:

1. Haga clic en Inicio, escriba regedit en el campo Buscar programas y archivos, y pulse Intro.

   Se abre el Editor del registro de Windows.

   Nota: Puede ser necesario proporcionar credenciales administrativas para poder abrir el Editor del registro de Windows.

2. Busque y haga clic en la clave de registro siguiente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. Desde el menú Editar, haga clic en Nuevo y después en Valor de DWORD (32 bits).
4. Especifique LocalAccountTokenFilterPolicy como el nombre de la nueva entrada y, a continuación, pulse Intro.
5. Haga clic con el botón secundario del ratón en LocalAccountTokenFilterPolicy y, a continuación, haga clic en Modificar.
6. Especifique 1 en el campo de datos Valores y, a continuación, haga clic en Aceptar.
7. Salga del Editor del registro.

   Para obtener más información sobre el comportamiento de Windows, consulte la documentación de Microsoft.

Importación de nodos desde un archivo CSV o TXT

Cuando se tienen varios nodos físicos que se deben agregar, en lugar de agregar un nodo por vez, se puede crear un archivo .csv o .txt con el formato <NombreNodo>, <NombreUsuario>, <Contraseña>. Posteriormente, se puede seleccionar e importar el archivo .txt o .csv a la Consola utilizando las opciones de exploración y carga.

Siga estos pasos:

1. En la lista desplegable **Acciones**, seleccione **Importar**.
2. Haga clic en **Examinar** para seleccionar el archivo guardado en formato .txt o .csv.
3. Haga clic en **Cargar**.

   Los nodos se agregan y se muestran en la página **Nodos: Todos los nodos**.

Cómo gestionar nodos

Al utilizar Arcserve UDP se podrán realizar varias acciones para gestionar un nodo como, por ejemplo, actualizar el nodo y el hipervisor, exportar nodos, suprimir nodos y realizar comprobaciones previas.

¿Qué hacer a continuación?

- Revisión de los requisitos previos
- Actualización de la información del hipervisor
- Especificación del hipervisor
- Actualización de la información de la máquina virtual
- Actualización de nodos
- Exportación de nodos
- Pausa de un nodo
- Reanudación de un nodo
- Sincronizar datos
- Supresión de nodos desde la consola
- Implementación del Agente en los nodos
- Realización de comprobaciones previas a las tareas de copia de seguridad

Revisión de los requisitos previos

Antes de empezar a gestionar los nodos, complete los requisitos previos siguientes:

- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.
- Inicie sesión en la Consola.
- Adición de un nodo

Actualización de la información del hipervisor

Después de agregar un nodo de máquina virtual en Arcserve Unified Data Protection, es posible que la información relacionada con la conexión, como el nombre de host o las credenciales del hipervisor de la máquina virtual, cambie. En tal caso, Arcserve Unified Data Protection permite actualizar la información del hipervisor.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. Haga clic con el botón secundario del ratón en el grupo de nodos bajo **Grupos de vCenter/ESX** o **Grupos de Hyper-V**.
3. Haga clic en **Actualizar vCenter/ESX** o en **Actualizar Hyper-V.**

   Se muestra el cuadro de diálogo **Actualizar vCenter/ESX** o **Actualizar Hyper-V**.
4. Introduzca los nuevos detalles en el cuadro de diálogo y haga clic en **Aceptar**.

   Se cierra el cuadro de diálogo **Actualizar vCenter/ESX** o **Actualizar Hyper-V**.

   La información del hipervisor se actualiza correctamente.

Especificación del hipervisor

Especifique los detalles del hipervisor para evitar utilizar una licencia extra mientras se protege una máquina virtual. Cuando se protege una máquina virtual mediante un plan de la copia de seguridad sin agente basada en el host, la licencia del host del hipervisor se utiliza para proteger la máquina virtual. No es necesario instalar ningún agente en la máquina virtual. En ciertos casos, se puede decidir instalar el agente en la máquina virtual y crear un plan de la copia de seguridad basada en el agente para proteger la máquina virtual. En tales casos, la máquina virtual utiliza otra licencia distinta de la licencia del host del hipervisor. Especifique los detalles del hipervisor en tales casos y la máquina virtual utiliza la licencia del host del hipervisor en vez de utilizar otra licencia.

Ejemplos que describen cuándo se debe especificar la información del hipervisor:

- Se tiene un plan de la copia de seguridad sin agente basada en el host para proteger las máquinas virtuales de un servidor de ESX o Hyper-V. El plan utiliza la licencia del hipervisor para proteger la máquina virtual. Ahora se instala el Agente de UDP en una máquina virtual del hipervisor especificado y se crea un plan basado en el agente para proteger la máquina virtual. Normalmente el plan utiliza una licencia extra para proteger la máquina virtual. Si se especifica el hipervisor para la máquina virtual, el plan utiliza la licencia del hipervisor.
- Se tiene un plan de Linux basado en el agente para proteger los nodos del Agente de máquina virtual de Linux. Si se especifica el hipervisor para la máquina virtual, todas las máquinas virtuales en el mismo hipervisor comparten la licencia del hipervisor.

Tenga en cuenta los puntos siguientes antes de especificar el hipervisor:

- No se puede especificar el hipervisor para un nodo físico.
- No se puede especificar el hipervisor para un nodo de máquina virtual que se importa desde vCenter/ESX o Hyper-V.
- Se puede especificar el hipervisor para varias máquinas virtuales, que pertenecen al mismo hipervisor, al mismo tiempo.
- Verifique que las últimas herramientas de VMware o el servicio de integración de Hyper-V estén instalados y que la máquina virtual esté encendida. También, verifique que el servicio Windows Management Instrumentation (WMI) esté en la lista de excepción del cortafuegos en el nodo del Agente de máquina virtual.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

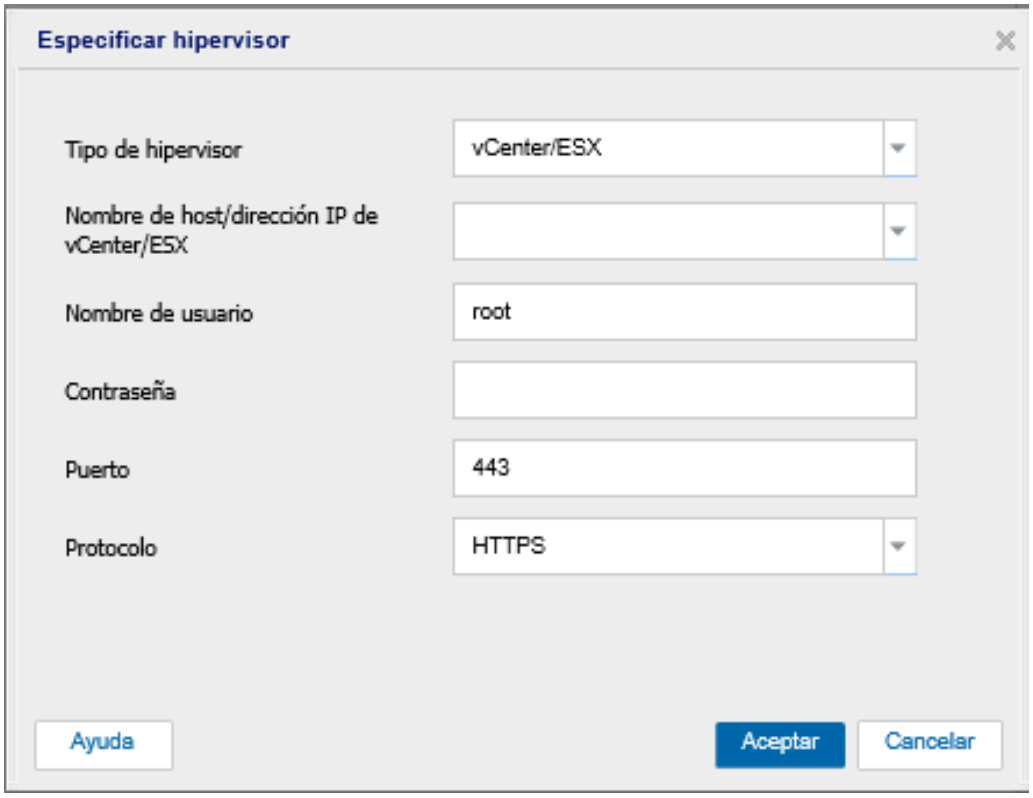
Se mostrará la página **Nodos: Todos los nodos**.

3. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en el nombre del nodo.
   - Seleccione el nombre de nodo y en el panel central haga clic en la lista desplegable **Acciones**.

   Aparecerá una lista de opciones.

4. Haga clic en **Especificar hipervisor**.

   Se abre el cuadro de diálogo Especificar hipervisor. El **Tipo de hipervisor** puede ser **Hyper-V**, **vCenter/ESX** y **Otro** (Xen, la máquina virtual basada en el kernel, Red Hat Enterprise Virtualization).



5. Introduzca los detalles del hipervisor y haga clic en **Aceptar.**

   La información del hipervisor se ha especificado.

Actualización de la información de la máquina virtual

Arcserve Unified Data Protection permite actualizar algunas de las propiedades de los nodos de la máquina virtual desde los hipervisores. Se puede activar la actualización manual o automáticamente. Las propiedades siguientes de los nodos de la máquina virtual se actualizan y se sincronizan con sus correspondientes máquinas virtuales en el hipervisor:

- Nombre de nodo
- Nombre de máquina virtual
- OS

Para activar manualmente la actualización, utilice la opción **Actualizar la información de la máquina virtual**.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: todos los nodos**.

2. En el panel central, haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Actualizar la información de la máquina virtual**.

   El cuadro de diálogo **Actualizar la información de la máquina virtual** se abre.

3. Haga clic en **Aceptar**.

   Se ha activado una detección manual y se han actualizado los nodos de la máquina virtual.

   La función de actualización automática se activa automáticamente cuando se realizan las acciones siguientes:

   - Abrir la ficha **recurso** en la consola.
   - Enviar un informe programado.

   Nota: Aunque active varias actualizaciones automáticas, solamente se ejecuta una actualización automática a la vez. Las actualizaciones automáticas restantes se ponen en una cola.

Actualización de nodos

Se puede actualizar la información relacionada con los nodos existentes. Se puede actualizar el nodo en cualquier momento. Se muestran a continuación algunas de las situaciones en las que es necesario actualizar un nodo:

- Se ha instalado un nuevo producto en el nodo después de que el nodo se registrara en Arcserve Unified Data Protection.
- El nombre de usuario o la contraseña del nodo se ha actualizado después de que el nodo se registrara en Arcserve Unified Data Protection.

Nota: Si un nodo sirve tanto de servidor de punto de recuperación como de agente y se cambian las credenciales o el protocolo de ese nodo, actualice el nodo desde la página **Destinos: servidor de punto de recuperación.** El plan se implementará automáticamente en el agente después de actualizar el servidor de punto de recuperación. Si se actualiza el nodo desde la página **Nodos: Todos los nodos**, los planes que implican esos nodos no se implementarán correctamente. Para implementar el plan, actualice otra vez el nodo desde la página **Destinos: servidor de punto de recuperación**.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: Todos los nodos**.

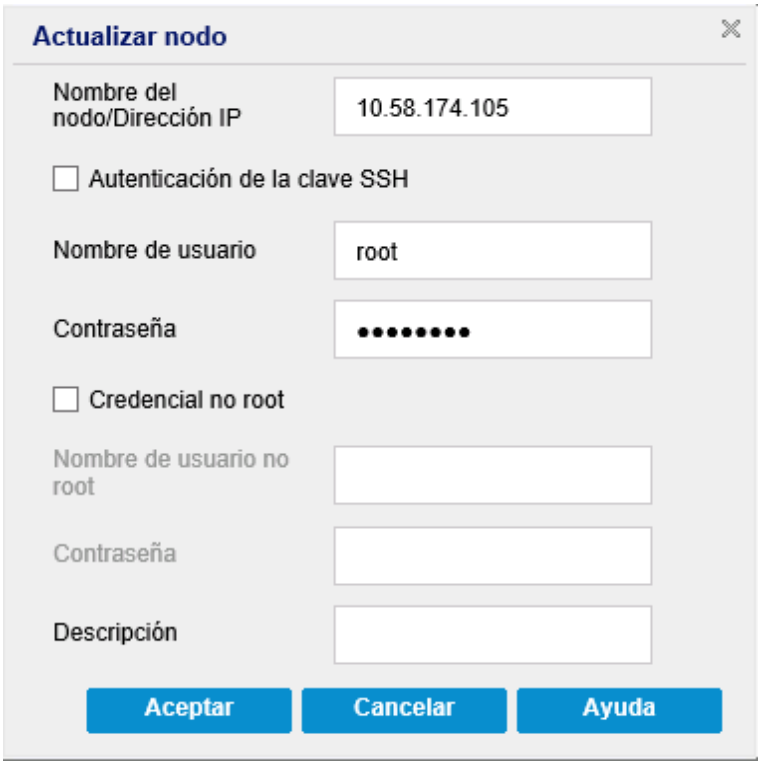
2. Realice una de las acciones siguientes:

   - Haga clic con el botón secundario del ratón en el nombre del nodo.
   - Seleccione el nombre de nodo y en el panel central haga clic en la lista desplegable **Acciones**.

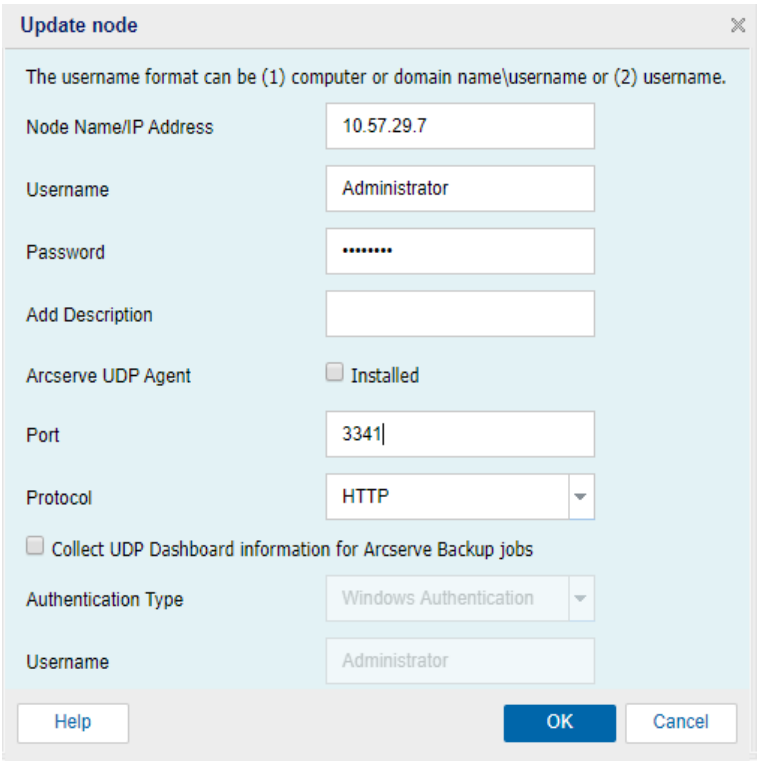
3. Haga clic en **Actualizar**.

   Se abrirá el cuadro de diálogo **Actualizar nodo**.

   El cuadro de diálogo siguiente se refiere a los nodos de Linux:



Aparece el cuadro de diálogo siguiente para el nodo de Windows (cuando se ha bloqueado el puerto de SMB) con un puerto personalizado:



4. Actualice los detalles y haga clic en **Aceptar**.

   Se actualizará la información del nodo.

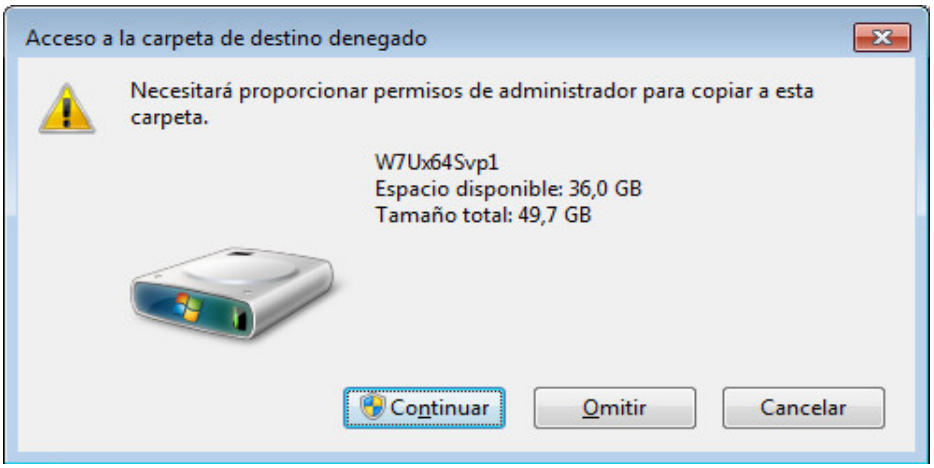
Actualización de los nodos utilizando una cuenta administrativa adicional

Una cuenta administrativa adicional hace referencia a esas cuentas que no están utilizando administradores predeterminados. También se hace referencia a tales cuentas como cuentas administrativas no integradas. Las funciones Actualización de nodos y Comprobación previa (PFC) utilizan la cuenta especificada en Actualización de nodos para conectarse a una máquina virtual y realizar comprobaciones relacionadas.

Nota: Se debe utilizar el administrador integrado o la cuenta del administrador de dominios integrada al realizar la función Actualización de nodos. Si es necesario, se puede utilizar un administrador no integrado, pero antes de hacerlo se deberá verificar que la cuenta que se está utilizando tiene los permisos de administrador obligatorios.

Siga estos pasos:

1. Verifique que se puede acceder a \\[nombre de host de la máquina virtual]\ADMIN$ utilizando la cuenta de administrador adicional de otro equipo. Si se tiene cualquier problema, verifique si el servicio Compartir archivos e impresoras está bloqueado por el cortafuegos. Si los valores de configuración del cortafuegos son correctos, es posible que sea necesario desactivar el acceso remoto del UAC. Para desactivar el acceso remoto del UAC, consulte Importación de la máquina virtual utilizando una cuenta administrativa adicional.
2. En VMware, cuando se actualizan nodos, Arcserve UDP automáticamente instala algunas herramientas en la máquina virtual para realizar la comprobación previa. Para verificar que la cuenta tiene los permisos obligatorios, realice lo siguiente:
    a. Inicie sesión en la máquina virtual mediante la cuenta de administrador no integrada.
    b. Copie un archivo de C:\Windows a C:\ y garantice que el mensaje siguiente no aparece:



c. Si se experimenta cualquier problema, se pueden modificar los valores de configuración del Control de cuentas de usuario (UAC). Para modificarlos, desactive **Ejecutar todos los administradores en Modo de aprobación de administrador** en la Política de seguridad local cambiando los valores de configuración del UAC en secpol.msc -> Políticas locales -> Opciones de seguridad. (Secpol.msc es el editor de políticas de seguridad de Microsoft).

Nota: No intente desactivar el UAC en el cuadro de diálogo Configuración del Control de cuentas de usuario que se abre desde el Panel de control.

Para obtener más información sobre cómo cambiar los valores de configuración del UAC, consulte la documentación de Microsoft correspondiente.

3. Para las máquinas virtuales de Hyper-V, la cuenta de administrador adicional debe tener permisos similares a los mencionados en Importación de la máquina virtual utilizando una cuenta administrativa adicional.

Exportación de nodos

Se pueden exportar los nodos como archivo ZIP (.zip). Cuando sea necesario, se puede importar el archivo ZIP para retener los nodos. Por ejemplo, exportar los nodos antes de las actualizaciones o volver a arrancar le ayuda a importar el mismo conjunto de nodos.

Se pueden exportar solamente aquellos nodos que tengan credenciales válidas y que estén ejecutando el sistema operativo de Windows.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: todos los nodos**.

2. Seleccione un nodo.
3. En el panel central, haga clic en la lista desplegable **Acciones** y haga clic en **Exportar**.

   Se abre un cuadro de diálogo en el que se solicita su acción en el archivo list.zip.

4. Haga clic en **Abrir** o en **Guardar**.

   La lista de nodos se exporta.

Pausa de nodos

Arcserve UDP permite pausar solamente los nodos seleccionados en lugar del plan completo. Para impedir que se ejecute una tarea programada, ahora ya no es necesario pausar y reanudar el plan completo, lo cual detenía todos los nodos asociados.

Importante: La función de pausa de nodos solamente funciona si el nodo está asociado a un plan de Windows basado en agente o a un plan sin agente basado en host. No se pueden pausar los nodos del resto de planes.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: Todos los nodos**.

2. Seleccione el nodo o nodos asociados a un plan que desee.

3. En el panel central, haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Pausar**.

   Aparece un cuadro de diálogo de confirmación en el que se informa de que solamente se pueden ejecutar tareas manuales para los nodos que están en pausa.

4. Haga clic en **Sí**.

   Se pausan los nodos. Si se produce un error en cualquier nodo al hacer una pausa, aparece un mensaje aparece con el motivo.

Reanudación de un nodo

Arcserve UDP permite reanudar nodos pausados. Ahora, en lugar de pausar y reanudar un plan, se pueden pausar y reanudar uno o varios nodos específicos asociados al plan.

Importante: La función de pausa y reanudación de nodos solo funciona si el nodo está asociado a un plan de Windows basado en el agente o a un plan sin agente basado en el host. No se pueden pausar o reanudar los nodos del resto de planes.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: Todos los nodos**.

2. Seleccione uno o varios nodos pausados.

3. En el panel central, haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Reanudar**.

   Se abrirá un cuadro de diálogo en el que se le solicitará que confirme la acción.

4. Haga clic en **Sí**.

   El nodo empieza a ejecutarse de nuevo.

Sincronizar datos

La sincronización de datos permite que los datos se mantengan consistentes y actualizados, incluso si están en bases de datos diferentes.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Se mostrará la página **Nodos: todos los nodos**.
3. (A nivel de grupo) Seleccione uno de los grupos de nodos que se muestran en el panel izquierdo y haga clic con el botón secundario del ratón.
4. Haga clic en una de las opciones siguientes:

   Nota: Únicamente se muestran las opciones agregadas para la sincronización con Arcserve Unified Data Protection.

   - Sincronización completa de Arcserve Backup
   - Sincronización incremental de Arcserve Backup

   El cuadro de diálogo **Información** explica que el método de sincronización seleccionado se ha enviado.

Supresión de nodos desde la consola

Arcserve Unified Data Protection incluye una opción que permite suprimir nodos. Si se suprimen los nodos, también se suprimirán los registros y los historiales de tareas asociados. Se puede agregar el nodo suprimido más tarde si fuese necesario.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: todos los nodos**.

2. Seleccione un nodo que se desea suprimir.
3. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en el nombre del nodo.
   - Seleccione el nombre de nodo y en el panel central haga clic en la lista desplegable **Acciones**.
4. Haga clic en **Suprimir**.

   Se abre el cuadro de diálogo **Confirmar**.

5. Haga clic en **Sí**.

   El nodo se suprime de la Consola.

Implementación del Agente en los nodos

Para actualizar o instalar el Agente de Arcserve Unified Data Protection para un nodo, utilice la opción **Instalar o actualizar agente**. Si el equipo de destino contiene una versión anterior del Agente de Arcserve Unified Data Protection, utilice la opción de actualización para obtener la última versión. De lo contrario, utilice la opción de instalación.

Nota: Se pueden implementar agentes de Arcserve Unified Data Protection en varios nodos. Al mismo tiempo se pueden ejecutar solamente 16 tareas de implementación. Si hay más de 16 tareas, otras tareas se mantienen a la espera y solo se ejecutan cuando alguna de las 16 tareas de implementación predeterminadas se completa. Para modificar el número máximo de tareas, actualice la siguiente clave del registro:

deployMaxThreadCount

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: todos los nodos**.

2. Seleccione uno o más nodos.

3. En el panel central, haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Instalar/actualizar agente**.

   Los detalles de la instalación o actualización se muestran por encima del nombre del nodo en el panel central.

4. Verifique los detalles.

5. Especifique la programación de instalación/actualización y haga clic en **Aceptar**.

   El nodo se actualiza o instala con la última versión del Agente de Arcserve Unified Data Protection.

   Nota: Se puede cancelar una implementación del agente si se programa para un momento posterior. Para cancelar una implementación del agente, seleccione el Agente y haga clic en **Acciones, Cancelar implementación del agente.**

Realización de comprobaciones previas a las tareas de copia de seguridad

La solución Arcserve Unified Data Protection proporciona una utilidad denominada Comprobación previa (PFC) que permite ejecutar comprobaciones vitales en nodos específicos para detectar condiciones que pueden causar errores en las tareas de copia de seguridad. La comprobación previa solo se aplica a nodos de máquina virtual que se importan desde vCenter/ESX, Hyper-V o Nutanix AHV. La comprobación previa no funciona para la plantilla de máquina virtual de VMware. PFC se ejecuta automáticamente cuando se realizan las siguientes acciones:

- Importar máquinas virtuales desde un sistema de servidor de vCenter/ESX, Hyper-V o Nutanix AHV
- Permitir que una tarea de copia de seguridad se ejecute.

Otras referencias:

- Soluciones para elementos de comprobación previa de las máquinas virtuales de VMware
- Soluciones para elementos de comprobación previa de las máquinas virtuales de Hyper-V
- Soluciones para elementos de comprobación previa de las máquinas virtuales de Nutanix AHV

Además, también se puede realizar una comprobación previa de forma manual.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Se muestra la página **Todos los nodos: Nodo** en el panel central.
3. Haga clic con el botón secundario del ratón en el nombre de un nodo y haga clic en **Comprobación previa**.

   Nota: Se puede realizar también una **Comprobación previa** mediante una de las opciones siguientes:

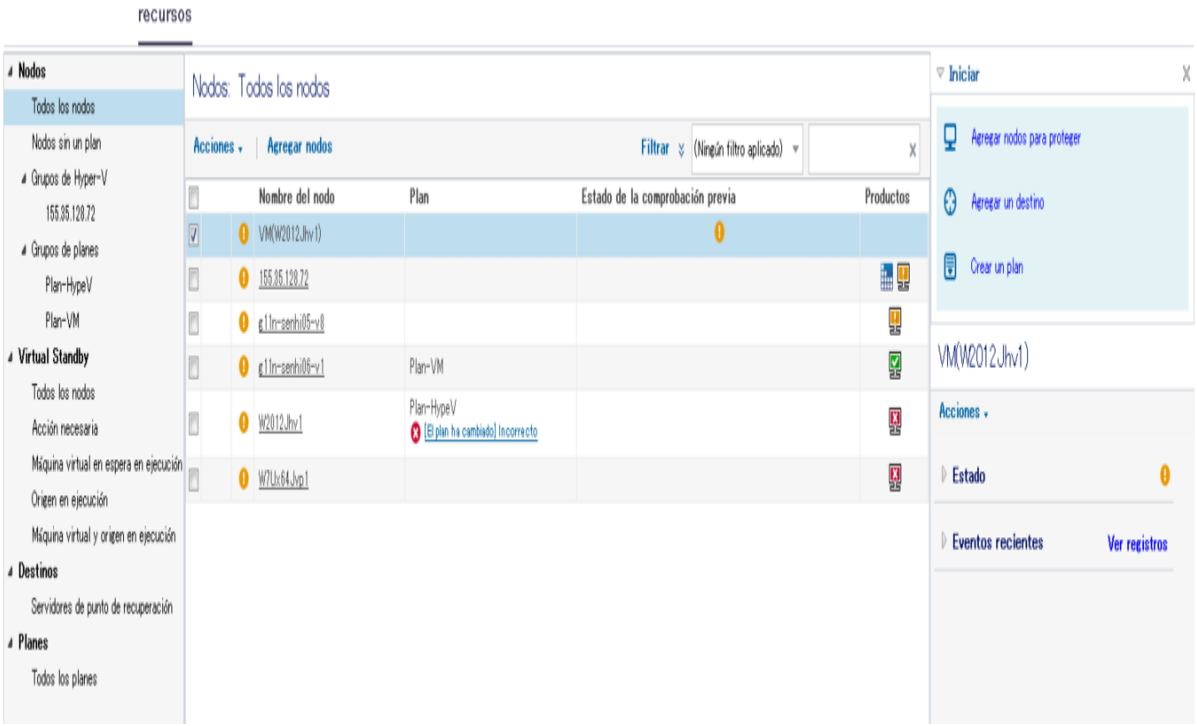
   - (A nivel de nodo) Seleccione las casillas de verificación de los nodos en los cuales se desea ejecutar una comprobación previa y, a continuación, haga clic en **Acciones** y seleccione **Comprobación previa**.
   - (A nivel de grupo) Haga clic con el botón secundario del ratón en el grupo que contiene los nodos y haga clic en **Comprobación previa**.

Se muestra el siguiente mensaje: **Iniciando la comprobación previa de la máquina virtual**.

4. Vaya a la columna **Estado de la comprobación previa** para ver el estado de la comprobación previa.

   Nota: De forma predeterminada, la columna Estado de la comprobación previa no es visible en la interfaz de usuario. Es necesario activar manualmente la columna Estado de la comprobación previa en la interfaz de usuario.

   Se puede ver también el estado de la comprobación previa haciendo clic en **Ver registros** en el panel derecho.



La tabla siguiente describe las comprobaciones que realiza la comprobación previa para la máquina virtual de VMware:

Elemento	Descripción
Seguimiento de bloque modificado (CBT)	Una función que realiza seguimientos de sectores de disco que se encuentran en una máquina virtual que ha cambiado. Esto ayuda a minimizar el tamaño de las copias de seguridad. Este elemento verifica que CBT está activado.
Herramientas de VMware	Este elemento verifica que las herramientas de VMware Tools están instaladas en cada máquina virtual.
Disco	Este elemento verifica los discos de la máquina virtual.
Estado de potencia	Este elemento verifica que la máquina virtual está encendida.

Coherencia de datos	Este elemento verifica si la instantánea coherente con la aplicación se puede tomar para la máquina virtual.
Servidor ESX	Este elemento verifica si un servidor puede detectar la máquina virtual. La opción solo es visible cuando el nodo no está disponible en ESX.

La tabla siguiente describe las comprobaciones que realiza la comprobación previa para la máquina virtual de Hyper-V:

Elemento	Descripción
Credenciales de Hyper-V	Las necesidades del producto para implementar una utilidad de copia de seguridad y una utilidad de seguimiento de bloques del cambio en servidor Hyper-V a través del recurso compartido ADMIN$ del sistema. La acción ayuda a verificar si el producto tiene los permisos necesarios para el recurso compartido. Se produce un error en la tarea de copia de seguridad/restauración si las credenciales de Hyper-V no son correctas o si el administrador cierra el recurso compartido ADMIN$.
Servicios de integración	Este elemento verifica que los servicios de integración de Hyper-V Tools están instalados y activados en cada máquina virtual. Sin los servicios de integración, Arcserve Unified Data Protection no puede completar las acciones siguientes: ▪ Ejecutar el comando previo y posterior y las acciones de borrado definitivo del registro de aplicaciones. ▪ Realizar una copia de seguridad coherente con la aplicación. Los servicios de integración contienen varios servicios. La solución Arcserve Unified Data Protection comprueba los estados de los dos servicios siguientes: ▪ Servicio de intercambio de datos de Hyper-V: Servicio necesario para recopilar la información de la máquina virtual, ejecutando los comandos previos y posteriores y las acciones de borrado definitivo del registro de aplicaciones. ▪ Solicitante de la instantánea VSS del volumen de Hyper-V: Servicio necesario para la copia de seguridad coherente con la aplicación.
Estado de potencia	Este elemento verifica que la máquina virtual está encendida. Se muestra una advertencia suspendida cuando la máquina virtual está en un estado que no sea Encendido o Apagado como, por ejemplo, Guardado. La solución Arcserve Unified Data Protection no puede ejecutar los comandos previos y posteriores ni las acciones de borrado definitivo del registro de aplicaciones cuando la máquina virtual no se encuentra en el estado Encendida. Además, Arcserve Unified Data Protection no puede realizar la copia de seguridad coherente con la aplicación cuando la máquina virtual se encuentra en el estado Suspendido.
Disco	Este elemento verifica si se ha adjuntado un disco que no es compatible con la máquina virtual.
Coherencia de datos	Este elemento verifica si la instantánea coherente con la aplicación se puede tomar para la máquina virtual.

La tabla siguiente describe las comprobaciones que realiza la comprobación previa para la máquina virtual de Nutanix AHV:

Elemento	Descripción
Estado de potencia	Este elemento verifica que la máquina virtual está encendida.
Coherencia de datos	Este elemento verifica si la instantánea coherente con la aplicación se puede tomar para la máquina virtual.
Servidor AHV	Este elemento verifica si un servidor puede detectar la máquina virtual. La opción solo es visible cuando el nodo no está disponible en Nutanix AHV.

Soluciones para elementos de comprobación previa de las máquinas virtuales de VMware

Otras referencias:

- Soluciones para elementos de comprobación previa de las máquinas virtuales de Hyper-V
- Soluciones para elementos de comprobación previa de las máquinas virtuales de Nutanix AHV

Las tablas siguientes muestran las soluciones que ayudarán a resolver errores y advertencias de los resultados de la comprobación previa para las máquinas virtuales de VMware:

Seguimiento de bloque modificado (CBT)

Estado	Mensaje	Solución
Error	No puede activarse el seguimiento de bloques modificados.	Si la máquina virtual no tiene la versión 7 o una versión posterior de hardware, actualice la versión del hardware de la máquina virtual o cree un plan de la copia de seguridad basada en agente en Arcserve Unified Data Protection y utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de la máquina virtual.
Advertencia	El seguimiento de bloques modificados está activado con las instantáneas actuales. Se aplicará una copia de seguridad completa del disco para tareas de copia de seguridad completa/verificación de la copia de seguridad.	**Nota:** Afecta únicamente a las tareas de copia de seguridad de verificación e incremental. En el caso de las tareas de copia de seguridad incrementales, solamente se realiza una copia de seguridad de los datos modificados. Para aplicar la copia de seguridad de bloques utilizados para las tareas de copia de seguridad de verificación e incremental, realice los pasos siguientes: 1. Suprima todas las instantáneas asociadas con la máquina virtual. 2. Inicie sesión en el servidor de proxy de la copia de seguridad. 3. Abra el editor del registro y busque la siguiente clave: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\ARCserve Unified Data Protection\Engine\AFBackupDll\<UUID-instancia-máquinavirtual>*

		Nota: Reemplace <UUID-instancia-máquinavirtual> por el valor de UUID de la máquina virtual donde CBT está produciendo un error. El valor se puede encontrar en la dirección URL de la máquina virtual que se usa para la conexión al Agente de Arcserve UDP para Windows. 4. Establezca la clave de registro como "full disk backupForFullBackup"=0. 5. Cree o establezca el registro a ResetCBT=1. 6. Envíe la tarea de copia de seguridad.

Herramientas de VMware

Estado	Mensaje	Solución
Advertencia	Desfasado.	Instale la última versión de VMware Tools.
Advertencia	No está instalado o no está ejecutándose.	Instale la última versión de VMware Tools y asegúrese de que la herramienta se esté ejecutando.

Disco

Estado	Mensaje	Solución
Error	Las instantáneas de máquina virtual no son compatibles con la máquina virtual porque hay un controlador de SCSI configurado para la configuración de participación de bus.	Cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de la máquina virtual.
Advertencia	No se realiza la copia de seguridad del disco físico de asignación del dispositivo son formato (RDM).	Cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de la máquina virtual.
Advertencia	Se realiza la copia de seguridad del disco virtual de asignación del dispositivo sin formato (RDM) como disco completo.	Cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de la máquina virtual.
Advertencia	No se realiza la copia de seguridad del disco independiente.	Cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de la máquina virtual.
Advertencia	Para tareas de copia de seguridad completa/verificación de la copia de seguridad, se realiza una copia de seguridad del disco del almacén de datos de	**Nota**: Afecta únicamente a las tareas de copia de seguridad de verificación e incremental. En el caso de las tareas de copia de seguridad incrementales, solamente se realiza una copia de seguridad de los datos modificados.

	NFS como disco completo.	Mueva el disco virtual al almacén de datos en un dispositivo de almacenamiento de bloques o cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de la máquina virtual.

Estado de potencia

Estado	Mensaje	Solución
Advertencia	Apagado	Encienda la máquina virtual.
Advertencia	Suspendido	Encienda la máquina virtual.

Coherencia de datos

Estado	Mensaje	Solución
Advertencia	VMware no permite la desactivación coherente con la aplicación de una máquina virtual con discos IDE.	Cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de los datos de Microsoft SQL Server y Exchange Server.
Advertencia	VMware no permite la desactivación coherente con la aplicación de una máquina virtual con discos SATA.	Cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para realizar la copia de seguridad de los datos de Microsoft SQL Server y Exchange Server.
Advertencia	VMware no permite la desactivación coherente con la aplicación porque la versión del servidor ESX es anterior a la versión 4.1.	Actualice el servidor ESX Server a la versión 4.1 o a una versión posterior, o cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de los datos de Microsoft SQL Server y Exchange Server.
Advertencia	VMware no permite la desactivación coherente con la aplicación porque no hay suficientes ranuras SCSI disponibles.	Agregue un controlador de SCSI a la máquina virtual desde el cliente web de vSphere o cree un plan de copia de seguridad basado en el agente en Arcserve Unified Data Protection o

		utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de los datos de Microsoft SQL Server y Exchange Server.
Advertencia	VMware no permite la desactivación coherente con la aplicación si el sistema operativo invitado tiene discos dinámicos.	Cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de los datos de Microsoft SQL Server y Exchange Server. **Nota:** VMware no admite la desactivación de nivel de aplicación en máquinas virtuales que son Windows Server 2008 con discos básicos o dinámicos.
Advertencia	No se ha verificado debido a que se ha producido un error cuando la aplicación trataba de acceder a la máquina virtual. Compruebe que las credenciales de inicio sesión son correctas y que dispone de permisos de administración.	Proporcione las credenciales del administrador local integrado o del administrador de dominios para iniciar sesión en el sistema operativo invitado de la máquina virtual. También, verifique que las herramientas de VMware de la máquina virtual se han actualizado y que están en ejecución. Debido a una limitación de VMware, la copia de seguridad solo es compatible máquinas virtuales que se ejecutan en un servidor ESX que tiene una licencia pagada. La copia de seguridad no es compatible en un servidor ESXi con una licencia gratis. **Nota:** La comprobación de la coherencia de los datos es compatible con Windows Server 2008 y posterior.
Advertencia	Unable to verify whether data-consistent backup is possible because the virtual machine is not powered on (No se puede verificar si la copia de seguridad coherente con los datos porque la máquina virtual no está encendida).	Consulte la columna Estado de energía
Advertencia	VMware no permite la desactivación	Cree un plan de copia de seguridad

	coherente con la aplicación si el sistema operativo invitado tiene activados los espacios de almacenamiento. La recuperación de nivel de archivo solo es compatible para esos volúmenes que no tienen activados los espacios de almacenamiento. (La recuperación completa de la máquina virtual es compatible a través de Recuperar máquina virtual).	basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para Windows para realizar la copia de seguridad de los datos de Microsoft SQL Server y Microsoft Exchange Server.

Cómo crear instantáneas coherentes con la aplicación para VMware

En algunos casos, el editor de VSS de VMware no crea instantáneas coherentes con la aplicación en algunas máquinas virtuales. Como resultado, es posible que los datos de los que se ha realizado la copia de seguridad no estén en un estado coherente en la aplicación.

Verificación de los requisitos previos:

Complete los siguientes requisitos previos para crear instantáneas coherente con la aplicación:

- Se debe haber instalado y ejecutado la última versión de VMware Tools en el sistema operativo invitado de la máquina virtual. Además, asegúrese de que el servicio VMware Snapshot Provider esté instalado (no tiene que estar en ejecución).
- La máquina virtual se debe ejecutar en ESXi 4.1 o posterior.
- La máquina virtual solo debe usar discos de SCSI. La máquina virtual debe tener un número igual de ranuras de SCSI libres para coincidir con el número de discos.
- No se compatible con la desactivación coherente con la aplicación para las máquinas virtuales que tienen discos de IDE o SATA.
- Todos los volúmenes de la máquina virtual son discos básicos y no hay ningún disco dinámico.
- El SO invitado de la máquina virtual no tiene activado el espacio de almacenamiento.
- El parámetro disk.EnableUUID de la máquina virtual se debe configurar. Las máquinas virtuales creadas en la versión 4.1 o posterior tienen este parámetro activado de forma predeterminada. La tarea de copia de seguridad realiza las siguientes configuraciones automáticamente para evitar datos incoherentes y realizar una copia de seguridad coherente con la aplicación. Si la tarea de copia de seguridad no puede activar el parámetro disk.EnableUUID debido a algunos motivos, configure manualmente el parámetro utilizando el procedimiento siguiente:
  - Si disk.EnableUUID existe y es FALSO, cámbielo a VERDADERO.
  - Si disk.EnableUUID no existe, créelo y establézcalo en VERDADERO.
  - Si disk.EnableUUID existe y es VERDADERO, manténgalo tal como está.

Nota: Para obtener más información sobre cómo crear una copia de seguridad coherente con la aplicación, consulte el artículo de la base de conocimiento de VMware.

Funciones afectadas:

Si alguno de los requisitos no se cumple, los datos de la sesión se bloquearán. Como resultado, las funciones siguientes se verán afectadas:

- Los datos de los que se ha realizado la copia virtual que incluyen datos de la aplicación de una máquina virtual como SQL, Exchange y SharePoint pueden permanecer en un estado de bloqueo coherente.
- Es posible que se produzca un error en la tarea de catálogo.

Soluciones para elementos de comprobación previa de las máquinas virtuales de Hyper-V

Otras referencias:

- Soluciones para elementos de comprobación previa de las máquinas virtuales de VMware
- Soluciones para elementos de comprobación previa de las máquinas virtuales de Nutanix AHV

Las tablas siguientes muestran las soluciones que ayudarán a resolver errores y advertencias de los resultados de la comprobación previa para las máquinas virtuales de Hyper-V:

Credenciales de Hyper-V

Estado	Mensaje	Solución
Error	Se ha producido un error al acceder al recurso compartido ADMIN$ desde el servidor Hyper-V o no dispone de las credenciales correctas.	■ Verifique que el servidor Hyper-V está en ejecución. ■ Verifique si se puede conectar a la red del servidor Hyper-V. ■ Verifique si el recurso compartido ADMIN$ del servidor Hyper-V está activado. ■ Proporcione derechos de administrador de Hyper-V al importar la máquina virtual desde Hyper-V.

Servicios de integración

Estado	Mensaje	Solución
Advertencia	No instalado, en ejecución, operacional.	Instale/actualice/active los servicios de integración. **Notas:** ■ Para la máquina virtual de Windows, si los servicios de integración están instalados, verifique que los siguientes dos servicios obligatorios se están ejecutando en la máquina virtual: Servicio de intercambio de datos de Hyper-V y Solicitante de instantánea VSS del volumen de Hyper-V. También verifique si hay errores de servicios de Hyper-V en

		el registro de eventos de la máquina virtual. ■ Para una máquina virtual de Linux, verifique que los últimos servicios de integración están instalados y que las funciones *Par de clave/valor* y *Copia de seguridad de la máquina virtual en vivo* están disponibles en la máquina virtual de Linux expecífica. Para obtener más información sobre los servicios integrados de Linux en la máquina virtual de Hyper-V, consulte el artículo de la base de conocimiento de Microsoft.
Advertencia	No responde.	Reinicie los servicios de integración en el sistema operativo invitado de la máquina virtual.
Advertencia	El servicio de integración de la máquina virtual no es compatible con el servicio de integración del servidor Hyper-V.	Cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para realizar la copia de seguridad de la máquina virtual.
Advertencia	Desfasado.	Actualice los servicios de integración.

Estado de potencia

Estado	Mensaje	Solución
Advertencia	Apagado.	Encienda la máquina virtual.
Advertencia	Suspendido.	Encienda la máquina virtual.

Disco

Estado	Mensaje	Solución
Advertencia	No se realizará la copia de seguridad del disco duro físico que se ha adjuntado a la máquina virtual.	Cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para realizar la copia de seguridad de la máquina virtual.
Advertencia	Se ha producido un error al obtener la máquina virtual mediante el UUID de instancia.	Verifique si la máquina virtual existe en el servidor Hyper-V.

Coherencia de datos

Estado	Mensaje	Solución
Advertencia	No se es compatible con una instantánea coherente con la aplicación. La máquina vir-	Cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para realizar la copia de seguridad de la máquina virtual.

	tual tiene un disco dinámico.	
Advertencia	No se admite una instantánea coherente con la aplicación porque la máquina virtual tiene espacios de almacenamiento.	Cree un plan de copia de seguridad basado en un agente de Arcserve UDP o utilice el agente de Arcserve UDP para realizar la copia de seguridad de la máquina virtual.
Advertencia	La instantánea coherente con la aplicación no es compatible porque la máquina virtual tiene un volumen y el almacenamiento de instantáneas se encuentra en otro volumen.	Cambie el área de almacenamiento de instantáneas de volumen al propio volumen. **Nota**: Para una máquina virtual en Hyper-V 2012 R2, si se aplica la última actualización de Microsoft en el host de Hyper-V, la instantánea coherente con la aplicación todavía será compatible en tales casos.
Advertencia	No se es compatible con una instantánea coherente con la aplicación. La máquina virtual tiene sistemas de archivos distintos de NTFS/Refs.	Si desea realizar la copia de seguridad de la máquina virtual pero desea omitir los sistemas de archivos distintos de NTFS/Refs, cree un plan de copia de seguridad basada en agente en Arcserve Unified Data Protection o utilice el Agente de Arcserve Unified Data Protection para realizar una copia de seguridad de la máquina virtual. **Nota**: Para una máquina virtual en Hyper-V 2012 R2, si se aplica la última actualización de Microsoft en el host de Hyper-V, la instantánea coherente con la aplicación todavía será compatible en tales casos.
Advertencia	No se es compatible con una instantánea coherente con la aplicación. La función Scoped Snapshot se activa en la máquina virtual.	Desactive ScopedSnapshot dentro de la máquina virtual agregando una clave de registro de DWORD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\ScopeSnapshots con el valor 0.
Advertencia	No se es compatible con una instantánea coherente con la aplicación. El servicio de integración no está operacional (estado Erróneo).	Consulte la columna Servicios de integración.
Advertencia	No se verifica debido a que se ha producido un error en la aplicación al obtener la máquina virtual mediante el UUID	Verifique si la máquina virtual existe en el servidor Hyper-V.

	de instancia.	
Advertencia	No se verifica porque la máquina virtual no está encendida.	Consulte la columna Estado de energía.
Advertencia	No se es compatible con una instantánea coherente con la aplicación. Se ha producido un error al iniciar sesión en la máquina virtual para comprobar el motivo.	Proporcione las credenciales del administrador local integrado o del administrador de dominios para iniciar sesión en el sistema operativo invitado de la máquina virtual. Además, verifique que la máquina virtual tenga conectividad de red.
Advertencia	La instantánea coherente con la aplicación no es compatible por algún motivo desconocido.	Para identificar el motivo por el que no se puede tomar una instantánea coherente con la aplicación, compruebe los registros de eventos. El registro de eventos se encuentra en la ubicación siguiente: Dentro de la máquina virtual: Visor de eventos > Registros de Windows > Aplicación y sistema. En el registro, busque los errores que procedan del disco, VSS y VolSnap. En el servidor Hyper-V: Visor de eventos > Registros de Windows > Registros de aplicaciones y servicios > Microsoft > Windows > Hyper - V-*. En el registro, busque los errores de la máquina virtual correspondiente.

Cómo crear instantáneas coherentes con la aplicación para Hyper-V

En algunos casos, el editor de VSS de Hyper-V no crea instantáneas coherentes con la aplicación en algunas máquinas virtuales. Como resultado, es posible que los datos de los que se ha realizado la copia de seguridad no estén en un estado coherente en la aplicación.

Verificación de los requisitos previos:

Complete los siguientes requisitos previos para crear instantáneas coherente con la aplicación:

- En la máquina virtual secundaria, el servicio de integración llamado Solicitante de instantánea VSS del volumen de Hyper-V está instalado y ejecutándose.
- La máquina virtual secundaria está en ejecución.
- La ubicación del archivo de la instantánea para la máquina virtual se establece en el mismo volumen en el sistema operativo del host que los archivos de VHD para la máquina virtual.
- Todos los volúmenes de la máquina virtual secundaria son discos básicos y no hay ningún disco dinámico.
- Todos los discos de la máquina virtual secundaria deben usar un sistema de archivos que sea compatible con instantáneas (por ejemplo, NTFS).

Verificación de las consideraciones:

Complete las consideraciones siguientes para crear instantáneas coherentes con la aplicación:

- El servicio de integración instalado en la máquina virtual secundaria debe ser compatible con el host de Hyper-V.
  - Por ejemplo: El servicio de integración de Windows 8.1/2012 R2 que se encuentra dentro de la máquina virtual no es compatible con el host de Hyper-V de Windows 2008 R2.
- Para Windows 8 2012 y posterior, y para la máquina virtual ejecutándose en el host de Hyper-V de Windows 2008R2, la función Scoped Snapshot de la máquina virtual se deberá desactivar. Para desactivar la función Scoped Snapshot, siga estos pasos:
  1. Inicie sesión en la máquina virtual.
  2. Vaya a la ubicación siguiente:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

3. Abra la clave SystemRestore.

   Nota: Cree la clave si no existe.

4. Agregue un valor del registro de DWORD de 32 bits llamado "ScopeSnapshots" y establezca el valor en 0.

Funciones afectadas:

Si alguno de los requisitos no se cumple, los datos de la sesión se bloquean. Como resultado, las funciones siguientes se verán afectadas:

- Los datos de los que se ha realizado la copia virtual que incluyen datos de la aplicación de una máquina virtual como SQL, Exchange y SharePoint pueden permanecer en un estado de bloqueo coherente.
- Es posible que se produzca un error en la tarea de catálogo.

Soluciones para elementos de comprobación previa de las máquinas virtuales de Nutanix AHV

Otras referencias:

- Soluciones para elementos de comprobación previa de las máquinas virtuales de VMware
- Soluciones para elementos de comprobación previa de las máquinas virtuales de Hyper-V

Las tablas siguientes muestran las soluciones que ayudarán a solucionar errores y advertencias de los resultados de la comprobación previa para las máquinas virtuales de Nutanix AHV:

Nutanix Guest Tools (NGT)

Estado	Mensaje	Solución
Advertencia	No se está ejecutando	Active Nutanix Guest Tools para la máquina virtual.
Advertencia	Herramientas activadas	Nutanix Guest Tools activadas pero no en ejecución. Instale Nutanix Guest Tools en la máquina virtual.

Estado de potencia

Estado	Mensaje	Solución
Advertencia	Apagado	Encienda la máquina virtual.
Advertencia	Suspendido	Continúe con la máquina virtual.

Coherencia de datos

Estado	Mensaje	Solución
Advertencia	Nutanix AHV no admite la desactivación coherente con la aplicación de una máquina virtual con discos IDE.	Cree un plan de copia de seguridad basado en Arcserve UDP o utilice el Agente de Arcserve UDP (Windows) para realizar la copia de seguridad de los datos de Microsoft SQL Server y Exchange Server.
Advertencia	Nutanix AHV no admite la desactivación coherente con la aplicación de una máquina virtual con discos SATA.	Cree un plan de copia de seguridad basado en Arcserve UDP o utilice el Agente de Arcserve UDP para realizar la copia de seguridad de los datos de Microsoft SQL Server y Exchange Server.
Advertencia	Nutanix AHV no admite la desactivación coherente con la aplicación porque no hay suficientes ranuras de SCSI disponibles.	Cree un plan de copia de seguridad basado en Arcserve UDP o utilice el Agente de Arcserve UDP (Windows) para realizar la copia de seguridad

		de los datos de Microsoft SQL Server y Exchange Server.
Advertencia	No se ha verificado debido a que se ha producido un error cuando la aplicación trataba de acceder a la máquina virtual. Compruebe que las credenciales de inicio sesión son correctas y que dispone de permisos de administración.	Proporcione las credenciales del administrador local integrado o del administrador de dominios para iniciar sesión en el sistema operativo invitado de la máquina virtual.
Advertencia	No se puede verificar si la copia de seguridad coherente con los datos es posible porque la máquina virtual no está encendida.	Consulte la columna Estado de energía.

Cómo agregar y gestionar una ruta UNC/NFS

La ruta UNC/NFS se introduce como un tipo de nodo en Arcserve UDP. A diferencia de otros nodos, no se puede agregar el nodo Ruta UNC/NFS desde la sección Todos los nodos. Como en el caso del nodo Exchange Online, solamente se puede agregar el nodo Ruta UNC/NFS cuando se crea un plan. Una vez agregado, se puede gestionar el nodo Ruta UNC/NFS desde la sección Todos los nodos para actualizar o suprimir.

¿Qué hacer a continuación?

- Adición de una ruta UNC/NFS
- Actualización de una ruta UNC/NFS
- Supresión de una ruta UNC/NFS

Adición de una ruta UNC/NFS

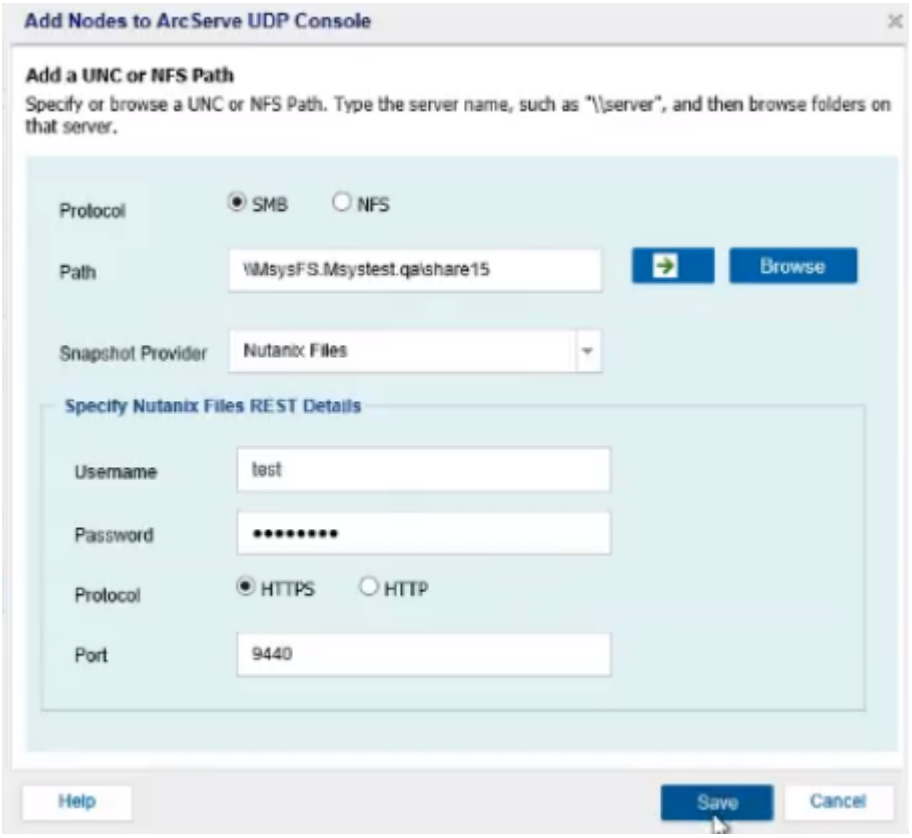
Se puede agregar una ruta UNC/NFS solo cuando se crea un plan de copia de seguridad de la ruta UNC/NFS. Durante la creación del plan, en la ficha **Origen** se puede agregar un nodo Ruta UNC/NFS.

Siga estos pasos:

1. En la ficha **Origen** del plan de copia de seguridad de la ruta UNC, haga clic en la opción **Agregar ruta UNC o NFS**.

   Aparece el cuadro de diálogo Agregar nodos a la Consola de Arcserve UDP.

2. En la página Agregar una ruta UNC o NFS, realice los pasos siguientes:



   a. Seleccione **SMB** o **NFS** como protocolo.

      - Si selecciona **SMB**, haga lo siguiente:

        1. Introduzca la ruta UNC con el siguiente formato:

           *Hostname**share*

           Notas:

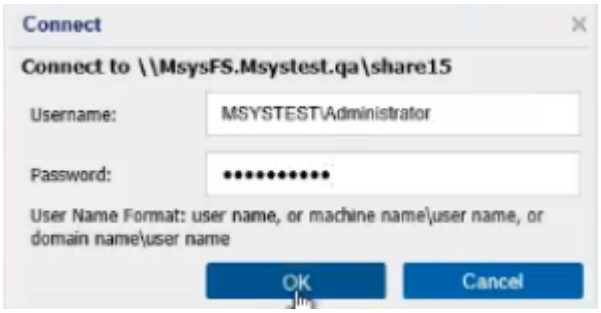
- Al proporcionar el recurso compartido de Nutanix File como origen para la copia de seguridad con los archivos de Nutanix como proveedor de instantáneas, las copias de seguridad solo se pueden realizar en el nivel del recurso compartido pero no en el nivel de subcarpeta.
- Para obtener la ruta UNC, haga lo siguiente:
  a. Seleccione el recurso compartido recién creado en el panel central.
  b. En la columna COMPARTIR/EXPORTAR DETALLES, en el panel Resumen, vaya a **Ruta de montaje** y, a continuación, copie la ruta de montaje.

     Si la ruta UNC es válida, se activarán una flecha hacia la derecha y la opción Explorar.

2. Haga clic en la flecha hacia la derecha (>) para validar la ruta UNC.

   Aparece el cuadro de diálogo Conectar.

3. Introduzca el nombre de usuario y la contraseña según sea necesario y, a continuación, haga clic en **Aceptar**.



   El cuadro de diálogo Adición de nodos en la Consola de Arcserve UDP muestra la ruta UNC verificada.

- Si selecciona NFS, haga lo siguiente:

  1. Introduzca la ruta UNC con el siguiente formato:

     *Hostname**share*

  2. Seleccione una Codificación entre las opciones disponibles: ANSI, GB2312-80, KSC5601, BIG5, SHIFT-JIS, EUC-KR, EUC-TW, EUC-JP.

     El valor predeterminado es ANSI.

     Nota: Durante la copia de seguridad de una carpeta compartida de NFS, se omiten todos los archivos o carpetas cuyo nombre

tenga un código de idioma no admitido o su nombre aparecerá como no deseado.

b. En la lista desplegable Proveedor de instantáneas, seleccione **Nutanix Files**.

c. Para el cuadro Especificar detalles de REST de Nutanix Files, especifique las credenciales siguientes:

Nombre de usuario

Hace referencia al nombre de usuario creado por el usuario de la API de REST mediante Nutanix Prism.

Nota: Para una comunicación más segura, seleccione el protocolo HTTPS.

Contraseña

Hace referencia a la contraseña del nombre de usuario.

Protocolo

Especifica el protocolo que se desea utilizar para comunicarse con el servidor de destino. Las opciones disponibles son HTTP y HTTPS.

Puerto

Se refiere al número de puerto. El valor de puerto predeterminado es 9440 para acceder a las llamadas de la API de REST y a Prism.

3. Haga clic en **Guardar**.

Se puede actualizar o suprimir el nodo Ruta UNC/NFS.

Actualización de una ruta UNC/NFS

Se puede actualizar la información relacionada con los nodos existentes. Al modificar las credenciales de la ruta UNC/NFS, se debe actualizar la ruta UNC/NFS en la Consola.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: Todos los nodos**.

2. En el panel de la izquierda, vaya a **Nodos** y haga clic en **Rutas UNC/NFS**.

   Los nodos Ruta UNC/NFS existentes se muestran en el panel central.

3. En el panel central, seleccione una ruta UNC/NFS y haga clic en **Acciones**.

   Aparece una lista de opciones.

4. En la lista, haga clic en **Actualizar**.

   Se abrirá el cuadro de diálogo **Actualizar nodo**.

5. Actualice los detalles y haga clic en **Aceptar**.

   Se actualizará la información del nodo.

Supresión de una ruta UNC/NFS

Se puede suprimir un nodo Ruta UNC/NFS existente desde la ficha **Recursos**:

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: Todos los nodos**.
2. En el panel de la izquierda, vaya a **Nodos** y haga clic en **Rutas UNC/NFS**.

   Los nodos Ruta UNC/NFS existentes se muestran en el panel central.
3. Seleccione la ruta UNC/NFS que desee y haga clic en **Acciones**.

   Aparece una lista de opciones.
4. Haga clic en **Suprimir**.

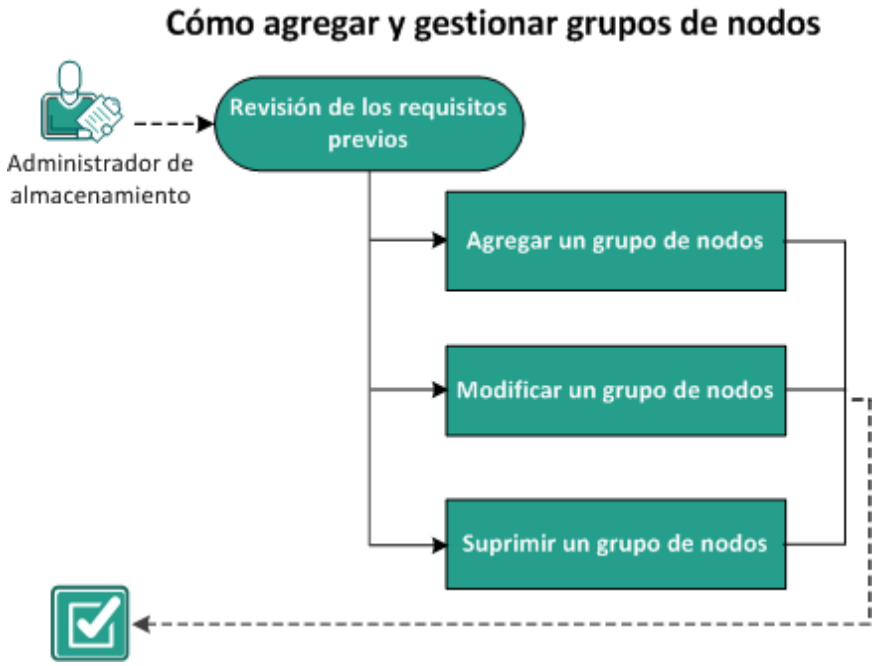
   Aparecerá un diálogo de confirmación.
5. Haga clic en **Aceptar**.

   La ruta UNC/NFS se ha suprimido correctamente

Cómo agregar y gestionar grupos de nodos

Arcserve Unified Data Protection permite agregar varios nodos a un único grupo. Se pueden agregar grupos de nodos para gestionar el entorno físico y de las máquinas virtuales.

El diagrama siguiente ilustra cómo se pueden agregar y gestionar los grupos de nodos:



La solución Arcserve Unified Data Protection contiene los grupos de nodos siguientes:

- Grupos predeterminados:
  - **Todos los nodos**: muestra todos los nodos que se agregan a la consola.
  - **Nodos sin un plan**: muestra los nodos que no tienen ningún plan asignado.

  Nota: No se pueden modificar ni suprimir los grupos de nodos predeterminados.
- Grupos que aparecen cuando se agregan grupos secundarios:
  - **Grupos de planes**: muestra la lista de planes que se han creado. Seleccione cada plan debajo del grupo para ver todos los nodos asociados con ese plan.

- **Grupos personalizados**: muestra la lista de grupos de nodos personalizados creados. Por ejemplo, el grupo de nodos que se crea haciendo clic en **Acciones**, **Grupo de nodos**, **Agregar** en el panel central.
- **Grupos de vCenter/ESX**: muestra los nodos que se agregan mediante la opción **Importación desde vCenter/ESX**.
- **Grupos del servidor de copia de seguridad de Linux**: muestra los nodos del servidor de copia de seguridad.
- **Nodos de Exchange Online**: Muestra los nodos de Exchange Online.
- **Rutas UNC**: Muestra los nodos de UNC.
- **Grupos del perfil del acuerdo de nivel de servicio**: Muestra los nodos relacionados con el acuerdo de nivel de servicio.
- **Grupos de Hyper-V**: muestra los nodos que se agregan mediante la opción **Importación desde Hyper-V.**
- **Grupos del cuadro de mandos global**: muestra todo el servidor primario filial de Arcserve Backup bajo el servidor de GDB. El Grupo de cuadro de mandos global se agrega cuando se agrega un servidor del cuadro de mandos global de Arcserve Backup a la Consola y se realiza una sincronización de la copia de seguridad completa de Arcserve Backup para el servidor de GDB agregado.
- **Grupo de la base de datos de Oracle:** Muestra los nodos de la base de datos de Oracle.

¿Qué hacer a continuación?

- Revise de los requisitos previos
- Agregación de grupos de nodos
- Modificación de grupos de nodos
- Supresión de grupos de nodos

Revisión de los requisitos previos

Antes de trabajar en los grupos de nodo, complete los requisitos previos siguientes:

- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.
- Inicie sesión en la consola.
- Adición de un nodo

Agregación de grupos de nodos

Para gestionar la lista de nodos, se puede crear un grupo para los nodos seleccionados. Por ejemplo, puede agrupar los nodos por su función de negocio o por la aplicación instalada en los mismos. También se pueden agregar nodos en cualquier grupo personalizado más tarde después de agregar un grupo en blanco.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Se mostrará la página **Nodos: todos los nodos**.
3. En el panel central, haga clic en la lista desplegable **Acciones**.
4. Haga clic en **Cree un grupo de nodos**.

   El cuadro de diálogo **Agregar grupo** se abre mostrando todos los nodos disponibles.
5. Complete las acciones siguientes para agregar nodos al grupo y haga clic en **Aceptar**.
   - Seleccione los nodos que se desea agregar a un grupo.
   - Proporcione un nombre al grupo.

     Se abre el cuadro de diálogo **Información** en el panel derecho para proporcionar el mensaje que indica que el grupo de nodos se ha creado.

   El grupo agregado se coloca por debajo de **Grupos personalizados** en el panel izquierdo.

   Nota: Las opciones **Modificar** y **Suprimir** están activadas solamente cuando se ha agregado un grupo.

Modificación de grupos de nodos

La solución Arcserve Unified Data Protection permite modificar los grupos de nodos creados. Se pueden agregar y eliminar nodos de los grupos de nodos y cambiar los nombres de los mismos.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Se mostrará la página **Nodos: todos los nodos**.
3. Seleccione un grupo en **Grupos personalizados** en el panel izquierdo.

   Los detalles del grupo seleccionado se muestran en el panel central.
4. Haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Editar este grupo de nodos**.

   Se abrirá el cuadro de diálogo **Modificar grupo**.
5. Actualice los detalles y haga clic en **Aceptar**.

   Se actualiza el grupo de nodos.

Supresión de grupos de nodos

Se puede suprimir un grupo, si es necesario. Cuando se suprime un grupos que se ha agregado de forma manual, las máquinas virtuales o físicas no se eliminan de Arcserve Unified Data Protection. Sin embargo, si suprime grupos creados de forma automática a partir de la detección del servidor de ESX o vCenter, el grupo y todas las máquinas virtuales se suprimirán de la consola.

Importante: No se pueden suprimir los grupos de nodos predeterminados.

Nota: El proceso de supresión de los grupos de nodos no suprimirá nodos individuales de la consola.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Se mostrará la página **Nodos: todos los nodos**.
3. Seleccione un nombre de grupo en **Grupos personalizados** en el panel izquierdo.

   Los detalles del grupo seleccionado se muestran en el panel central.
4. Haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Suprimir este grupo de nodos**.

   Se abre el cuadro de diálogo **Confirmar**.
5. Haga clic en **Sí**.

   Se abre el cuadro de diálogo **Información** en el panel derecho para proporcionar el mensaje que indica que el grupo de nodos se ha suprimido.

Cómo gestionar nodos para la nube

Mediante Arcserve UDP, se pueden realizar varias acciones para gestionar un nodo para la nube.

¿Qué hacer a continuación?

- Descargar punto de recuperación de la nube
- Cargar punto de recuperación en la nube
- Copiar punto de recuperación en el disco local o recurso compartido de red

Descarga de un punto de recuperación de la nube

Mediante esta función, se pueden descargar puntos de recuperación desde la nube hasta un recurso compartido local o de red.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Aparecerá la página **Nodos: Todos los nodos**.

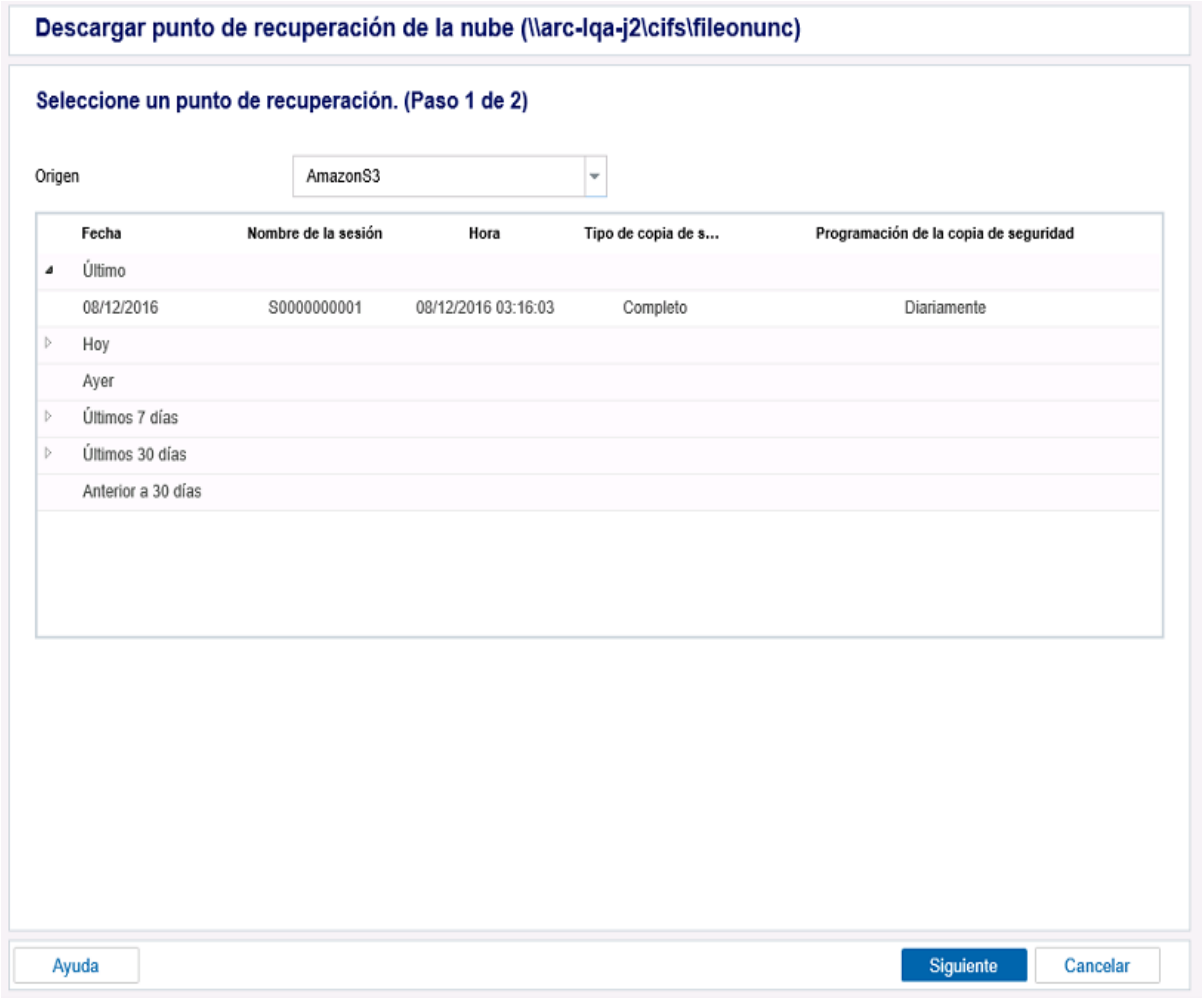
2. Realice una de las acciones siguientes:

   - Haga clic con el botón secundario del ratón en el nombre del nodo.
   - Seleccione el nombre de nodo y en el panel central haga clic en la lista desplegable **Acciones**.

3. Haga clic en **Descargar punto de recuperación de la nube**.

   Aparece la página **Descargar punto de recuperación de la nube**.

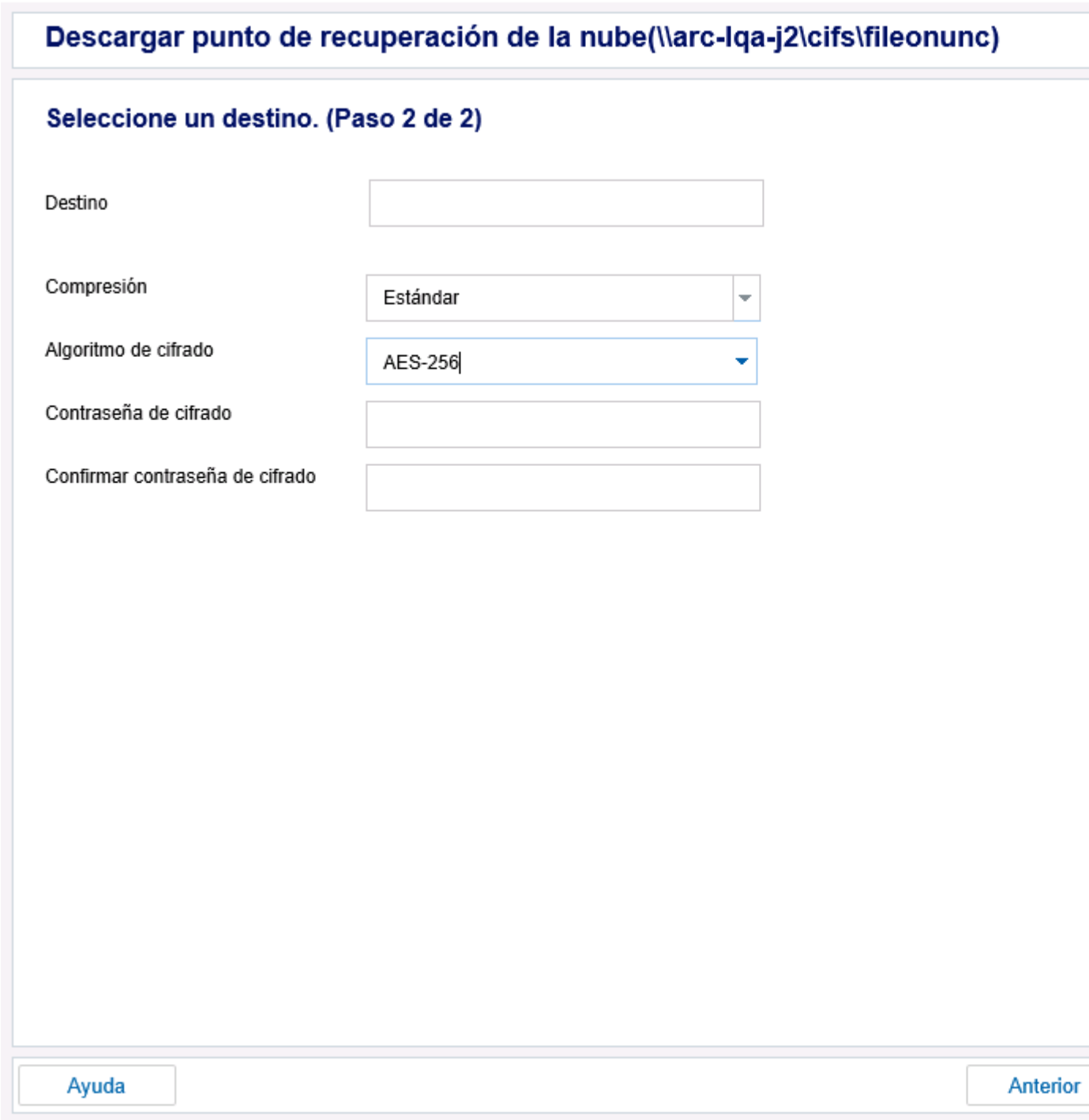
   El punto de recuperación se puede descargar de la nube en dos pasos.



4. En el paso 1, para seleccionar un punto de recuperación, haga lo siguiente y, a continuación, haga clic en **Siguiente**.
   a. En la lista desplegable Servicio de la nube, seleccione un servicio de la nube.
   b. En la lista desplegable Almacenamiento en la nube, seleccione un almacenamiento en la nube.
   c. En la lista desplegable Nombre de depósito, seleccione un nombre de depósito que contenga un punto de recuperación.

      Los detalles del punto de recuperación solo aparecen cuando se configura una tarea de copia del punto de recuperación en el plan.

   Aparecerá la pantalla para seleccionar un destino.



5. En el paso 2, proporcione los detalles siguientes y haga clic en **Finalizar**.
   a. Introduzca el **destino**.

      Nota: Si se ha introducido un destino remoto que requiere validación, después de hacer clic en **Finalizar**, aparecerá en cuadro de diálogo **Conectar**. Introduzca los detalles para que se valide el destino.

   b. Seleccione el tipo de **compresión**.

c. Seleccione el tipo de **algoritmo de cifrado**.

d. Introduzca la **contraseña de cifrado** dos veces.

El punto de recuperación se descarga desde la nube.

Carga de un punto de recuperación a la nube

Mediante esta función, se pueden cargar puntos de recuperación desde destinos de copia de seguridad, tales como el Servidor de puntos de recuperación, una carpeta local o un recurso compartido remoto, a una ubicación en la nube.

Importante: Se debe tener un nodo con un plan de copia de seguridad y una sesión de copia de seguridad completa disponible para realizar la copia en la nube.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: Todos los nodos**.

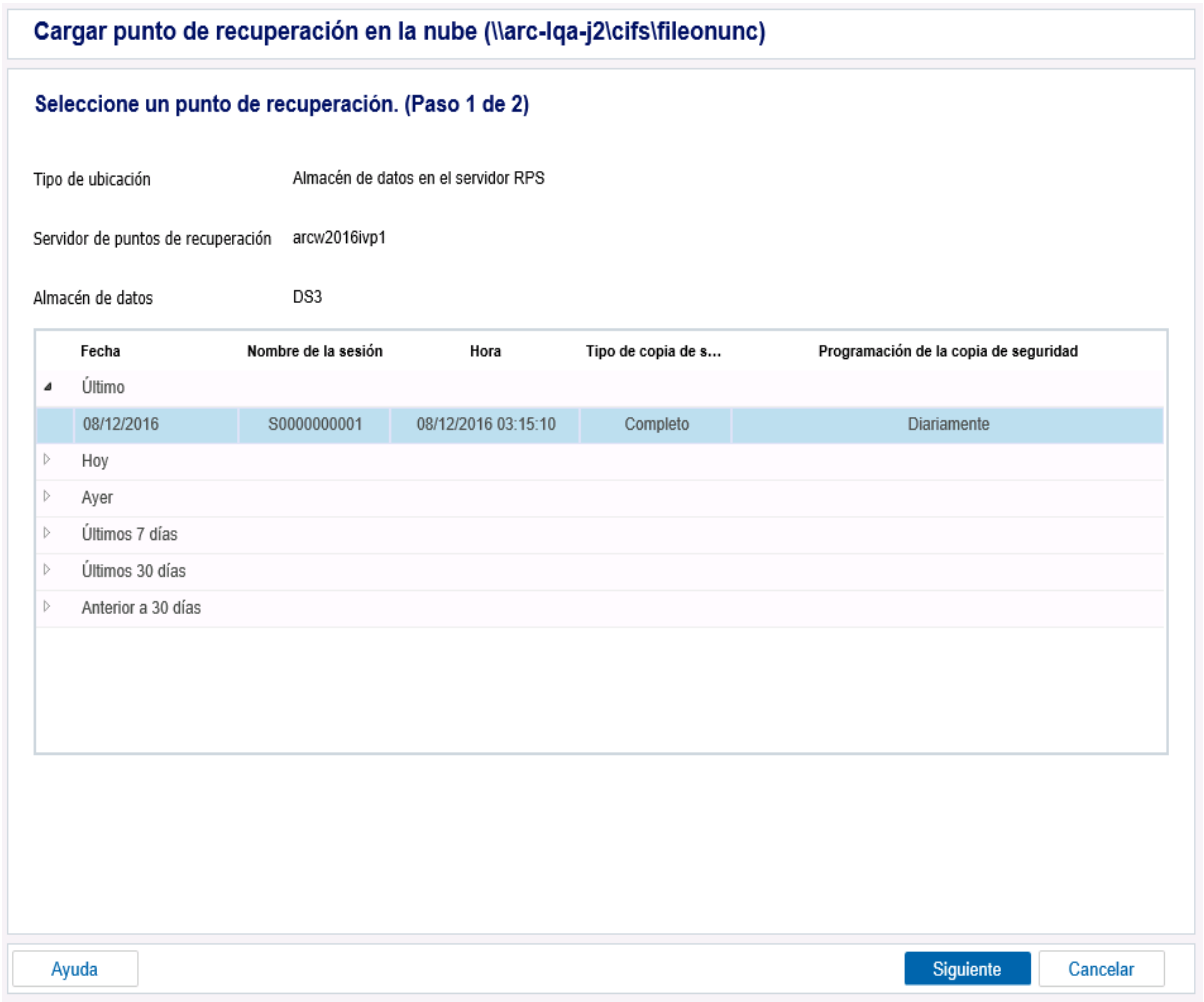
2. Realice una de las acciones siguientes:

   - Haga clic con el botón secundario del ratón en el nombre del nodo.
   - Seleccione el nombre de nodo y en el panel central haga clic en la lista desplegable **Acciones**.

3. Haga clic en **Cargar punto de recuperación en la nube**.

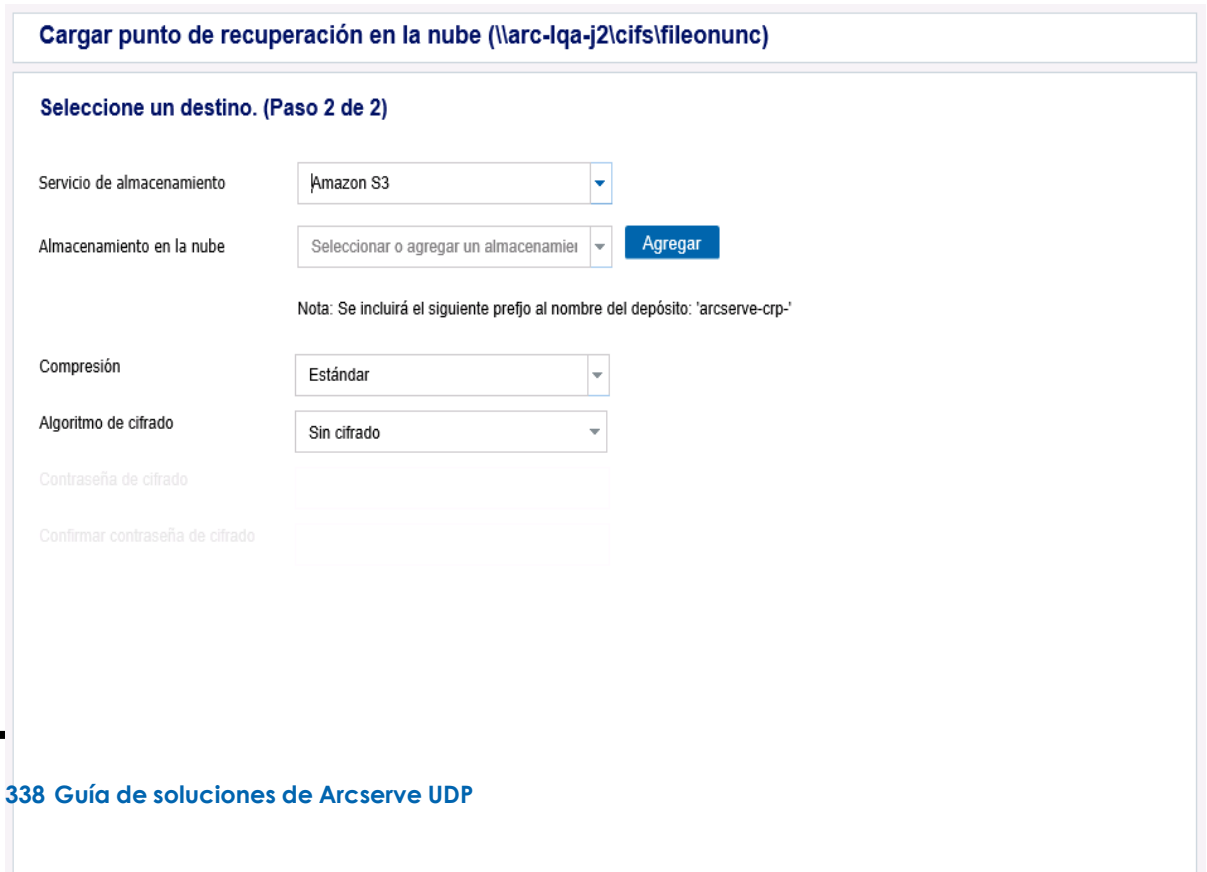
   Se abre el cuadro de diálogo **Cargar punto de recuperación en la nube**.

   El punto de recuperación se puede cargar en la nube en dos pasos.



4. En el paso 1, seleccione un **Punto de recuperación** y haga clic en **Siguiente**.

   Aparecerá la siguiente pantalla de carga.



5. En el paso 2, proporcione los detalles siguientes y haga clic en **Finalizar**.
   a. Seleccione **Servicio de almacenamiento** de la lista desplegable.
   b. Seleccione **Almacenamiento en la nube** de la lista desplegable.

      Nota: Si antes no se ha agregado una cuenta de la nube, haga clic en **Agregar** para agregar una cuenta de la nube.
   c. Seleccione el tipo de compresión de la lista desplegable.
   d. Seleccione el tipo de **algoritmo de cifrado**.
   e. Introduzca la **contraseña de cifrado** dos veces.

   Nota: Un depósito o contenedor se crea con la convención de nomenclatura *arcserve-{ID-generado-aleatoriamente}-<NombreDepósito>*. Sin embargo, cada tarea de *carga de un punto de recuperación a la nube* crea un depósito o contenedor nuevo con un ID *{ID-generado-aleatoriamente}* único. Para obtener el nombre exacto del depósito o contenedor, consulte el registro de actividad de la tarea.

   El punto de recuperación se carga en la nube.

Copia de puntos de recuperación en el disco local o en un recurso compartido de red

Mediante esta función, se pueden copiar puntos de recuperación de destinos de copia de seguridad, tales como el Servidor de puntos de recuperación, una carpeta local o un recurso compartido remoto, a una ubicación local o remota.

Importante: Para copiar a un recurso compartido local o remoto, es necesario tener un nodo con un plan de copia de seguridad configurado y una sesión de copia de seguridad completa disponible.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página **Nodos: Todos los nodos**.

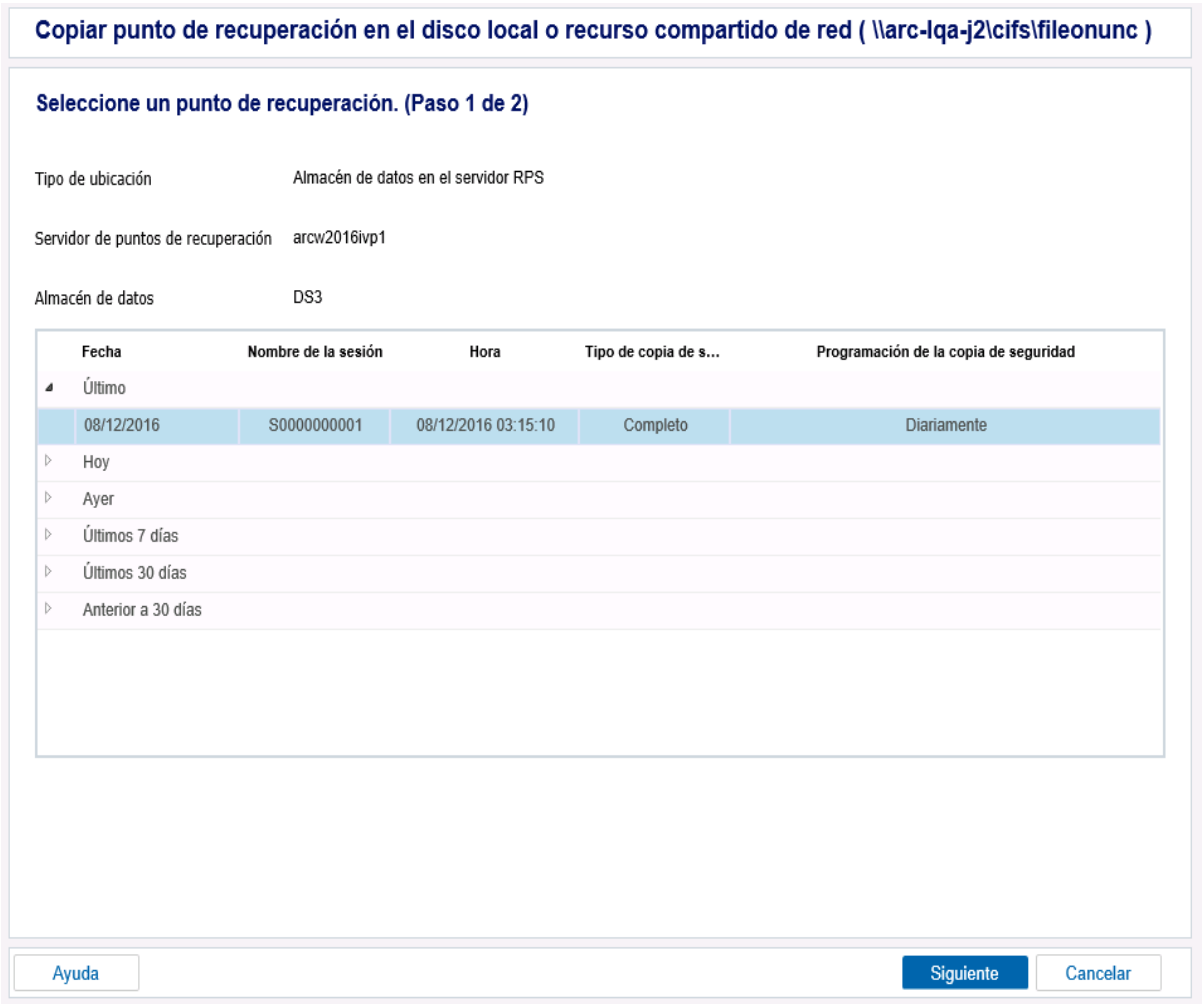
2. Realice una de las acciones siguientes:

   - Haga clic con el botón secundario del ratón en el nombre del nodo.
   - Seleccione el nombre de nodo y en el panel central haga clic en la lista desplegable **Acciones**.

3. Haga clic en **Copiar punto de recuperación en el disco local o recurso compartido de red**.

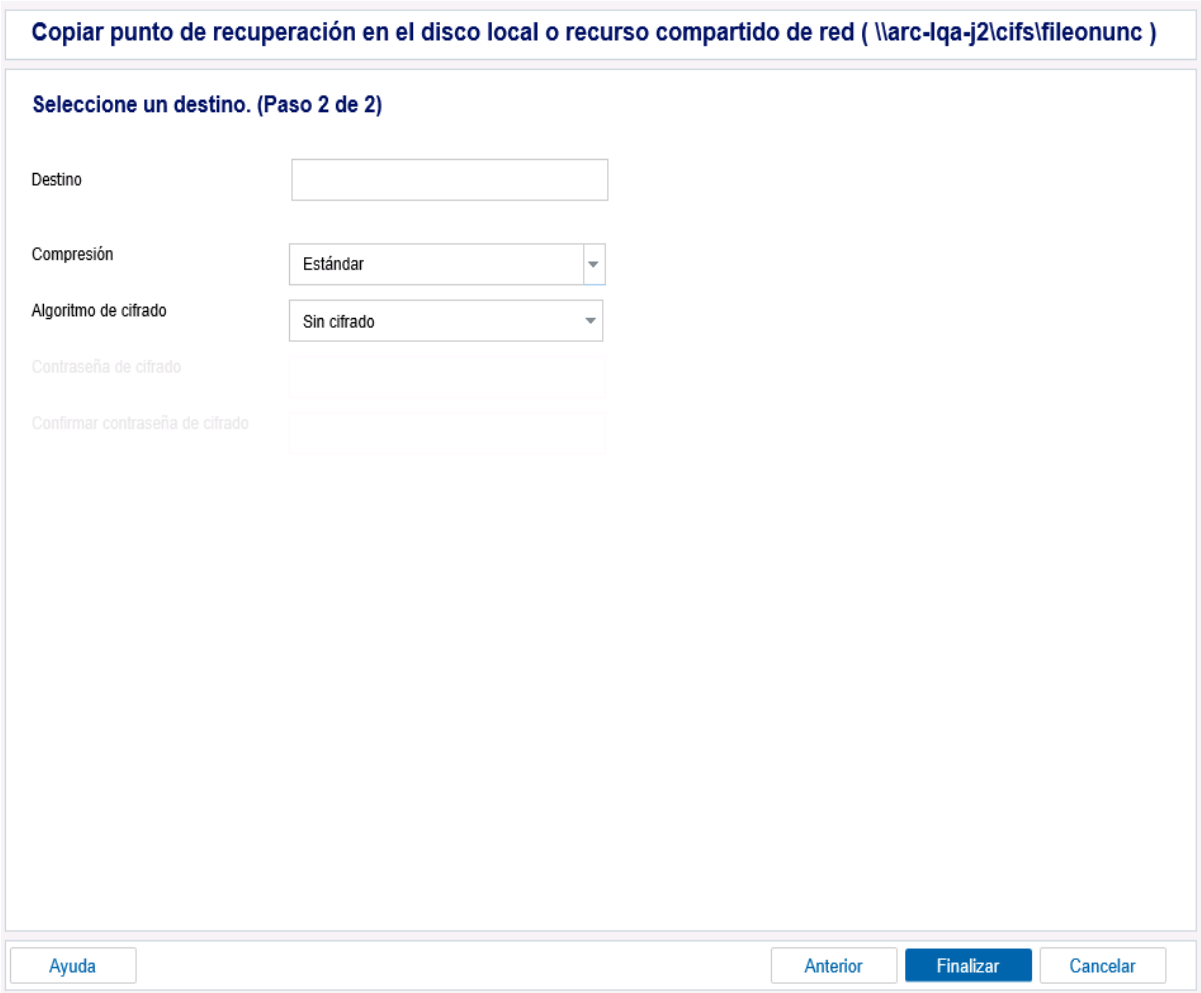
   Se abre el cuadro de diálogo **Copiar punto de recuperación en el disco local o recurso compartido de red**.

   Se puede copiar el punto de recuperación en el disco local o en un recurso compartido de red en dos pasos.



4. En el paso 1, seleccione un **Punto de recuperación** y haga clic en **Siguiente**.

   Aparecerá la pantalla siguiente de la copia del punto de recuperación.



5. En el paso 2, proporcione los detalles siguientes y haga clic en **Finalizar**.
   a. Introduzca el **destino**.

      Nota: Si se ha introducido un destino remoto que requiere validación, después de hacer clic en **Finalizar**, aparecerá en cuadro de diálogo **Conectar**. Introduzca los detalles para que se valide el destino.

   b. Seleccione el tipo de **compresión**.
   c. Seleccione el tipo de **algoritmo de cifrado**.
   d. Introduzca la **contraseña de cifrado** dos veces.

El punto de recuperación se ha copiado desde la nube.

Adición de una matriz de almacenamiento de

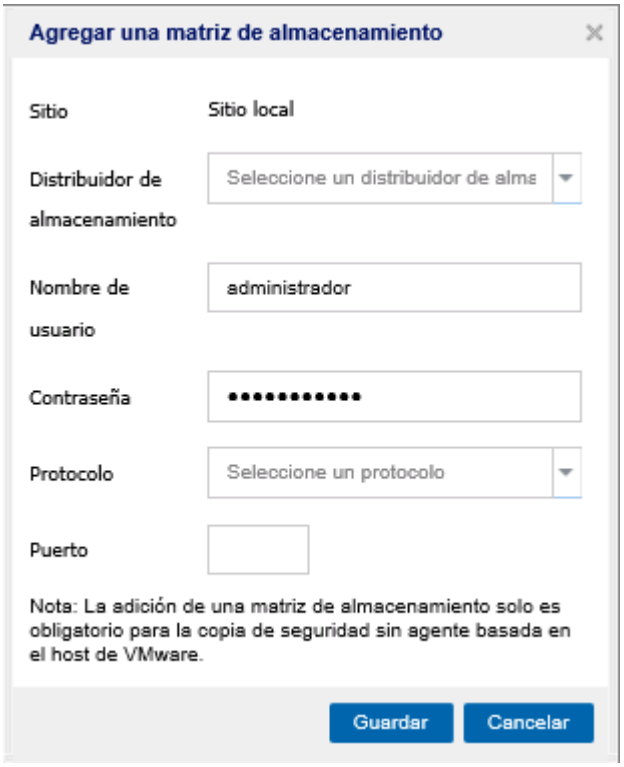
Si utiliza las instantáneas de hardware, se deben agregar los detalles de la matriz de almacenamiento a la Consola. Si no se agrega la matriz de almacenamiento y se envía una tarea de copia de seguridad mediante la instantánea de hardware, la tarea de copia de seguridad buscará primero los detalles de la matriz de almacenamiento en la Consola. Cuando la tarea de copia de seguridad no encuentra los detalles de la matriz de almacenamiento, la tarea utiliza una instantánea de software para crear sesiones de copia de seguridad.

La adición de una matriz de almacenamiento solo se requiere en el caso de las copias de seguridad de VMware sin agente basadas en host.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructura** en el panel izquierdo y haga clic en **Matrices de almacenamiento**.

   Se abre el cuadro de diálogo **Agregar una matriz de almacenamiento**.



   Se puede agregar una matriz de almacenamiento para las siguientes opciones:

   - NetApp

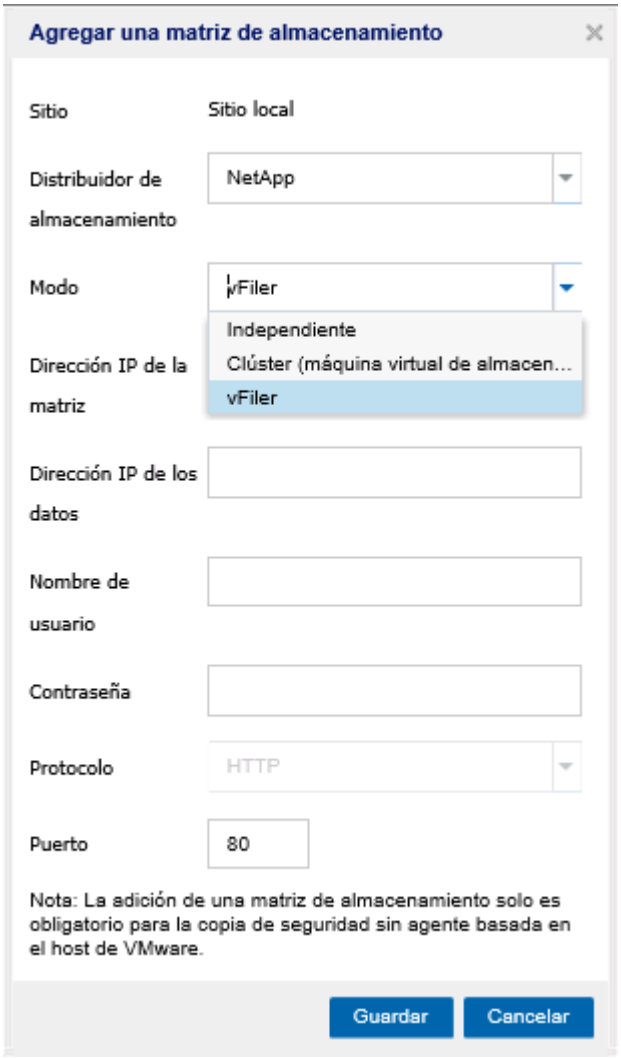
- HPE 3PAR
- Nimble

Adición de una matriz de almacenamiento para NetApp

Se puede agregar una matriz de almacenamiento de NetApp con tres opciones.

Siga estos pasos:

1. En el cuadro de diálogo **Agregar una matriz de almacenamiento**, seleccione NetApp en la opción desplegable **Distribuidor del almacenamiento**.



2. En Modo, seleccione una de las opciones siguientes para el tipo de matriz:

Independiente

Especifica que la matriz de almacenamiento es un dispositivo independiente.

Clúster (SVM)

Especifica que la matriz de almacenamiento pertenece a un clúster de matrices.

vFiler

Especifica que la matriz de almacenamiento es un vFiler.

3. Proporcione los detalles siguientes para el tipo específico de matriz:

Sitio

Especifica el nombre del sitio.

Dirección IP de la matriz

Especifica la dirección IP de la matriz. Si se utiliza 7-Mode, indique la dirección IP que pueda acceder a la interfaz iSCSI y a NFS. VMware(ESXi) utiliza la dirección IP para tener acceso a la matriz de almacenamiento para las operaciones de lectura y escritura. En lo que respecta a los clústeres y al vFiler, especifique la dirección IP de gestión de la matriz de almacenamiento o la de la máquina virtual de almacenamiento (SVM).

Para encontrar la dirección IP de la matriz, consulte el tema Buscar matriz y dirección IP de los datos de la matriz de almacenamiento de la máquina virtual de almacenamiento para la Consola de Arcserve UDP.

Dirección IP de los datos

Especifique la IP de acceso a los datos (interfaz lógica) de la máquina virtual de almacenamiento (SVM), con la que las máquinas de destino (ESXi) puedan acceder a esta matriz de almacenamiento y efectuar operaciones de lectura y escritura. Esta opción solo es aplicable para Clúster y vFiler. Si la máquina virtual de almacenamiento solo es compatible con el protocolo FC, introduzca N/D.

Para encontrar la dirección IP de los datos, consulte el tema Buscar matriz y dirección IP de los datos de la matriz de almacenamiento de la máquina virtual de almacenamiento para la Consola de Arcserve UDP.

Nombre de usuario

Especifica el nombre de usuario para conectarse a la matriz de almacenamiento.

Contraseña

Especifica la contraseña para el nombre de usuario.

Protocolo

Especifica el protocolo para conectarse a la matriz.

Puerto

Especifica el número de puerto de la matriz.

Valor predeterminado: 443 (HTTPS), 80 (HTTP)

4. Haga clic en **Guardar**.

La matriz de almacenamiento se agrega a la Consola.

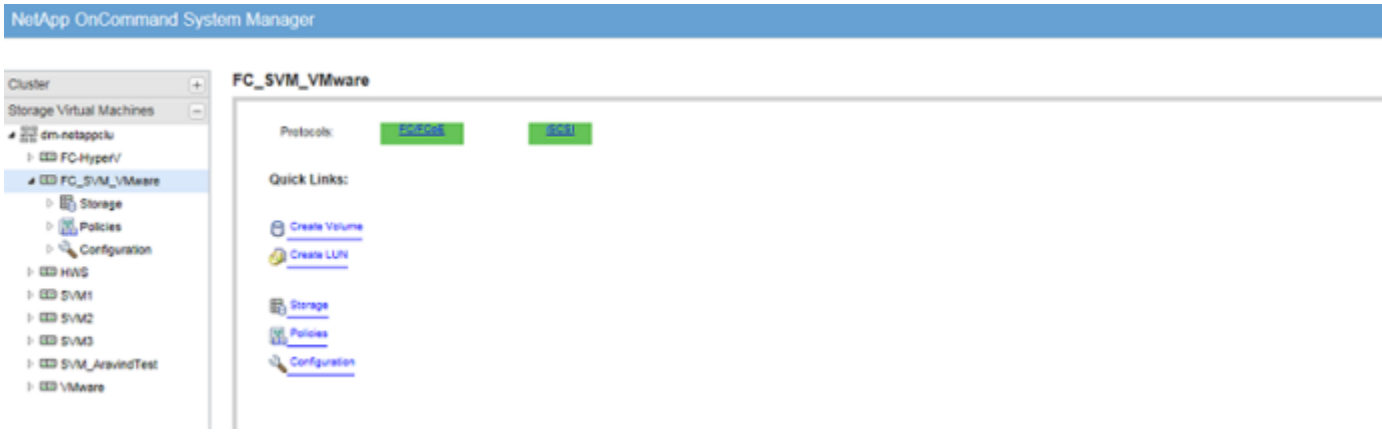
Búsqueda de la matriz y de la dirección IP de los datos de la matriz de almacenamiento de la máquina virtual de almacenamiento para la Consola de Arcserve UDP

Esta sección describe cómo buscar la matriz y la dirección IP de los datos cuando la matriz de almacenamiento de NetApp se está ejecutando en el modo de cDOT (en clúster).

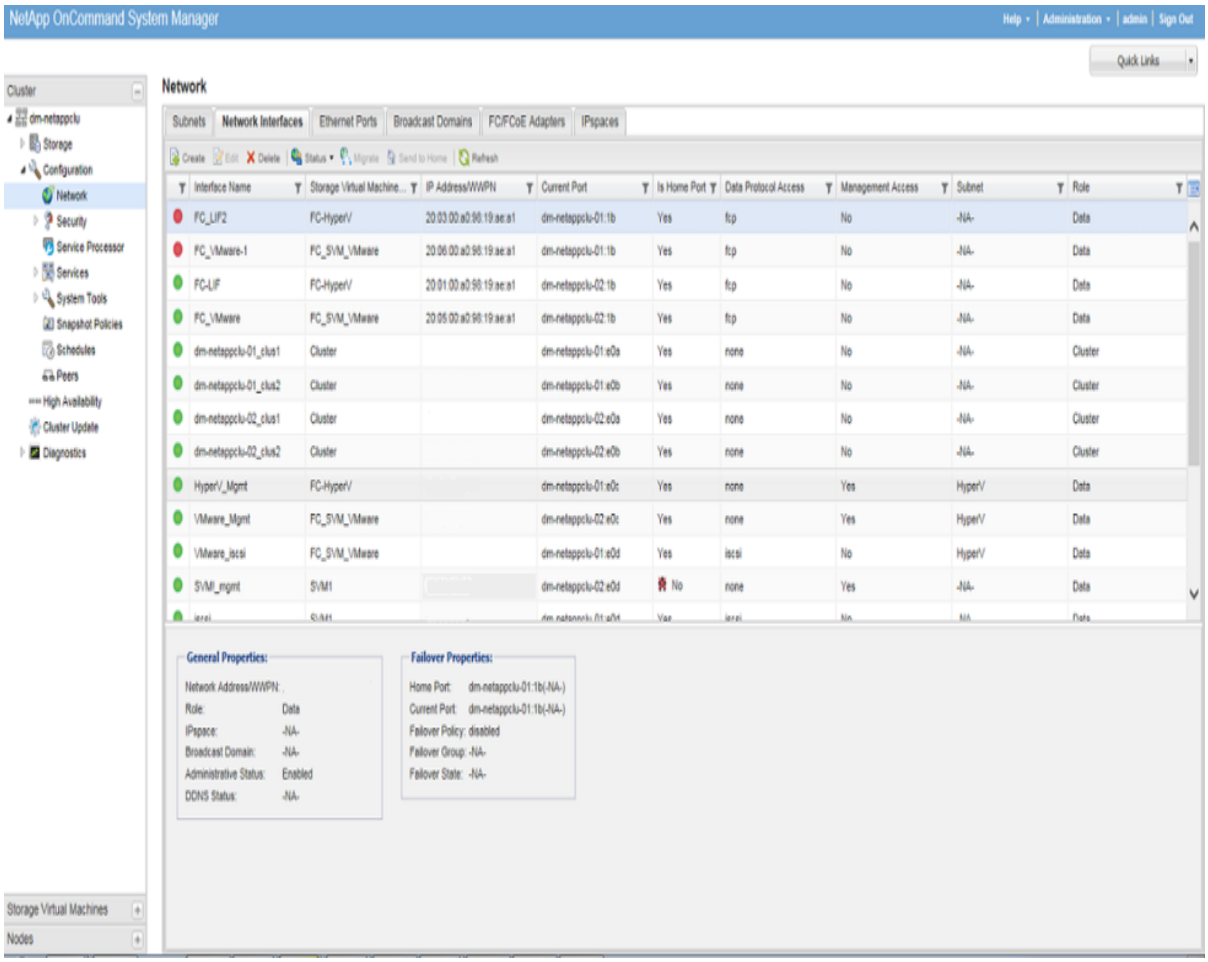
Nota: Solo es aplicable para el clúster (máquina virtual de almacenamiento).

Siga estos pasos:

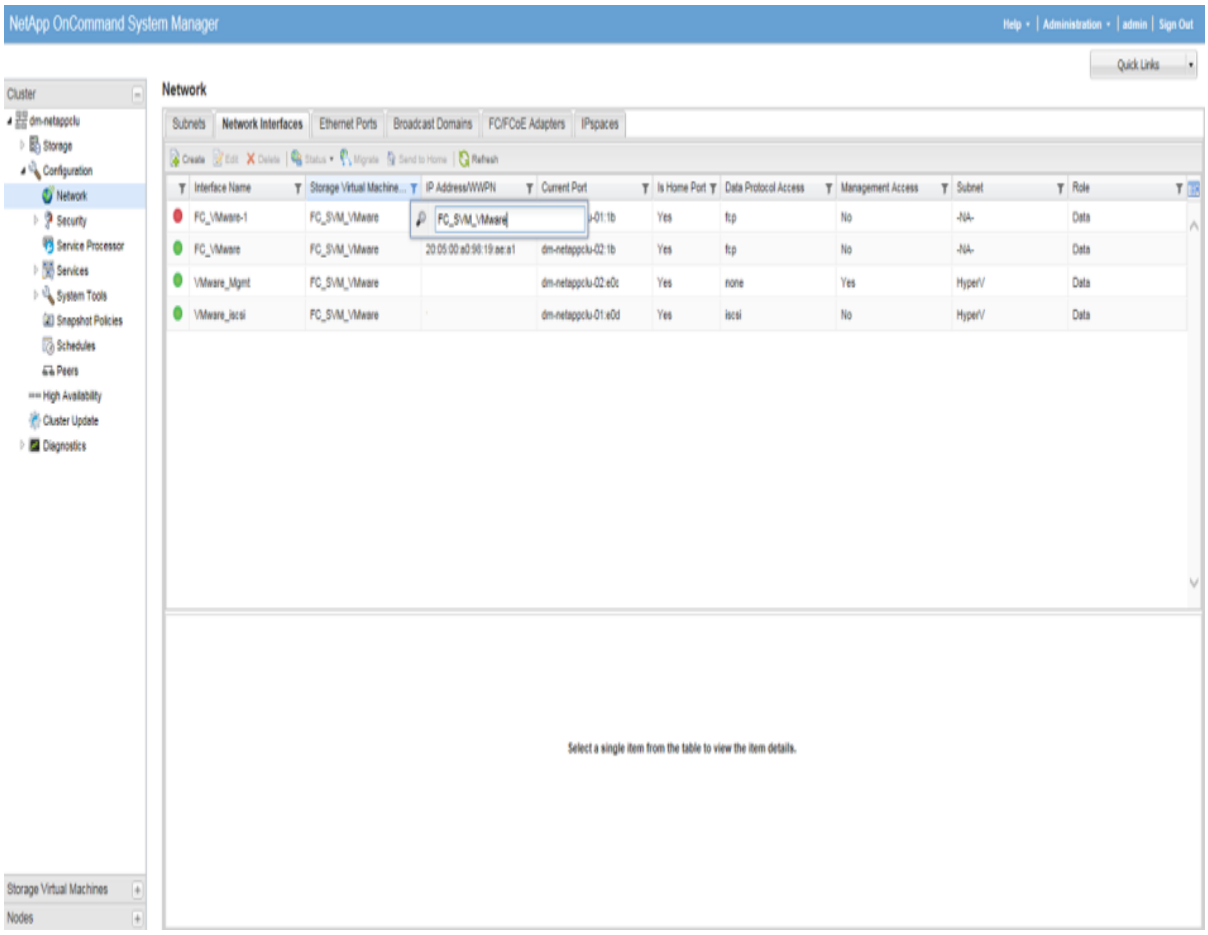
1. Inicie sesión en el gestor del sistema de NetApp y conéctese al clúster con credenciales válidas.
2. Identifique la máquina virtual de almacenamiento (SVM) que se desea agregar a la Consola de Arcserve UDP.



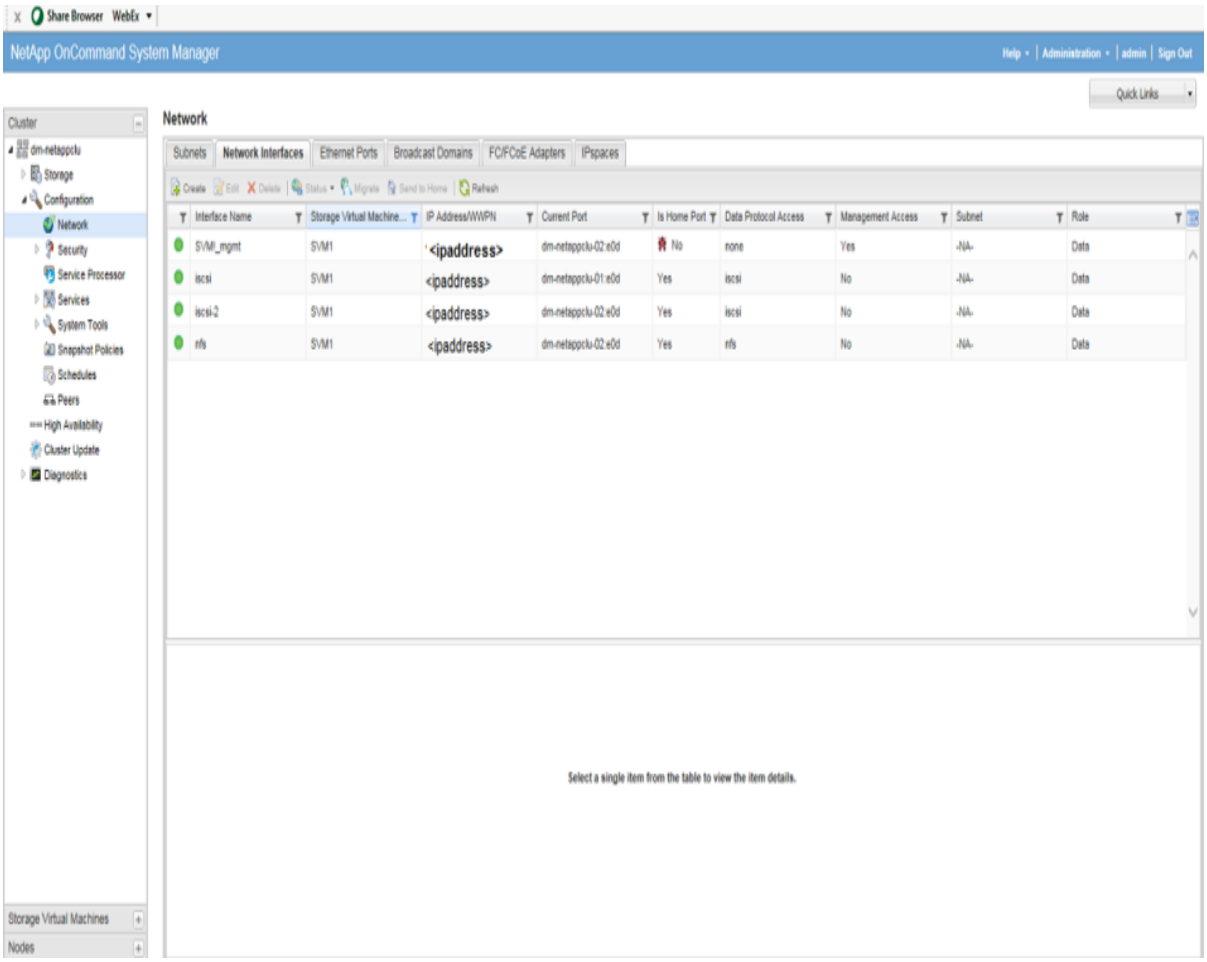
3. Cambie la vista a Clúster.
4. En Clúster > Configuración, haga clic en Red y, a continuación, abra Interfaces de red.

5. 

6. Filtre la máquina virtual de almacenamiento por la SVM que se ha identificado.

7. 

8. Averigüe en qué interfaz se encuentra la dirección IP de acceso de gestión y la dirección IP de acceso al protocolo de datos, y proporciónelas al agregar la matriz de almacenamiento en la Consola de UDP.
   - Obtenga la dirección IP de acceso de gestión:
     - Busque la interfaz de usuario que tenga la opción **Sí** en la columna **Acceso de gestión**.
     - Desde la interfaz, seleccione la dirección IP disponible en **Dirección IP/WWPN**.
   - Obtenga la dirección IP de acceso al protocolo de datos:
     - Busque la interfaz de usuario que tenga la opción **iSCSI** o **NFS** en la columna **Protocolo de datos**.
     - En la interfaz de ISCSI o NFS, seleccione la dirección IP correspondiente disponible en **Dirección IP/WWPN**.



Notas: El servidor ESXi debe utilizar la misma dirección IP de acceso de protocolo de datos para tener permisos de lectura y escritura en la matriz de almacenamiento de NetApp para iSCSI o NFS.

Agregación de los detalles de HPE RMC que gestiona la matriz de almacenamiento HPE 3PAR Storeserv

Se pueden agregar los detalles de HPE RMC que gestiona una matriz HPE 3PAR Storeserv.

Importante: HPE 3PAR StoreServe debe estar gestionado por HP RMC..

Siga estos pasos:

1. En el cuadro de diálogo **Agregar una matriz de almacenamiento**, seleccione HP RMC en la lista desplegable **Distribuidor del almacenamiento**.



2. Proporcione los siguientes detalles:

IP de RMC

Especifica la dirección IP de gestión de HPE RMC.

Nombre de usuario

Especifica el nombre de usuario para conectarse a la matriz de almacenamiento.

Contraseña

Especifica la contraseña para el nombre de usuario.

Protocolo

Especifica el protocolo para conectarse a la matriz.

Nota: Solo se admite HTTPS.

Puerto

Especifica el número de puerto de la matriz.

Valor predeterminado: 443

3. Haga clic en **Guardar**.

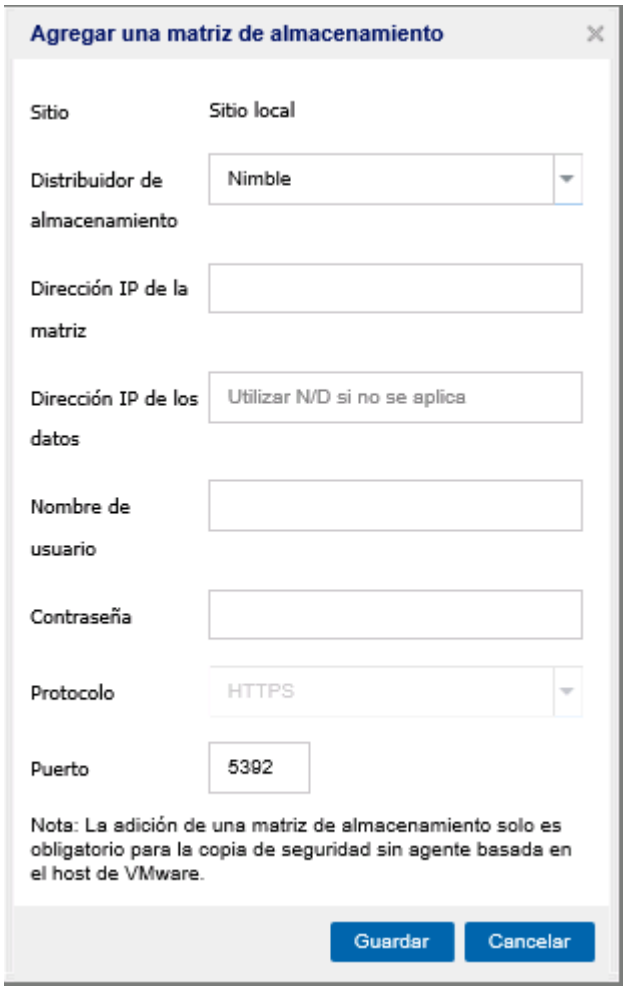
La matriz de almacenamiento se agrega a la Consola.

Adición de una matriz de almacenamiento de Nimble

Se puede agregar una matriz de almacenamiento de Nimble.

Siga estos pasos:

1. En el cuadro de diálogo **Agregar una matriz de almacenamiento**, seleccione Nimble en la opción desplegable **Distribuidor del almacenamiento**.



2. Proporcione los detalles siguientes para el tipo específico de matriz:

Dirección IP de la matriz

Especifica la dirección IP de la matriz. Introduzca la dirección IP de gestión de la matriz de almacenamiento de Nimble.

Dirección IP de los datos

Especifica la dirección IP de acceso a los datos (interfaz lógica) de la matriz de almacenamiento de Nimble, donde las máquinas de destino (ESXi) puedan acceder a esta matriz de almacenamiento y efectuar operaciones de lectura y escri-

tura. Si la matriz de almacenamiento de Nimble solo es compatible con el protocolo FC, introduzca N/D.

Nombre de usuario

Especifica el nombre de usuario para conectarse a la matriz de almacenamiento.

Contraseña

Especifica la contraseña para el nombre de usuario.

Protocolo

Especifica el protocolo para conectarse a la matriz.

Nota: Solo se admite HTTPS.

Puerto

Especifica el número de puerto de la matriz.

Valor predeterminado: 5392

3. Haga clic en **Guardar**.

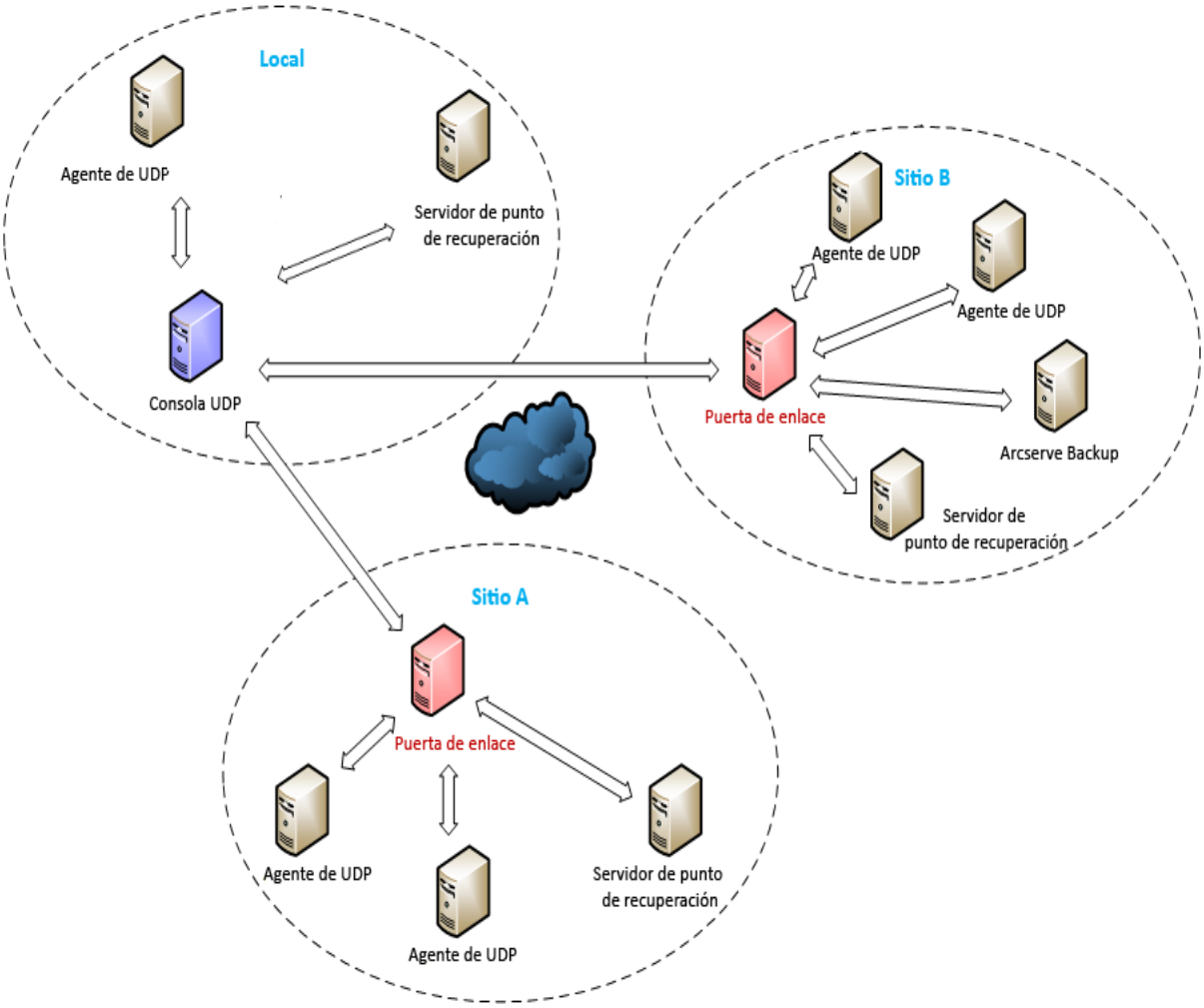
La matriz de almacenamiento se agrega a la Consola.

Cómo agregar y gestionar un sitio

La Consola de Arcserve UDP puede gestionar nodos remotos y servidores de punto de recuperación desde otra subred a través de una WAN. Los nodos remotos y el servidor de un sitio interactúan con la Consola mediante una puerta de enlace. La puerta de enlace se instala en los sitios. A pesar de que la Consola no puede conectarse directamente a los nodos remotos, Arcserve UDP utiliza la puerta de enlace para establecer una conexión entre los nodos y la Consola.

Importante: Si los puntos de recuperación están en un sitio remoto, la consola debe conectarse al sitio remoto mediante una conexión de VPN para restaurar los datos.

El siguiente diagrama muestra la conexión entre locales y sitios.



Después de agregar un sitio, se pueden modificar, actualizar o suprimir sitios desde la Consola. Además, se pueden gestionar los nodos remotos desde la consola.

Especificación del nombre del sitio

La página Nombre del sitio permite especificar un nombre para el sitio y seleccionar un intervalo de latido. Este nombre del sitio se muestra en la consola.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Infraestructuras** y haga clic en**Sitios**.

   Se abre la página Infraestructura: Sitios remotos en el panel central.
3. Haga clic en **Agregar un sitio**.

   Se abre el asistente para **agregar un sitio**.
4. Proporcione los detalles siguientes en la página del sitio:

   Nombre del sitio

   Proporcione un nombre para el sitio.

   Intervalo de latido

   Seleccione un intervalo de tiempo para el latido en la lista desplegable. El latido comprueba la conexión entre la consola y el sitio en un intervalo especificado.

   URL de conexión de la Consola de UDP

   Especifica la dirección URL de la Consola de UDP. El servidor de la puerta de enlace se conecta a esta dirección URL.

   Recordar la dirección URL de conexión de la Consola de UDP

   Seleccione esta casilla de verificación para que se recuerde la URL de la Consola.
5. Haga clic en **Siguiente**.

   Se abre la página de instrucciones de instalación de la puerta de enlace de gestión remota de Arcserve.

   Se ha especificado el nombre para el sitio remoto.

Compartir instrucción de registro

La función Compartir instrucción de registro incluye la información para descargar e instalar la puerta de enlace. Las instrucciones de descarga se envían al administrador remoto. El administrador remoto debe utilizar la información de descarga para descargar e instalar la puerta de enlace.

Siga estos pasos:

1. Copie las instrucciones y guárdelas como referencia.

   Si no se ha configurado el correo electrónico de Arcserve UDP, envíe las instrucciones copiadas al administrador remoto desde otro servidor de correo electrónico.

2. Seleccione **Enviar instrucciones a través del correo electrónico de Arcserve UDP** y proporcione la dirección de correo electrónico del administrador remoto.

3. Haga clic en **Siguiente**.

   Se abre la página **Confirmación**.

   Ha compartido correctamente la instrucción de registro.

Comprobar y agregar el sitio

Verifique los detalles antes de agregar el sitio. Haga clic en **Anterior** para visitar las páginas anteriores.

Siga estos pasos:

1. Especifique los detalles siguientes en la página de confirmación.

   Si es necesario, se puede modificar cualquier información de las páginas anteriores.

2. Haga clic en **Finalizar**.

   Se cierra el asistente.

   Se crea el sitio remoto en la página **Infraestructura: Sitios.**

   Cuando el administrador remoto instala Arcserve Remote Management Gateway y proporciona el código de autorización de la puerta de enlace correcto, aparece una marca de verificación verde junto al nombre del sitio en la Consola.

   El sitio se ha agregado correctamente.

Modificación de la dirección URL de la consola

Cuando se cambia la dirección URL de la consola, debe registrarse la puerta de enlace de nuevo para gestionar el sitio desde la consola. El administrador remoto realiza el registro de la puerta de enlace. Cuando se actualiza la dirección URL de la consola, Arcserve UDP envía un correo electrónico al administrador remoto con instrucciones detalladas sobre cómo registrar la puerta de enlace en la consola.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructura** en el panel izquierdo y haga clic en **Sitios**.

   Se abre la página **Infraestructura: sitios** en el panel central.
3. Seleccione el sitio y haga clic en **Acciones**, **Actualizar URL de la consola**.

   Se abre el cuadro de diálogo **Actualizar URL de la consola**.
4. Especifique la nueva URL de la consola.
5. Haga clic en **Enviar**.

   Se envía un correo electrónico al administrador remoto. Cuando el administrador remoto actualiza la nueva dirección URL en el servidor de puerta de enlace, la consola muestra una marca de verificación verde al lado del sitio actualizado.

   Se ha modificado correctamente la dirección URL de la Consola.

Modificación del sitio

Se puede modificar el sitio para cambiar cualquiera de los parámetros del sitio agregado. Por ejemplo, se puede cambiar el nombre del sitio o cambiar el intervalo de latido.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructura** en el panel izquierdo y haga clic en **Sitios**.

   Se abre la página **Infraestructura**: **Sitio** en el panel central.
3. Seleccione el sitio y haga clic en **Acciones**, **Modificar**.

   Se abre el asistente para **modificar un sitio**.
4. Utilice **Anterior** y **Siguiente** para visitar cualquier página y modificar cualquier parámetro.
5. Haga clic en **Finalizar**.

   Se cierra el asistente para **modificar un sitio**.

   El sitio se ha modificado correctamente.

Eliminación de un sitio

Se puede suprimir un sitio que no desee gestionar. Antes de suprimir un sitio, deben suprimirse todos los nodos y filtros de detección de nodos relacionados con el sitio.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructura** en el panel izquierdo y haga clic en **Sitios**.

   Se abre la página **Infraestructura**: **Sitio** en el panel central.
3. Seleccione el sitio y haga clic en **Acciones**, **Suprimir**.

   Se abre el cuadro de diálogo **Confirmar**.
4. Haga clic en **Sí**.

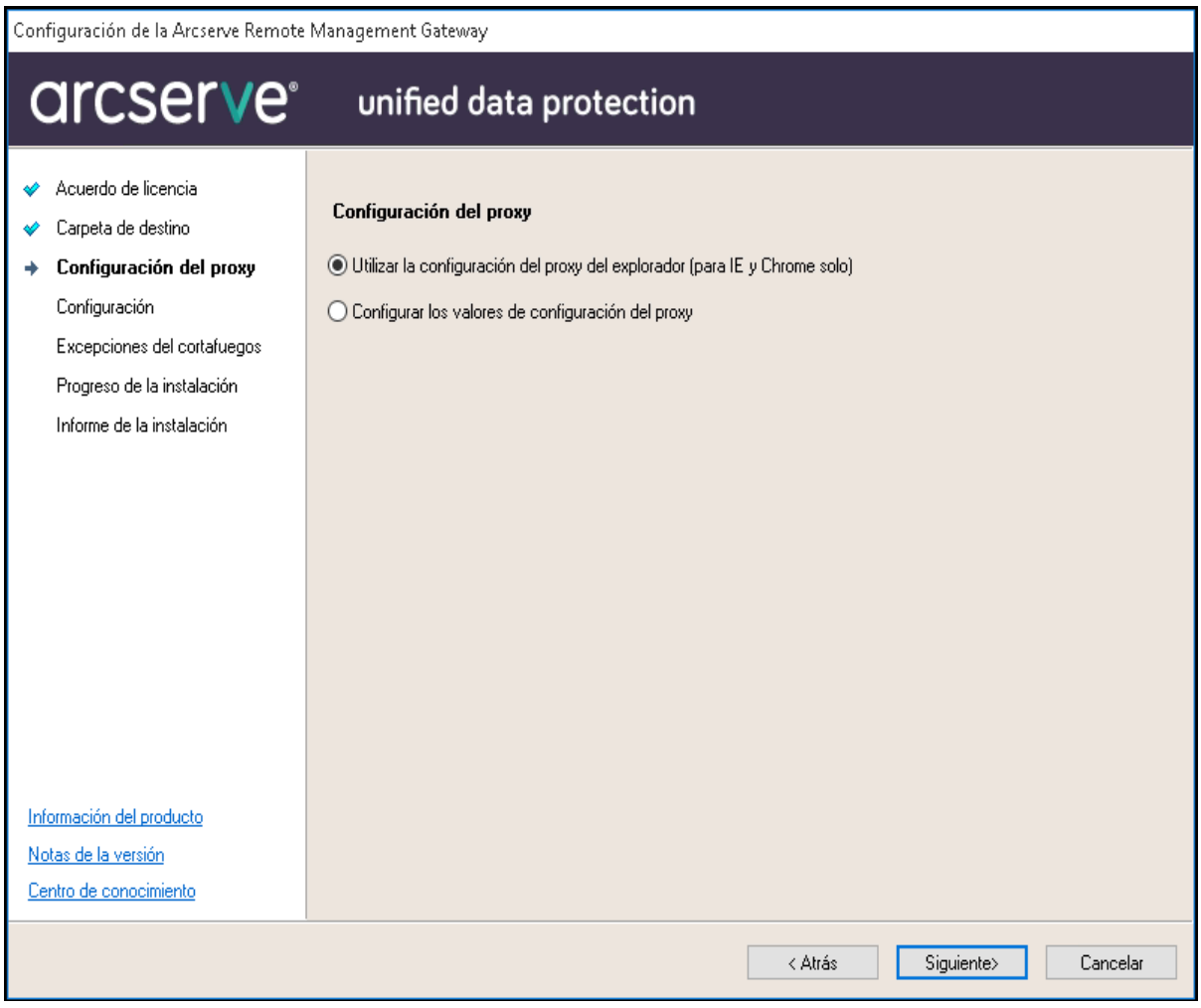
   Se suprime el sitio.

Configuración de un servidor proxy para la puerta de enlace

Arcserve UDP es compatible con la instalación de un servidor proxy en el equipo de la puerta de enlace. La puerta de enlace utiliza esta configuración proxy para comunicarse con su Consola registrada.

Siga estos pasos:

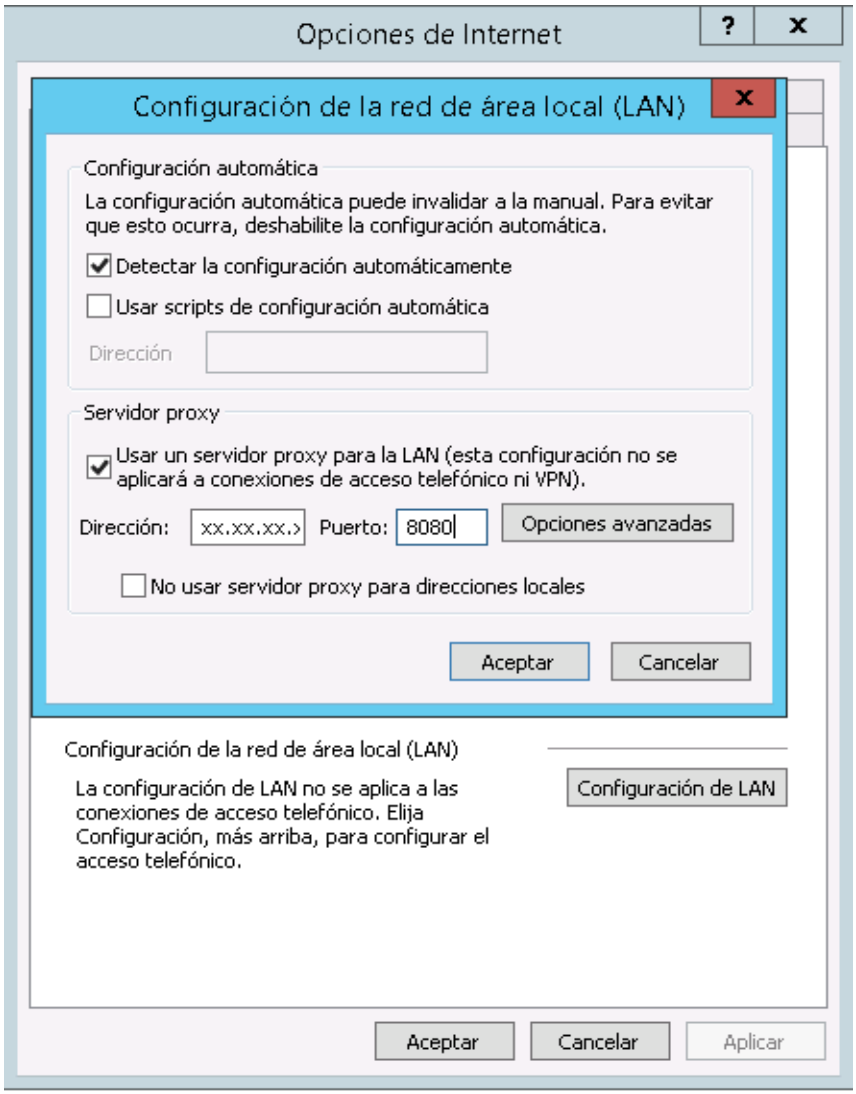
1. Abra el asistente de instalación de puerta de enlace de gestión remota de Arcserve.



2. En el cuadro de diálogo Configuración proxy, seleccione una de las siguientes opciones:

   Utilizar la configuración de proxy del explorador (sólo IE y Chrome)

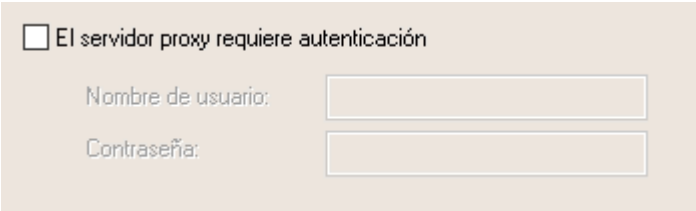
Especifica la utilización de los valores de configuración del servidor proxy del explorador. Se debe actualizar la configuración proxy del explorador. Abra el explorador y haga clic en **Opciones Conexión Configuración de LAN**.



Configuración del proxy

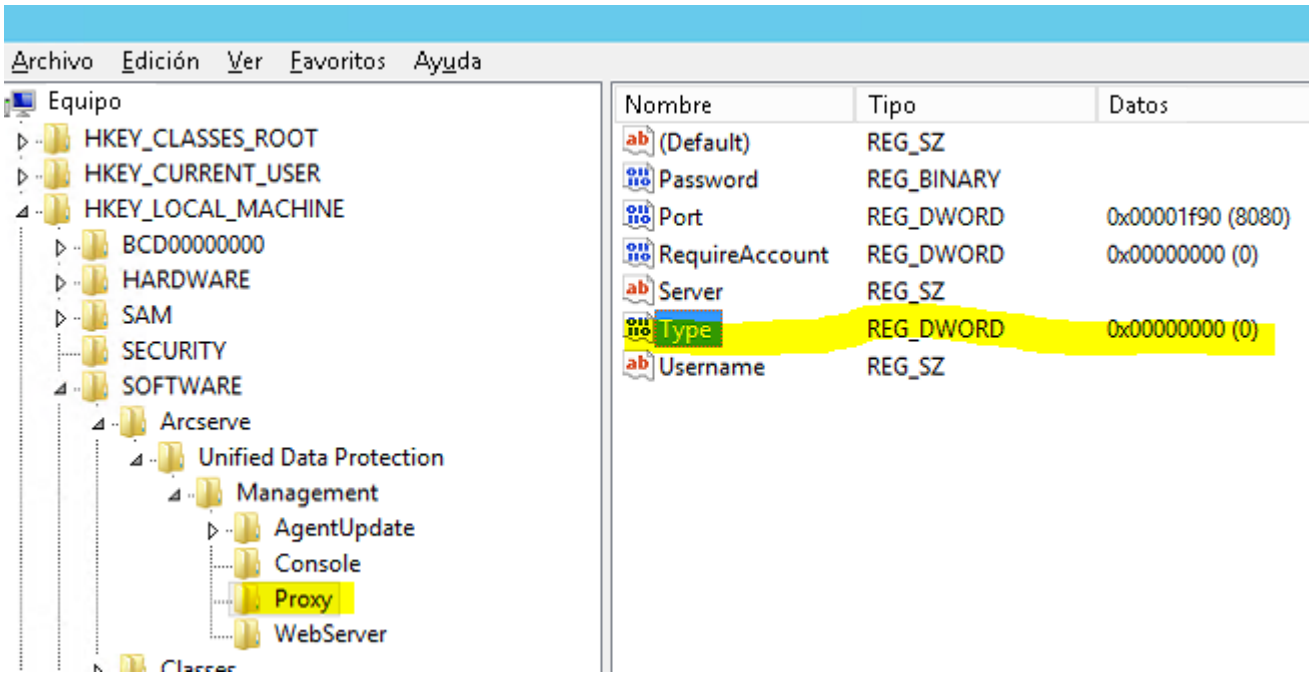
Especifica que se deben proporcionar los detalles del servidor proxy en la página del asistente.

3. Si el servidor proxy no admite credenciales, anule la selección de la casilla de verificación de autenticación.



El servidor proxy está configurado para la puerta de enlace.

4. Para verificar la configuración proxy, abra regedit y vaya al servidor Proxy.



En el campo Tipo, 0 indica la configuración del explorador y 1 indica otros valores de configuración.

Nota: Utilice regedit para modificar cualquiera de las configuraciones del servidor proxy como el puerto, la dirección IP del servidor o el tipo.

Cómo gestionar los nodos de Exchange Online

No se pueden agregar directamente los nodos de Exchange Online a la vista de todos los nodos. Una vez se haya agregado el nodo al plan de copia de seguridad, se agregará directamente el nodo de Exchange Online a la vista de todos los nodos.

Se pueden realizar las tareas siguientes:

1. Adición de un nodo de Exchange Online
2. Actualización de un nodo de Exchange Online
3. Supresión de un nodo de Exchange Online
4. Compatibilidad con el buzón de correo de la carpeta pública para la protección de Exchange Online

Adición de un nodo de Exchange Online

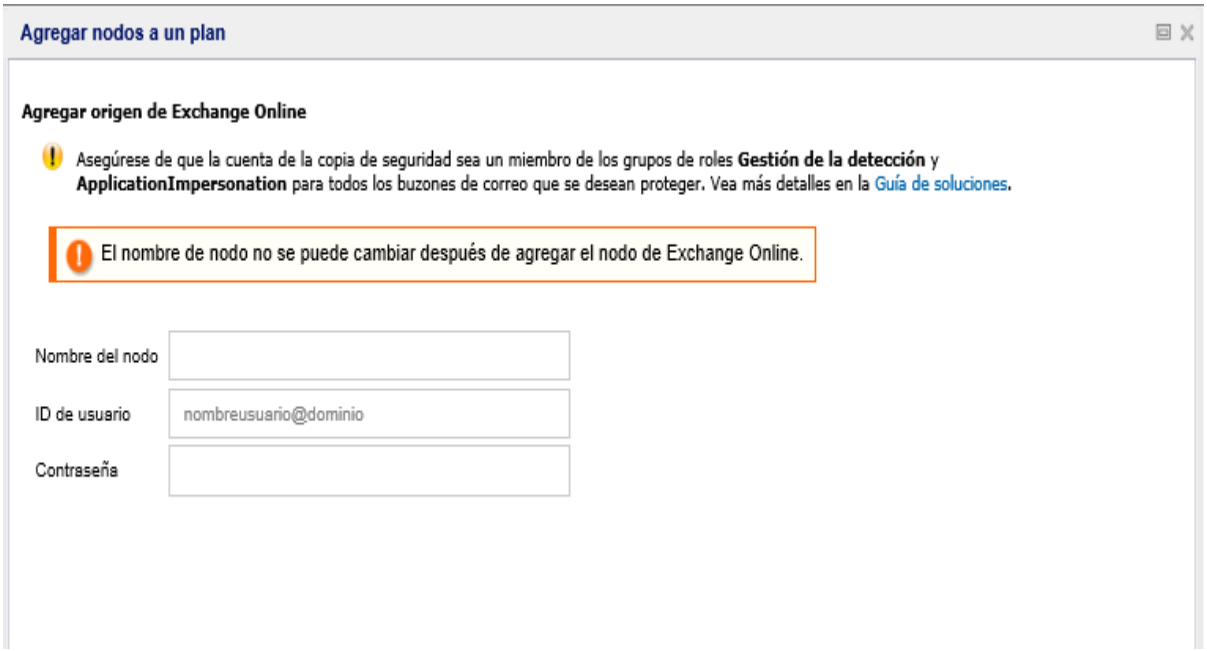
Nota: A diferencia de otros nodos, no se puede agregar el nodo de Exchange Online desde la página Todos los nodos. Solo se agrega un nodo de Exchange Online a un plan o al modificar un plan.

Para obtener más información sobre cómo crear un plan, consulte Cómo crear un plan de Exchange Online.

Siga estos pasos:

1. Introduzca el nombre de usuario de la cuenta de copia de seguridad de Exchange Online que cumpla los requisitos previos en el campo Nombre de usuario o Cuenta del usuario para el nodo en línea de Exchange.

   Varios nodos de Exchange Online pueden utilizar la misma cuenta de usuario (cuenta de servicio) de Exchange Online. Para agregar el nodo de Exchange por plan, especifique el nombre del nodo, el nombre de usuario y la contraseña. Una vez creado, no se puede cambiar el nombre de nodo del nodo de Exchange Online.



   Nota: Es posible que al realizar una actualización o cambio en la cuenta de usuario se pueda cambiar el número de buzones de correo protegidos. Compruebe que la cuenta de servicio nueva o actualizada tiene derechos de suplantación para que los buzones puedan estar protegidos.

2. Introduzca la contraseña y haga clic en **Conectar**.
3. Seleccione las cuentas de Exchange Online que se van a proteger y haga clic en la flecha hacia la derecha (>) para moverlas a la lista protegida.

Nota: Si se desea proteger todas las cuentas de Exchange Online en todas las páginas, seleccione la casilla de verificación para proteger todos los orígenes de Office 365 Exchange. Para agregar todas las cuentas de Exchange Online que se muestran en la página a la lista protegida, haga clic en la flecha hacia la derecha (>).

4. Haga clic en **Guardar**.

   También se pueden seleccionar las carpetas que no se desean incluir en la copia de seguridad utilizando la opción Seleccionar carpetas para excluir de la copia de seguridad en la ficha Origen.

   Se agregan las cuentas de Exchange Online seleccionadas.

Actualización de un nodo de Exchange Online

Al modificar las credenciales del nodo de Exchange Online, actualice el nodo de Exchange Online en la Consola.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Nodos de Exchange Online**.

   Los nodos de Exchange Online creados se muestran en el panel central.
3. Seleccione el nodo de Exchange Online y haga clic en **Acciones**.
4. Haga clic en **Actualizar**.

   Aparece el cuadro de diálogo **Actualizar nodo**.
5. Modifique los detalles según sea necesario y haga clic en **Aceptar**.

   Se ha actualizado el nodo de Exchange Online.

Supresión de un nodo de Exchange Online

Suprima cualquier nodo de Exchange Online que ya no se necesite.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. Vaya a **Nodos** y haga clic en **Nodos de Exchange Online**.

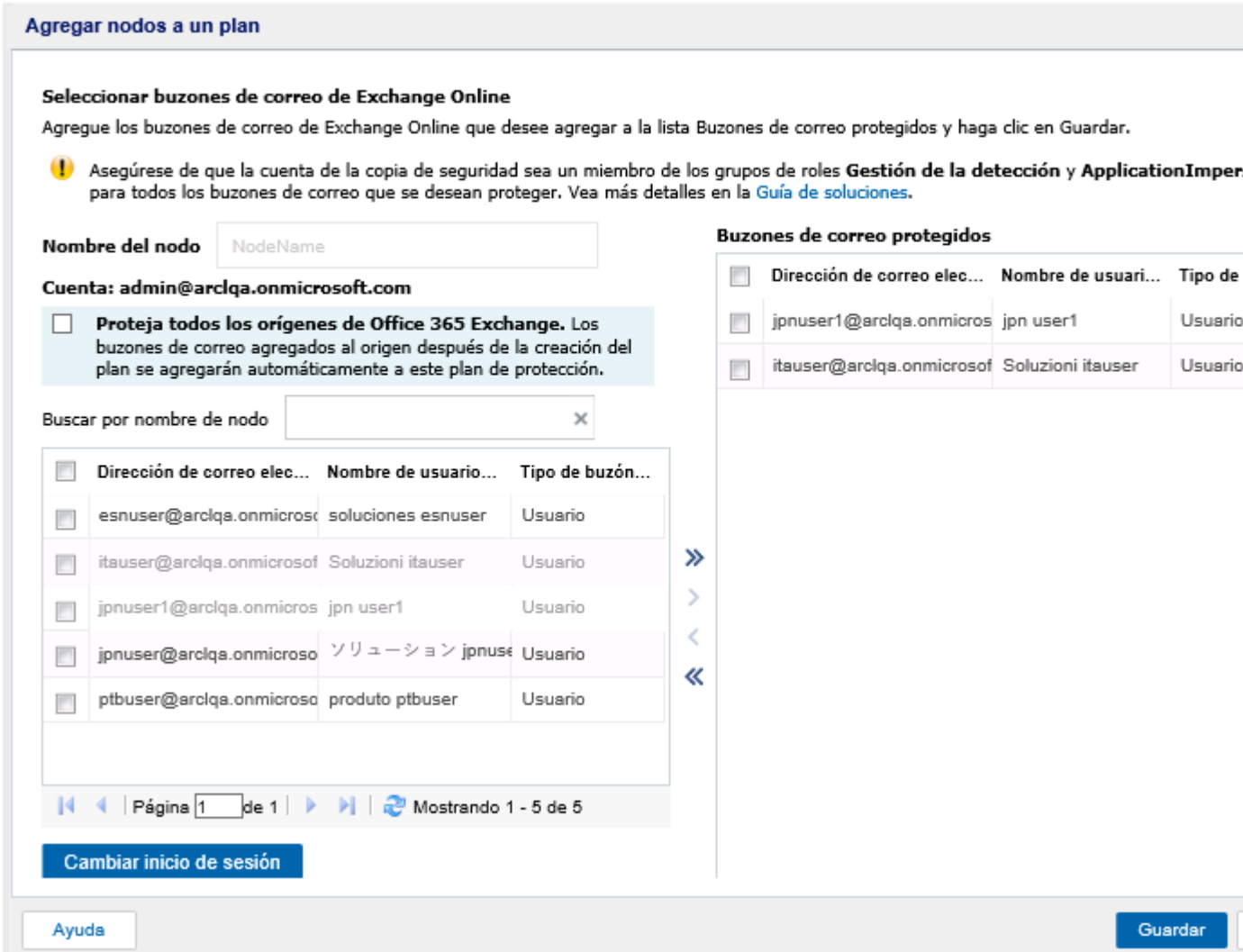
   Los nodos de Exchange Online creados se muestran en el panel central.
3. Seleccione el nodo de Exchange Online y haga clic en **Acciones**.
4. Haga clic en **Suprimir**.

   Aparecerá un diálogo de confirmación.
5. Haga clic en **Aceptar**.

   Se ha suprimido correctamente el nodo de Exchange Online.

Compatibilidad con el buzón de correo de la carpeta pública para la protección de Exchange Online

Al agregar el nodo de Exchange Online, se puede ver la columna de tipo de buzón en la ventana **Agregar nodos a un plan**. El buzón de la carpeta pública aparece en esta ventana y en la columna aparece como **carpeta pública**. Para proteger la carpeta pública, agregue el buzón público correspondiente en **Buzones protegidos** y, a continuación, guarde el plan.



Nota: Para obtener más información sobre el buzón de la carpeta pública de Exchange Online y los permisos, consulte vínculo 1 y vínculo 2.

Cómo gestionar los nodos de SharePoint Online

No se pueden agregar directamente los nodos de SharePoint Online a la vista de todos los nodos. Una vez se haya agregado el nodo al plan de copia de seguridad, se agregará directamente el nodo de SharePoint Online a la vista de todos los nodos.

Se pueden realizar las tareas siguientes:

1. Adición de un nodo de SharePoint Online
2. Actualización de un nodo de SharePoint Online
3. Supresión de un nodo de SharePoint Online

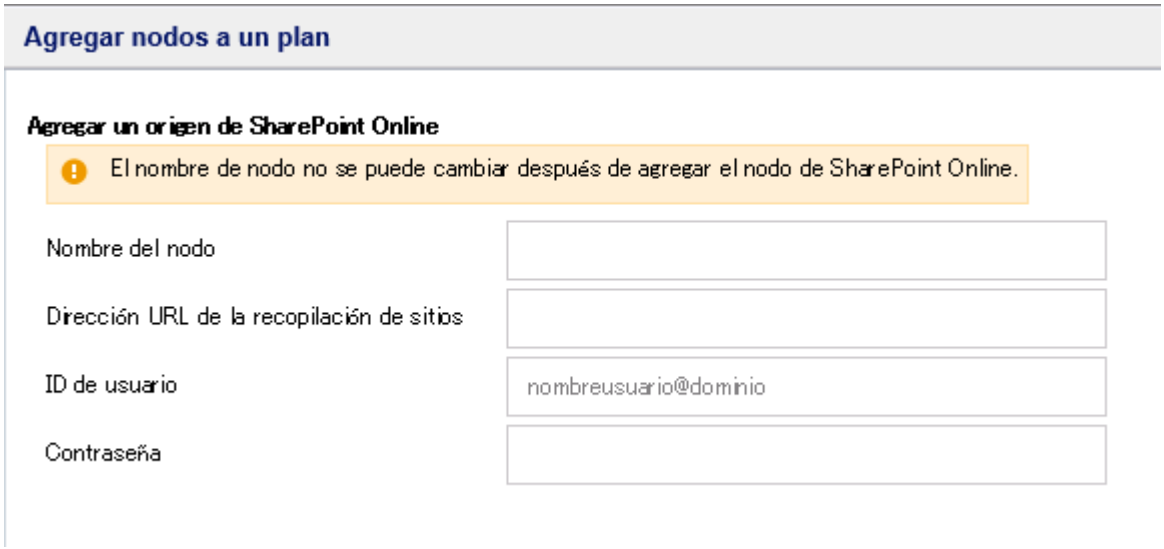
Adición de un nodo de SharePoint Online

Nota: A diferencia de otros nodos, no se puede agregar el nodo de SharePoint Online desde la página Todos los nodos. Solo se agrega un nodo de SharePoint Online a un plan al crear o modificar un plan.

Para obtener más información sobre cómo crear un plan, consulte Cómo crear un plan de SharePoint Online.

Siga estos pasos:

1. Introduzca el nombre de usuario del nodo de SharePoint e introduzca la dirección URL de la recopilación de sitios, el nombre de usuario del propietario del sitio y la contraseña.



2. Introduzca la contraseña y haga clic en **Conectar**.
3. Seleccione la lista o biblioteca de SharePoint, o los elementos de lista que se van a proteger.
4. Haga clic en **Guardar**.

   Se agregan las cuentas de SharePoint Online seleccionadas.

Actualización de un nodo de SharePoint Online

Al modificar las credenciales del nodo de SharePoint Online, actualice el nodo de SharePoint Online en la Consola.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Nodos de SharePoint Online**.

   Los nodos de SharePoint Online creados se muestran en el panel central.
3. Seleccione el nodo de SharePoint Online y haga clic en **Acciones**.
4. Haga clic en **Actualizar**.

   Aparece el cuadro de diálogo **Actualizar nodo**.
5. Modifique los detalles según sea necesario y haga clic en **Aceptar**.

   Se ha actualizado el nodo de SharePoint Online.

Supresión de un nodo de SharePoint Online

Suprima cualquier nodo de SharePoint Online que ya no se necesite.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. Vaya a **Nodos** y haga clic en **Nodos de SharePoint Online**.

   Los nodos de SharePoint Online creados se muestran en el panel central.
3. Seleccione el nodo de SharePoint Online y haga clic en **Acciones**.
4. Haga clic en **Suprimir**.

   Aparecerá un diálogo de confirmación.
5. Haga clic en **Aceptar**.

   Se ha suprimido correctamente el nodo de SharePoint Online.

Cómo gestionar el nodo de OneDrive

No se pueden agregar directamente los nodos de OneDrive a la vista de todos los nodos. Una vez se haya agregado el nodo al plan de copia de seguridad, se agregará directamente el nodo de OneDrive a la vista de todos los nodos.

Se pueden realizar las tareas siguientes:

1. Adición de un nodo de OneDrive
2. **Supresión del nodo:** En la opción Acciones en el nodo de OneDrive, haga clic en **Suprimir** y confirme en la ventana emergente que desea suprimir el nodo de la Consola.
3. **Exportación del nodo:** En la opción Acciones en el nodo de OneDrive, haga clic en **Exportar** y reciba el nodo como un archivo .zip.
4. **Modificación de un plan:** En la opción Acciones en el nodo de OneDrive, haga clic en **Modificar plan** para abrir el plan relacionado y actualícelo según sea necesario.
5. **Inicio de sesión en el Agente:** En la opción Acciones en el nodo de OneDrive, haga clic en **Iniciar sesión en el Agente** para realizar tareas específicas del Agente como, por ejemplo, la restauración utilizando la opción de montaje de volúmenes.
6. **Copia de seguridad ahora:** En la opción Acciones en el nodo de OneDrive, haga clic en **Realizar copia de seguridad ahora** para realizar la copia de seguridad manual.
7. **Restauración:** En la opción Acciones en el nodo de OneDrive, haga clic en **Restaurar** para iniciar la sesión en el Agente y realizar la restauración.
8. Descarga de un punto de recuperación de la nube

9. Actualización de un punto de recuperación en la nube
10. Copia de un punto de recuperación en el disco local o recurso compartido de red

Adición de un nodo de OneDrive

Nota: A diferencia de otros nodos, no se puede agregar el nodo de OneDrive desde la página Todos los nodos. Solo se agrega un nodo de OneDrive a un plan al crear o modificar un plan.

Para obtener información sobre cómo agregar el nodo, consulte la sección "Especificación del origen" en la página 1086 mientras se crea el plan de copia de seguridad de OneDrive.

Supresión de un nodo de OneDrive

Suprima cualquier nodo de OneDrive que ya no se necesite.

Siga estos pasos:

1. Haga clic en **Suprimir** en la opción **Acciones** en el nodo de OneDrive.
2. Confirme en la ventana emergente que desea suprimir el nodo de la Consola.

   Se ha suprimido correctamente el nodo de OneDrive.

Cómo gestionar los nodos del grupo de la base de datos de Oracle

Con Arcserve UDP, se pueden realizar varias acciones para gestionar los nodos de la base de datos de Oracle como, por ejemplo, actualizar el nodo, exportar el nodo, realizar la tarea de copia de seguridad, cancelar la tarea de copia de seguridad y suprimir un nodo.

Esta sección incluye los siguientes temas:

Actualización del nodo de la base de datos de Oracle

Se puede actualizar la información relacionada con los nodos existentes. Cuando se modifican las credenciales de los nodos de la base de datos de Oracle, se deben actualizar los nodos de la base de datos de Oracle en la Consola.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Haga clic en la ficha **recursos**.

   Se mostrará la página Nodos: Todos los nodos.

3. Realice uno de los procedimientos siguientes:
   - En el panel izquierdo, vaya a **Nodos**, **Grupo de la base de datos de Oracle**, haga clic con el botón secundario en el nodo que desea actualizar y, a continuación, haga clic en **Actualizar**.
   - En el panel central, seleccione el nodo que desea actualizar, haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Actualizar**.

   Aparece el cuadro de diálogo Actualizar nodo.
5. En el cuadro de diálogo Actualizar nodo, modifique los detalles según sea necesario y, a continuación, haga clic en **Aceptar**.

   El nodo de la base de datos de Oracle se actualiza.

Exportación de nodos

Se pueden exportar los nodos como archivo ZIP (.zip). Cuando sea necesario, se puede importar el archivo ZIP para retener los nodos. Por ejemplo, exportar los nodos antes de las actualizaciones o volver a arrancar le ayuda a importar el mismo conjunto de nodos.

Se pueden exportar solamente aquellos nodos que tengan credenciales válidas y que estén ejecutando el sistema operativo de Windows.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Haga clic en la ficha **recursos**.

   Se mostrará la página Nodos: Todos los nodos.
3. Realice uno de los procedimientos siguientes:
   - En el panel izquierdo, vaya a **Nodos**, **Grupo de la base de datos de Oracle**, haga clic con el botón secundario en el nodo que desea exportar y, a continuación, haga clic en **Exportar**.
   - En el panel central, seleccione el nodo que desea exportar, haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Exportar**.

   Se abre un cuadro de diálogo en el que se solicita su acción en el archivo list.zip.
4. Haga clic en **Abrir** o en **Guardar**.

   La lista de nodos se exporta.

Copia de seguridad del nodo de la base de datos de Oracle

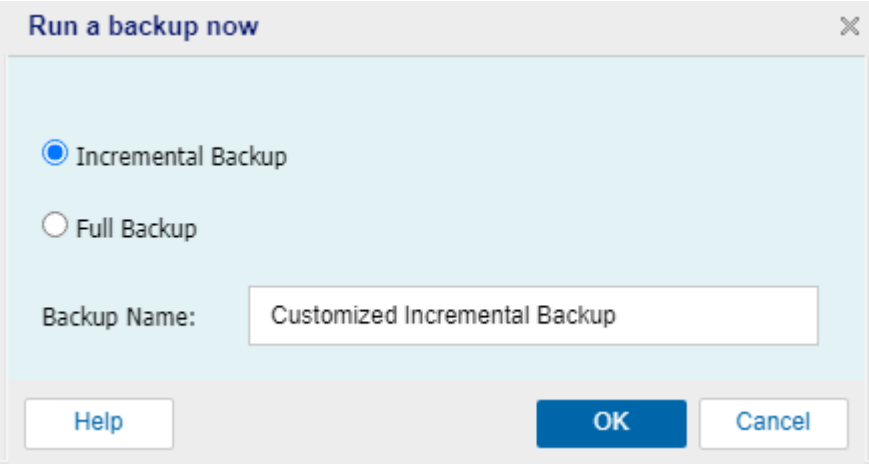
Normalmente se realizan copias de seguridad automáticamente y las controlan los valores de configuración de programación. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Haga clic en la ficha **recursos**.

   Se mostrará la página Nodos: Todos los nodos.
3. Realice uno de los procedimientos siguientes:
   - En el panel izquierdo, vaya a **Nodos**, **Grupo de la base de datos de Oracle**, haga clic con el botón secundario en el nodo del que desea realizar la copia de seguridad y, a continuación, haga clic en **Realizar copia de seguridad ahora**.
   - En el panel central, seleccione el nodo del que desea realizar la copia de seguridad, haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Realizar copia de seguridad ahora**.

   Aparece el cuadro de diálogo Ejecutar ahora una copia de seguridad.
4. En el cuadro de diálogo *Ejecutar una copia de seguridad ahora*, seleccione el tipo de copia de seguridad que desea realizar y, a continuación, especifique el nombre de la copia de seguridad si es necesario.



A continuación se especifican las opciones disponibles:

Copia de seguridad incremental

Inicia una copia de seguridad incremental del equipo. Una copia de seguridad incremental sólo hará una copia de seguridad de los bloques que han cambiado desde la copia de seguridad anterior.

Nota: Si está realizando una copia de seguridad por primera vez, la copia de seguridad completa se iniciará automáticamente aunque haya seleccionado la opción Copia de seguridad incremental.

Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Ésta es la manera más óptima de realizar copias de seguridad.

Copia de seguridad completa

Inicia una copia de seguridad completa del equipo o los volúmenes seleccionados.

Nota: Si no se especifica ningún nombre de copia de seguridad, de forma predeterminada se llamará Copia de seguridad incremental o completa personalizada.

5. Haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.

6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.

   La tarea de copia de seguridad se realiza correctamente.

Cancelación de la tarea de copia de seguridad de los nodos de la base de datos de Oracle

Después de iniciar la tarea de copia de seguridad de los nodos de la base de datos de Oracle, se podrá cancelar la tarea de copia de seguridad en cualquier momento. Cuando se cancela la tarea de copia de seguridad, la copia de seguridad se detiene inmediatamente.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página Nodos: Todos los nodos.

3. Realice uno de los procedimientos siguientes:

   - En el panel izquierdo, vaya a **Nodos**, **Grupo de la base de datos de Oracle**, haga clic con el botón secundario del ratón en el nodo para el que desea

cancelar la copia de seguridad y, a continuación, haga clic en **Cancelar**.

- En el panel central, seleccione el nodo para el cual desea cancelar la copia de seguridad, haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Cancelar**.

Aparecerá un mensaje de confirmación.

5. Haga clic en **Sí** para confirmar.

   Se cancela la tarea de copia de seguridad correctamente.

Supresión de los nodos de la base de datos de Oracle

Se pueden suprimir los nodos de la base de datos de Oracle que ya no se necesite. Si se suprimen los nodos, también se suprimirán los registros y los historiales de tareas asociados. Se puede agregar el nodo suprimido más tarde si fuese necesario.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.

   Se mostrará la página Nodos: Todos los nodos.

3. Realice uno de los procedimientos siguientes:

   - En el panel izquierdo, vaya a **Nodos**, **Grupo de la base de datos de Oracle**, haga clic con el botón secundario en el nodo que desea suprimir y, a continuación, haga clic en **Suprimir**.
   - En el panel central, seleccione el nodo que desea suprimir, haga clic en la lista desplegable **Acciones** y, a continuación, haga clic en **Suprimir**.

   Aparecerá un mensaje de confirmación.

5. Haga clic en **Sí** para confirmar.

   El nodo se suprime correctamente de la Consola.

Capítulo 9: Adición y gestión de destinos

Esta sección incluye los siguientes temas:

Cómo agregar un destino

Un destino es una ubicación donde se almacenan los datos de la copia de seguridad. Arcserve UDP permite agregar varios tipos de destinos.

Qué hacer a continuación:

1. Adición de un destino utilizando el servidor de puntos de recuperación
2. Adición de servidores de Arcserve Backup
3. Adición de una consola remota
4. Adición de una cuenta de la nube
5. Adición de una cuenta de la nube de Arcserve

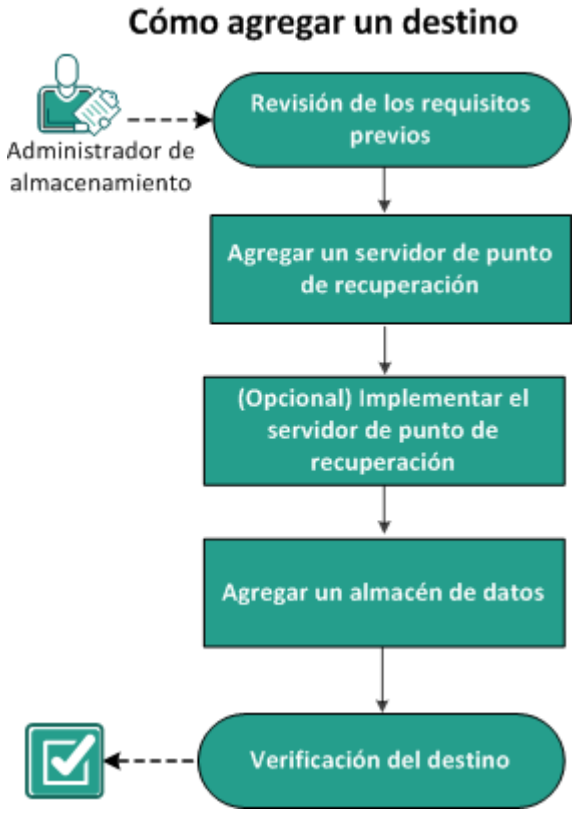
Cómo agregar un destino

Para Arcserve UDP, se puede asignar un servidor de puntos de recuperación (RPS) como destino central. Se pueden almacenar datos de varios nodos en un servidor de puntos de recuperación y, a continuación, recuperar los datos cuando sea necesario. El agregar un destino ante todo implica dos pasos:

a. Adición de un servidor de puntos de recuperación a la consola.

b. Adición de un almacén de datos al servidor de puntos de recuperación.

El diagrama siguiente ilustra cómo agregar un destino:



¿Qué hacer a continuación?

1. Revise de los requisitos previos
2. Cómo agregar un servidor de puntos de recuperación
3. (Opcional) Implementación del servidor de puntos de recuperación
4. Como agregar un almacén de datos
5. Verificación del destino

Revisión de los requisitos previos

Antes de configurar un servidor de punto de recuperación, complete los requisitos previos siguientes:

- Revise las Notas de la versión para obtener una descripción de los requisitos del sistema, los sistemas operativos compatibles y una lista de los problemas conocidos existentes en esta versión de Arcserve Unified Data Protection.
- Verifique que dispone de privilegios de administrador para instalar Arcserve Unified Data Protection.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Cómo agregar un servidor de puntos de recuperación

La adición de un destino empieza con la adición de un servidor de puntos de recuperación a la consola. Más tarde, se agregan almacenes de datos al servidor de puntos de recuperación.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de puntos de recuperación**.

   Se muestra la página **Destinos: servidores de puntos de recuperación** en el panel central.
3. Haga clic en **Agregar un servidor de puntos de recuperación**.

   Se muestra la página **Agregar un servidor de puntos de recuperación**.
4. Introduzca los siguientes detalles:

   Nombre del nodo/Dirección IP

   Define el nombre del nodo del servidor de puntos de recuperación que se desea agregar a la Consola.

   Nombre de usuario y Contraseña

   Define el nombre de usuario y la contraseña para iniciar sesión en el nodo.

   Nota: Utilice uno de los siguientes formatos para el nombre de usuario: Nombre del equipo, nombre de dominio/nombre de usuario o nombre de usuario.

   Descripción

   (Opcional) Define cualquier información adicional acerca del nodo.
5. Introduzca los campos siguientes para los **Valores de configuración de la instalación**:

   Nota: Si el nodo ya tiene el servidor de puntos de recuperación instalado, ignore estos valores de configuración de la instalación.

   Ubicación de la instalación

   Especifique la ubicación donde desea instalar el servidor de puntos de recuperación. Se puede aceptar la ruta predeterminada o bien se puede especificar una ruta alternativa.

   Puerto

   Especifica el número de puerto que se conecta a la interfaz de usuario web.

   Valor predeterminado: 8014

Protocolo

Especifique el protocolo que se desea utilizar para comunicarse con el servidor de destino. Las selecciones disponibles son HTTP y HTTPS.

Nota: Para una comunicación más segura, seleccione el protocolo HTTPS.

Controlador de seguimiento de cambios

Especifique si desea **Instalar el controlador de seguimiento de cambios del agente**.

6. Programe la instalación o actualización seleccionando una de las opciones de **Hora de inicio de la instalación o actualización**.

   Nota: Si el servidor ya tiene el servidor de punto de recuperación instalado, ignore estos valores de configuración.

7. Haga clic en **Guardar**.

   El progreso de la implementación se muestra en el panel derecho. El servidor de puntos de recuperación se agrega.

   Ahora, el servidor de puntos de recuperación se implementa. Una vez agregado el servidor de puntos de recuperación, se pueden agregar almacenes de datos.

(Opcional) Implementación del servidor de punto de recuperación

Mediante Arcserve Unified Data Protection, se puede detectar e implementar la última versión del componente Servidor de puntos de recuperación (RPS) en los servidores de puntos de recuperación. Después de implementar el componente del servidor de punto de recuperación RPS, el nodo está preparado de almacenar las sesiones de copia de seguridad y funcionar como un servidor de punto de recuperación.

Nota: Los componentes del servidor de puntos de recuperación se instalan con la instalación de Arcserve Unified Data Protection.

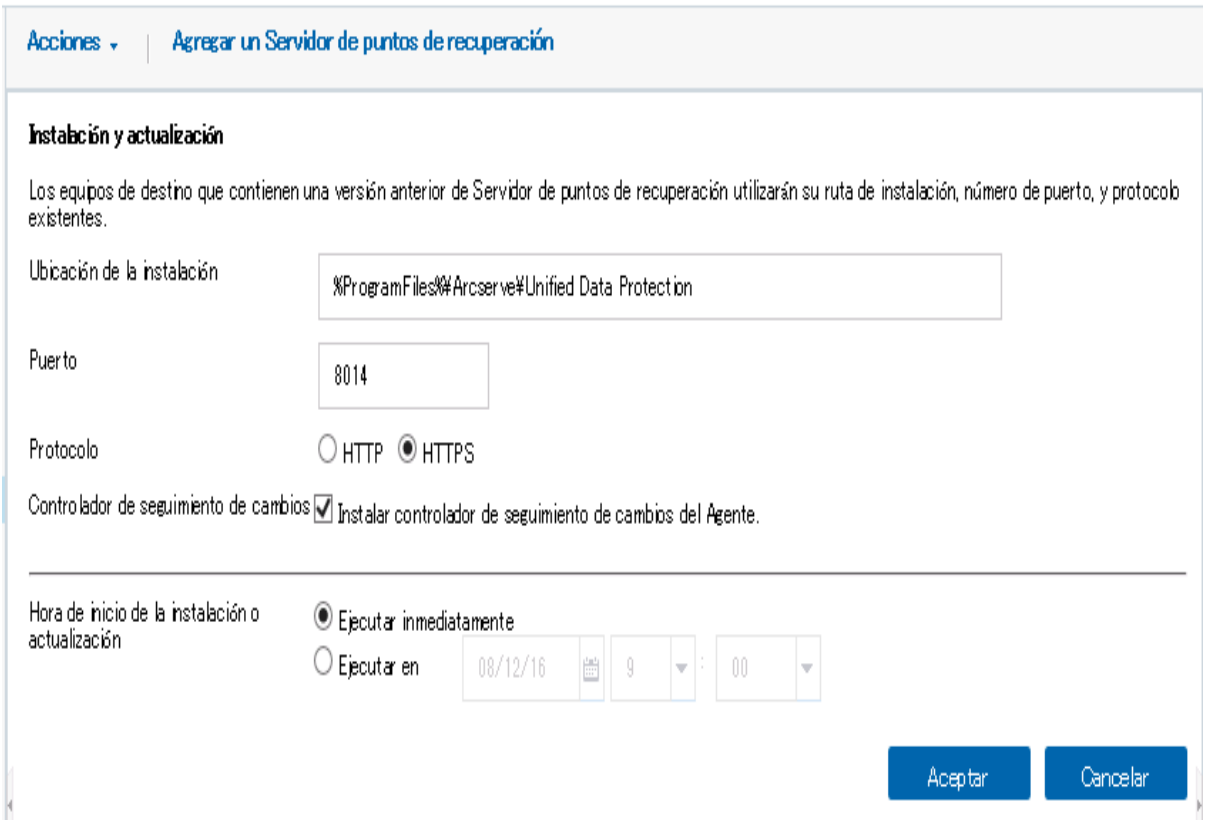
Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se muestra la página **Destino:Servidor de punto de recuperación**.
3. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en un servidor de punto de recuperación.
   - Seleccione un servidor de punto de recuperación y en el panel central haga clic en la lista desplegable **Acciones**.

   Aparecerá una lista de opciones.
4. Haga clic en **Instalar o actualizar el servidor de punto de recuperación**.

   Se muestra la página **Instalación y actualización**.



5. Modifique los valores de configuración de la implementación y haga clic en **Aceptar** para implementar el servidor de puntos de recuperación en el nodo seleccionado.

   La implementación del servidor de punto de recuperación se inicia. Se puede ver el progreso de la implementación en el panel derecho.

Adición de un almacén de datos

Para crear el destino, el servidor de punto de recuperación necesita almacenes de datos. El almacén de datos especifica donde se almacenan los datos de copia de seguridad. Se pueden agregar varios almacenes de datos a un servidor de puntos de recuperación.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se muestra la página **Destinos: Servidores de punto de recuperación**.
3. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en un servidor de punto de recuperación.
   - Seleccione un servidor de punto de recuperación y en el panel central haga clic en la lista desplegable **Acciones**.

   Aparecerá una lista de opciones.
4. Haga clic en **Agregar un almacén de datos**.

   Se muestra la página **Crear un almacén de datos** con el nombre del servidor de punto de recuperación especificado.
5. Rellene los siguientes campos y, a continuación, haga clic en **Guardar**.

   Servidor de puntos de recuperación

   Define el servidor de puntos de recuperación en el que se crea el almacén de datos. El servidor de puntos de recuperación ya está agregado de forma predeterminada.

   Nombre del almacén de datos

   Define el nombre del almacén de datos.

   Carpeta del almacén de datos

   Define la ubicación de la ruta para la carpeta donde se crea el almacén de datos. Haga clic en Examinar para seleccionar carpeta de destino.

   Notas:

   - Ahora se puede activar y ver los volúmenes ocultos. Para obtener más información, consulte Cómo activar y ver volúmenes ocultos al crear un

almacén de datos.

- Para el almacén de datos de deduplicación y de no deduplicación, la ruta de destino debe ser una carpeta vacía.

Límite de nodos activos simultáneos

Especifica el número máximo de tareas simultáneas en el almacén de datos.

Valor predeterminado: 4

hace referencia a un valor del 1 al 9999. El valor indica el número de tareas que se pueden ejecutar simultáneamente. Si las tareas en ejecución cumplen el número, otra tarea se coloca en la cola y la tarea solo puede iniciarse cuando una de las tarea en ejecución se completa. La tarea completada puede significar una tarea finalizada, cancelada o errónea.

El número se aplica a los Tipos de trabajo pero no a los nodos del servidor. Por ejemplo, el número 5 indica que se están ejecutando cinco tareas de copia de seguridad. Cualquier tarea programada para después de estas cinco tareas de copia de seguridad espera en la cola, pero se puede enviar otra tarea, como Catálogo del sistema de archivos.

Si el valor es más de 16 o 32, se muestran mensajes para advertir sobre el aumento de la demanda en el hardware.

Nota: El limitar el número solamente tiene un efecto en la tarea de salida de la replicación, no en la tarea de entrada de la replicación. El límite para contar no impacta en las tareas de restauración o de reconstrucción completa. Estas tareas no se colocan en una cola.

Activación de la deduplicación

Especifica que la deduplicación se activa para este almacén de datos. Arcserve UDP es compatible con los dos tipos de deduplicación: Deduplicación de origen y Deduplicación global. La deduplicación de origen impide que los bloques de datos duplicados se muevan a través de la red desde un agente concreto. La deduplicación global elimina los datos duplicados a través de todos los equipos cliente basándose en el nivel del clúster de volumen.

Tamaño de bloque de la deduplicación

Define el tamaño de bloque de la deduplicación. Las opciones son 4 kB, 8 kB, 16 kB, 32 kB y 64 kB. El tamaño de bloque de la deduplicación también tiene un impacto en la estimación de la capacidad de la deduplicación. Por ejemplo, si se cambia el valor predeterminado de 16 kB a 32 kB, las estimaciones de la capacidad de la deduplicación se doblan. Al aumentar el tamaño de bloque de la deduplicación se puede reducir el porcentaje de deduplicación.

Adjudicación de memoria hash

Especifica la cantidad de memoria física que se adjudica para mantener los hash. Este campo se rellena previamente con un valor predeterminado. El valor predeterminado se basa en el siguiente cálculo:

Si la memoria física del punto de recuperación es inferior a 4 GB (o es idéntica a 4 GB), el valor predeterminado de **Adjudicación de memoria hash** es idéntico al de la memoria física del servidor de puntos de recuperación.

Si la memoria física del servidor de puntos de recuperación es mayor de 4 GB, Arcserve UDP calcula la memoria libre disponible en ese momento. Suponga que la memoria libre disponible asciende a X GB en ese momento. Arcserve UDP también comprueba las siguientes condiciones:

- Si (X * 80 %) > 4 GB, el valor predeterminado de **Adjudicación de memoria hash** es (X * 80 %).
- Si (X * 80 %) ≤ 4 GB, el valor predeterminado de **Adjudicación de memoria hash** es 4 GB.

Ejemplo: Imagine que el servidor de puntos de recuperación cuenta con 32 GB de memoria física. Asuma que el sistema operativo y otras aplicaciones utilizan 4 GB de memoria a la hora de crear el almacén de datos. Por lo tanto, la memoria libre disponible en este momento es de 28 GB. El valor predeterminado de **Adjudicación de memoria hash** es 22,4 GB (22,4 GB = 28 GB * 80 %).

El destino de hash está en una unidad de estado sólido (SSD)

Especifica si la carpeta de hash está en una unidad de estado sólido.

Nota: Se debe configurar el destino de hash en la unidad de estado sólido (SSD) local si la opción El destino de hash está en una unidad de estado sólido (SSD) está activada.

Destino de los datos

Define la carpeta de destino de los datos para guardar los bloques de datos únicos reales. Use el disco más grande para almacenar datos ya que contiene los bloques de datos originales del origen.

Nota: La ruta de **Destino de los datos** debe ser una carpeta en blanco.

Destino del índice

Define la carpeta de destino del índice para almacenar los archivos de índice. Elija un disco diferente para mejorar el procesamiento de la deduplicación.

Nota: La ruta de **Destino del índice** debe ser una carpeta en blanco.

Destino de hash

Define la ruta para almacenar la base de datos de hash. Arcserve UDP emplea el algoritmo SHA1 para generar el hash de los datos de origen. Los valores de hash se gestionan mediante la base de datos de hash. Si se selecciona una unidad de estado sólido (SSD), se aumentará la capacidad de deduplicación y se reducirá la adjudicación de memoria necesaria. Para mejorar el rendimiento de hash, se recomienda formatear el volumen de SSD como sistema de archivos NTFS con el tamaño del clúster de volúmenes de 4 kB.

Nota: La ruta de **Destino de hash** debe ser una carpeta vacía.

Nota: No se puede especificar la misma ruta para las cuatro carpetas siguientes: **Almacén de datos, Destino de los datos, Destino del índice** y **Destino de hash**.

Activación de la compresión

Especifica que se ha activado la configuración de compresión de datos.

Tipo de compresión

Especifica si se debe utilizar el tipo de compresión estándar o máxima.

La compresión se realiza muchas veces para reducir el uso del espacio en disco, pero también tiene un efecto contrario en la velocidad de la copia de seguridad dado el incremento del uso de la CPU. Basándose en los requisitos, se puede seleccionar una de las tres opciones disponibles.

Nota: Para obtener más información, consulte Tipo de compresión.

Activación del cifrado

Especifica que se han activado los valores de configuración de cifrado. Cuando se selecciona esta opción, se debe especificar y confirmar la contraseña de cifrado.

El cifrado de datos es la traducción de los datos a una forma que resulte ininteligible sin un mecanismo de descifrado. La solución Arcserve Unified Data Protection utiliza algoritmos de cifrado seguros AES (Estándar de cifrado avanzado) para lograr la máxima seguridad y privacidad de los datos. Para los almacenes de datos, se es compatible tanto con el Cifrado como con Sin cifrado. Para Cifrado, solamente AES-256 está disponible.

No será necesaria ninguna contraseña si la restauración se realiza en el equipo desde donde se ha realizado la copia de seguridad. Sin embargo, sí será necesaria una contraseña si se intenta realizar la restauración en otro equipo. De forma predeterminada, solo se necesita una contraseña para el primer inicio de sesión. Para introducir la contraseña incluso después del primer inicio de sesión, el administrador debe detener manualmente el servicio de extensión del explorador del Agente de Arcserve UDP.

Enviar una alerta de correo electrónico cuando un destino se está acercando a su plena capacidad

Al seleccionar esta opción, se configurará el almacén de datos para que envíe alertas de correo electrónico. El servidor de puntos de recuperación envía alertas de correo electrónico a los destinatarios cuando la carpeta de destino del almacén de datos se está acercando a su plena capacidad.

Configurar correo electrónico

Este botón solo aparece cuando se activa la opción *Enviar una alerta de correo electrónico cuando un destino se está acercando a su plena capacidad*. El botón le ayuda a proporcionar un ID de correo electrónico para recibir alertas. Haga clic en el botón **Configurar correo electrónico** para cargar la configuración global de alertas de correo electrónico en Consola > Configuración > Configuración del correo electrónico y de alertas. Si la configuración global del correo electrónico no está disponible, al hacer clic en el botón **Configurar correo electrónico** se abre el cuadro de diálogo **Configuración del correo electrónico** para establecer los detalles del correo electrónico.

El almacén de datos se crea y se muestra en el panel central. Haga clic en el almacén de datos para ver los detalles en el panel derecho.

Diversos estados del almacén de datos

El almacén de datos muestra diferentes estados en función de la tarea realizada por el almacén de datos. Cuando se selecciona un almacén de datos desde la ficha **recursos**, el estado del almacén de datos se muestra en el panel derecho

- **Detenido:** El almacén de datos está inactivo. No se puede enviar ninguna tarea en este estado.
- **Iniciando**: El almacén de datos se está iniciando. Cuando se está iniciando el almacén de datos, el progreso se muestra en la consola.
- **En ejecución:** El almacén de datos está activo. Se pueden enviar tareas en este estado.
- **Detención:** El almacén de datos se está deteniendo. Cuando se está deteniendo el almacén de datos, el progreso se muestra en la consola.
- **Modificación**: El almacén de datos se está actualizando con nuevos datos. Cuando se está modificando el almacén de datos, el progreso se muestra en la consola.
- **Supresión**: El almacén de datos se está suprimiendo. Cuando se está suprimiendo el almacén de datos, el progreso se muestra en la consola.
- **Fuera de servicio:** El almacén de datos no está funcionando correctamente. No se puede enviar ninguna tarea en este estado. Detenga el almacén de datos y verifique el motivo de este comportamiento. Los siguientes casos pueden dar como resultado el estado Fuera de servicio de un almacén de datos:
  - No se puede acceder al destino de la copia de seguridad del almacén de datos.
  - Las configuraciones del archivo o del registro están dañadas.
  - El rol de índice o datos de GDD tiene errores internos.
  - Se ha detenido manualmente el proceso de rol de índice o datos de GDD.
- **Restaurar solo**: En el estado Restaurar solo, no se ejecuta ninguna tarea que deba escribir datos en el almacén de datos. Tareas como las de copia de seguridad, de replicación (entrada), de JumpStart (entrada) y de migración de datos. Las demás tareas se ejecutan, las que necesitan leer datos del almacén de datos. El estado del almacén de datos cambia a Restaurar solo en las siguientes condiciones:

- Cuando el proceso de rol de hash se detiene manualmente.
- Cuando la memoria de hash asignada o la capacidad del volumen de la ruta de destino/datos/índice/hash alcanza su límite máximo.

Importante: Cuando el estado del almacén de datos es Restaurar solo (estado degradado) o Fuera de servicio (mal estado), el almacén de datos no funcionará correctamente. Se debe detener el almacén de datos y comprobar la causa raíz del estado. Por ejemplo, es posible que el problema sea que el volumen de deduplicación de datos haya alcanzado el máximo. Después de solucionar la causa raíz, inicie el almacén de datos y vuelva a enviar la tarea de copia de seguridad.

Verificación del destino

Después de completar todos los procedimientos implicados en cómo agregar un servidor de punto de recuperación, verifique si el servidor de punto de recuperación se ha agregado correctamente.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destinos: servidores de punto de recuperación**.
3. Verifique los siguientes detalles:
   - Se muestra el servidor de punto de recuperación creado.
   - Los almacenes de datos se muestran bajo el servidor de punto de recuperación.

Agregar servidores de Arcserve Backup

Agregar un servidor de Arcserve Backup para replicar datos a una cinta. Cuando se crea un plan para archivar datos en un dispositivo de cinta, se puede utilizar este destino.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de Arcserve Backup**.

   Se mostrará la página **Destinos: servidores de Arcserve Backup** en el panel central.
3. Haga clic en **Agregar un servidor de Arcserve Backup**.

   Se muestra la página **Agregar un servidor de Arcserve Backup**.
4. Introduzca los siguientes detalles:

   Nombre del nodo/Dirección IP

   Especifica el nombre de nodo o la dirección IP del servidor de Arcserve Backup.

   Tipo de autenticación

   Especifica el tipo de autenticación utilizado para iniciar sesión en el servidor de Arcserve Backup. Están disponibles las dos opciones siguientes:

   Autenticación de Windows

   Especifica que se utilizará la autenticación de Windows para iniciar sesión en el servidor de Arcserve Backup.

   Nota: El usuario de Windows se debe registrar primero en Arcserve Backup utilizando el Gestor de perfiles de usuario de Arcserve Backup.

   Autenticación de Arcserve Backup

   Especifica que se utilizará la autenticación de Arcserve Backup para iniciar sesión en el servidor de Arcserve Backup.

   Nombre de usuario y Contraseña

   Especifica el nombre de usuario y la contraseña para ayudar a iniciar sesión en el nodo.

   Nota: Utilice uno de los siguientes formatos para el nombre de usuario: nombre del equipo, nombre de dominio/nombre de usuario o nombre de usuario.

   Puerto

Especifica el número de puerto que se utiliza para conectarse al servidor de Arcserve Backup.

Nota: Arcserve UDP utiliza el número de puerto para conectarse a los dos servidores, es decir, al servidor primario de Arcserve Backup y al servidor miembro en el dominio de Arcserve Backup.

5. Haga clic en **Guardar**.

   El servidor de Arcserve Backup se ha agregado a la Consola.

   Después de agregar el servidor de Arcserve Backup a la Consola, puede desplazarse hasta **recursos, Destino, Servidores de Arcserve Backup**y comprobar la información detallada de los medios de cinta.

Adición de una consola remota

Agregue una consola remota para replicar los puntos de recuperación en un servidor de punto de recuperación gestionado de forma remota. Se puede utilizar la consola remota para crear un plan de replicación para enviar datos a la consola de destino. También se puede gestionar la consola remota agregada.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Consola remota**.

   Se muestra la página **Destinos: Consola remota** en el panel central.
3. Haga clic en **Agregar una consola remota**.

   Se muestra la página **Adición de una consola remota**
4. Introduzca los siguientes detalles:

   Consola remota

   Hace referencia a la dirección URL de la cuenta de la consola remota que se desea agregar a la consola.

   Nombre de usuario

   Hace referencia al nombre de usuario que ayuda a iniciar una sesión en la consola remota.

   Nota: Utilice uno de los siguientes formatos para el nombre de usuario: Nombre del equipo, nombre de dominio/nombre de usuario o nombre de usuario.

   Contraseña

   Se refiere a la contraseña del nombre de usuario.

   Puerto

   Hace referencia al número de puerto que se conecta a la interfaz de usuario basada en la Web.

   Valor predeterminado: 8015

   Protocolo

   Especifique el protocolo que se desea utilizar para comunicarse con el servidor de destino. Las selecciones disponibles son HTTP y HTTPS.

   Nota: Para una comunicación más segura, seleccione el protocolo HTTPS.

   Configuración proxy

Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

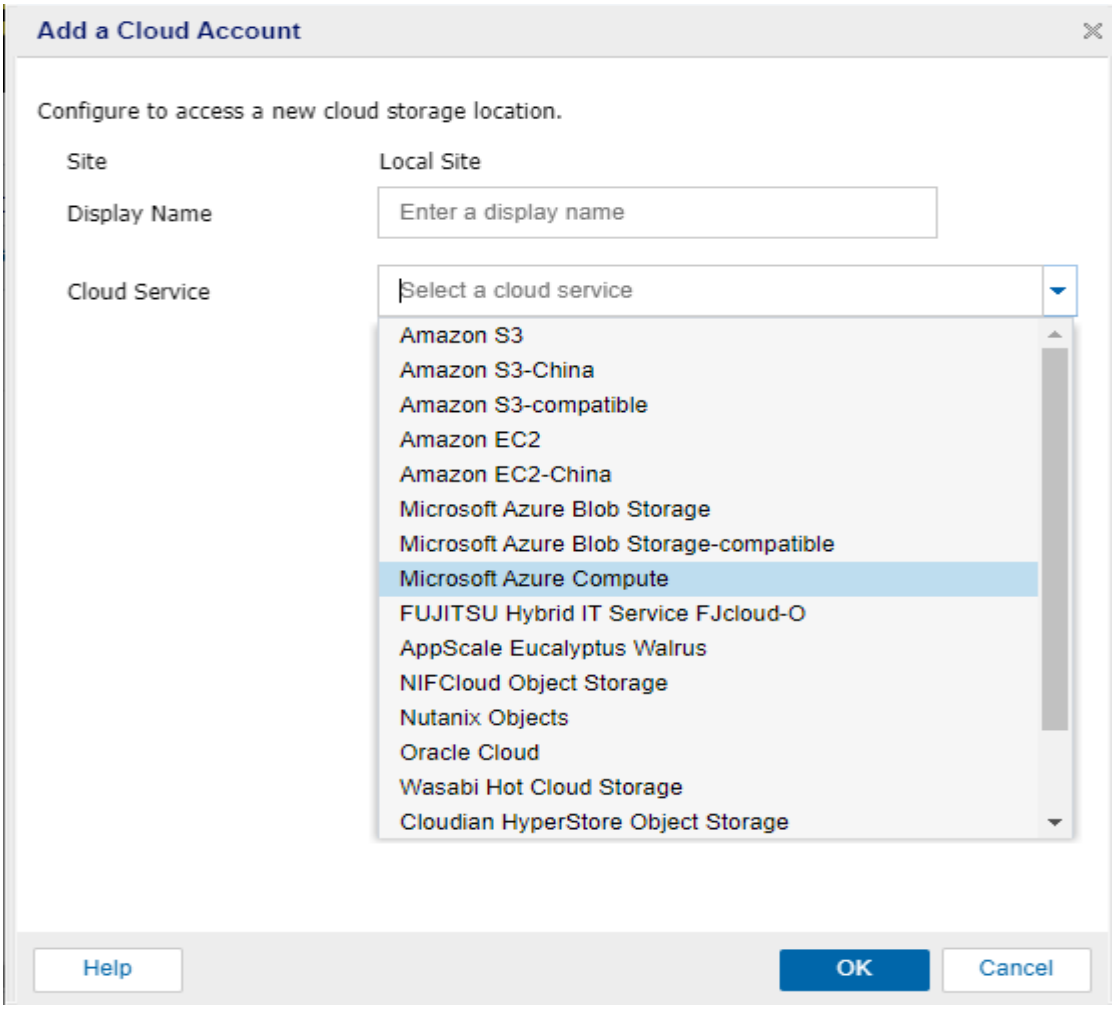
5. Haga clic en **Aceptar**.

   Ahora se ha agregado la consola remota.

Adición de una cuenta de la nube

Agregue una cuenta en la nube para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se pueden utilizar cuentas relacionadas al crear tareas o uno o más planes en Copia de punto de recuperación/Copia de archivo/Archivado de archivos/Virtual Standby a la nube/Máquina virtual instantánea en Amazon EC2. Proporcione un nombre único de almacenamiento y seleccione el servicio de almacenamiento necesario en las diversas opciones que se muestran en la lista desplegable.

Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.



Las opciones de configuración para cada distribuidor de la nube son similares (con una terminología diferente) y se describe cualquier diferencia patente. Agregue una cuenta de la nube de su elección.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

   El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.
5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.
6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   Las opciones disponibles del servicio de almacenamiento son Amazon S3, Compatible con Amazon S3, Almacenamiento de blobs de Microsoft Azure, Compatible con el Almacenamiento de blobs de Microsoft Azure, FUJITSU Hybrid IT Service FJcloud-O, AppScale Eucalyptus Walrus, Amazon EC2, Amazon EC2-China, Microsoft Azure Compute, Nutanix Objects, Wasabi Hot Cloud Storage y Oracle Cloud.

   Nota: Haga clic en los nombres de servicios de almacenamiento para ver cómo agregar una cuenta de la nube a ese servicio de almacenamiento.

   La opción de configuración varía en función del servicio de almacenamiento que se haya seleccionado.

   La cuenta de la nube del servicio de almacenamiento seleccionada se agrega a la Consola de Arcserve UDP y se muestra en la pantalla **Destinos: Cuentas de la nube**.

Por ejemplo, las cuentas de Amazon S3 se muestran a continuación.



¿Qué hacer a continuación?

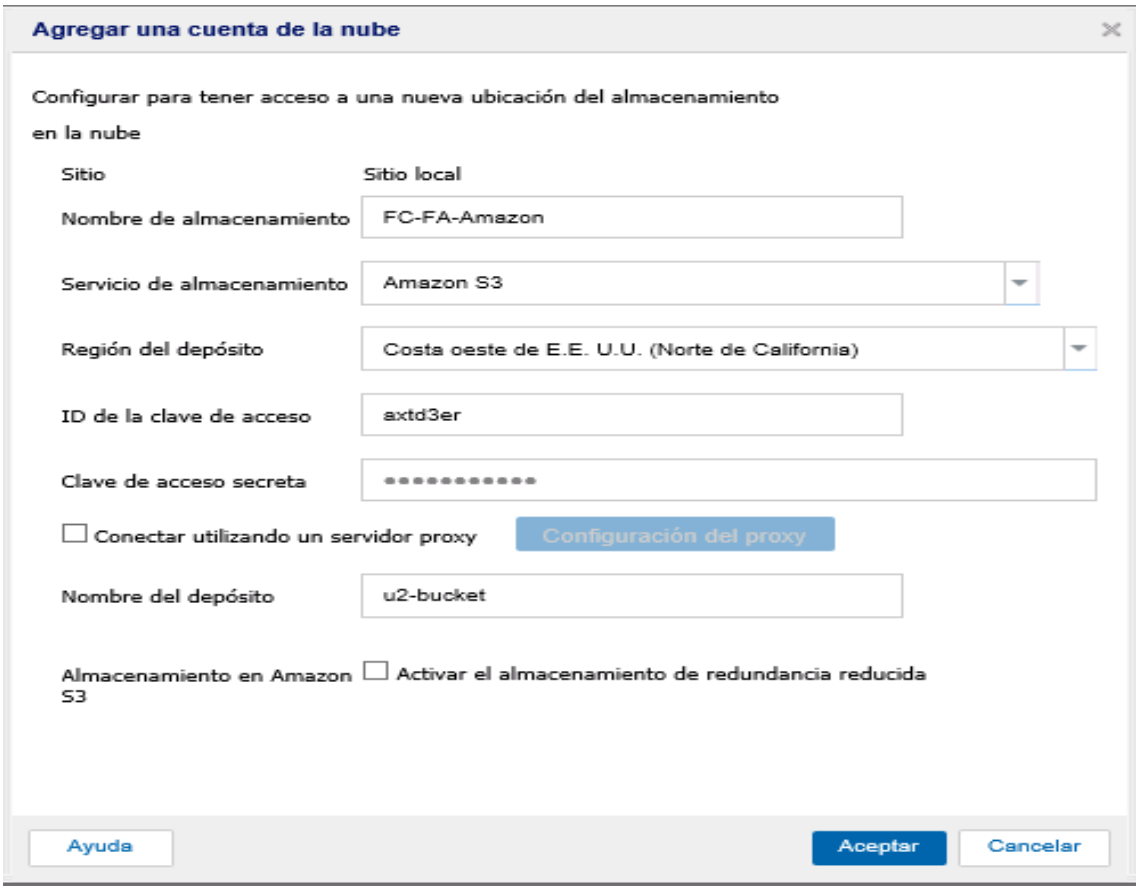
Agregue una cuenta de la nube para:

- Amazon S3
- Compatible con Amazon S3
- Almacenamiento de blobs de Microsoft Azure
- Compatible con Almacenamiento de blobs de Microsoft Azure
- FUJITSU Hybrid IT Service FJcloud-O
- AppScale Eucalyptus Walrus
- Amazon EC2
- Amazon EC2-China
- Microsoft Azure Compute
- Nutanix Objects
- Wasabi Hot Cloud Storage
- Oracle Cloud

Adición de una cuenta de la nube para Amazon S3

Se debe agregar una cuenta de la nube de Amazon S3 para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube.

Se puede utilizar esta cuenta mientras se crean las tareas Copia de punto de recuperación / Copia de archivo /Archivado de archivos.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

   El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.

5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.

6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   Zona de depósito

   Se refiere a la región del depósito en Amazon.

   ID de clave de acceso

   Identifica el usuario que solicita acceso a esta ubicación.

   Clave de acceso secreta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la clave de acceso no está cifrada.

   Importante: Esta clave de acceso secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave de acceso secreta en una página Web ni en otro código de origen accesible públicamente ni la transmita a través de canales no seguros.

   Configuración proxy

   Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

   Nombre de depósito

   Todos los archivos y las carpetas movidos o copiados al distribuidor de la nube se almacenan y se organizan en los depósitos. Los depósitos son como un contenedor para los archivos y se utilizan para agrupar y organizar objetos conjuntamente. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

   Activar el almacenamiento de redundancia reducida

   Para Amazon S3 solamente, esta opción permite la selección para activar el almacenamiento de redundancia reducida (RRS). RRS es una opción de almacenamiento de Amazon S3 que facilita la reducción de costes a través del

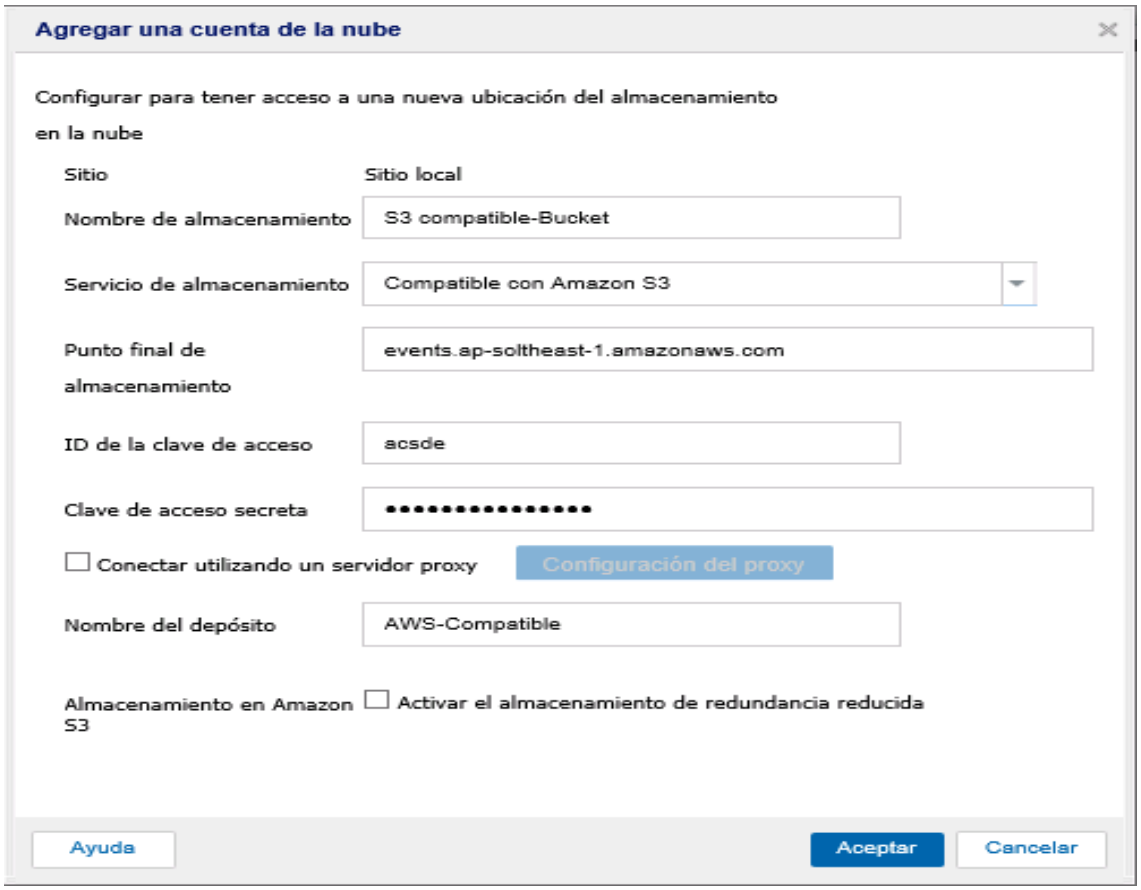
almacenamiento de datos no críticos y reproducibles a niveles de redundancia más bajos que el almacenamiento estándar de Amazon S3. Ambas opciones de almacenamiento de redundancia estándares y reducidas almacenan datos en diferentes funcionalidades y dispositivos, pero con RRS los datos se replican menos veces, de modo que el coste es menor. Se debería esperar la misma latencia y rendimiento mediante el almacenamiento estándar de Amazon S3 o RRS. De forma predeterminada, esta opción no está seleccionada (Amazon S3 utiliza la opción de almacenamiento estándar).

La cuenta de la nube se agrega a la consola.

Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube compatible con Amazon S3

Se debe agregar una cuenta de la nube compatible con Amazon S3 para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se puede utilizar esta cuenta mientras se crean las tareas Copia de punto de recuperación / Copia de archivo /Archivado de archivos.



Notas:

- En el caso de los subdistribuidores de S3 o compatibles con S3 que utilizan el tipo de autenticación V3/V2 para obtener la certificación con Arcserve CCI, se debe conservar el indicador de anulación de tipo de firmante establecido en **True** de forma predeterminada. Sin embargo, para los subdistribuidores que utilizan la autenticación V4, se debe cambiar el indicador a **False** en el archivo AmazonPlugin.properties y reiniciar los servicios.

  SIGNER_OVERRIDE=false

- Para admitir la nube de HGST en la opción Compatible con Amazon S3, se debe modificar lo siguiente en el archivo AmazonPlugin.properties:

  SET_STORAGECLASS_HEADER=false

Esta propiedad permite omitir el encabezado de almacenamiento. De este modo, si se utiliza esta propiedad cuando se agrega una tarea de copia o de archivado de archivos con Amazon como destino de la nube, el encabezado de almacenamiento se omite de manera predeterminada.

El archivo AmazonPlugin.properties se encuentra en la siguiente ubicación:

C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN\CCI\Config

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

   El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.
5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.
6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   Punto final del almacenamiento

   Especifica la dirección URL del servicio distribuidor. Por ejemplo, *http:///[nombre servidor]:número puerto*

   ID de clave de acceso

   Identifica el usuario que solicita acceso a esta ubicación.

   Clave de acceso secreta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la clave de acceso no está cifrada.

   Importante: Esta clave de acceso secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave de acceso secreta en una página Web ni

en otro código de origen accesible públicamente ni la transmita a través de canales no seguros.

Configuración proxy

Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

Nombre de depósito

Todos los archivos y las carpetas movidos o copiados al distribuidor de la nube se almacenan y se organizan en los depósitos. Los depósitos son como un contenedor para los archivos y se utilizan para agrupar y organizar objetos conjuntamente. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

Activar el almacenamiento de redundancia reducida

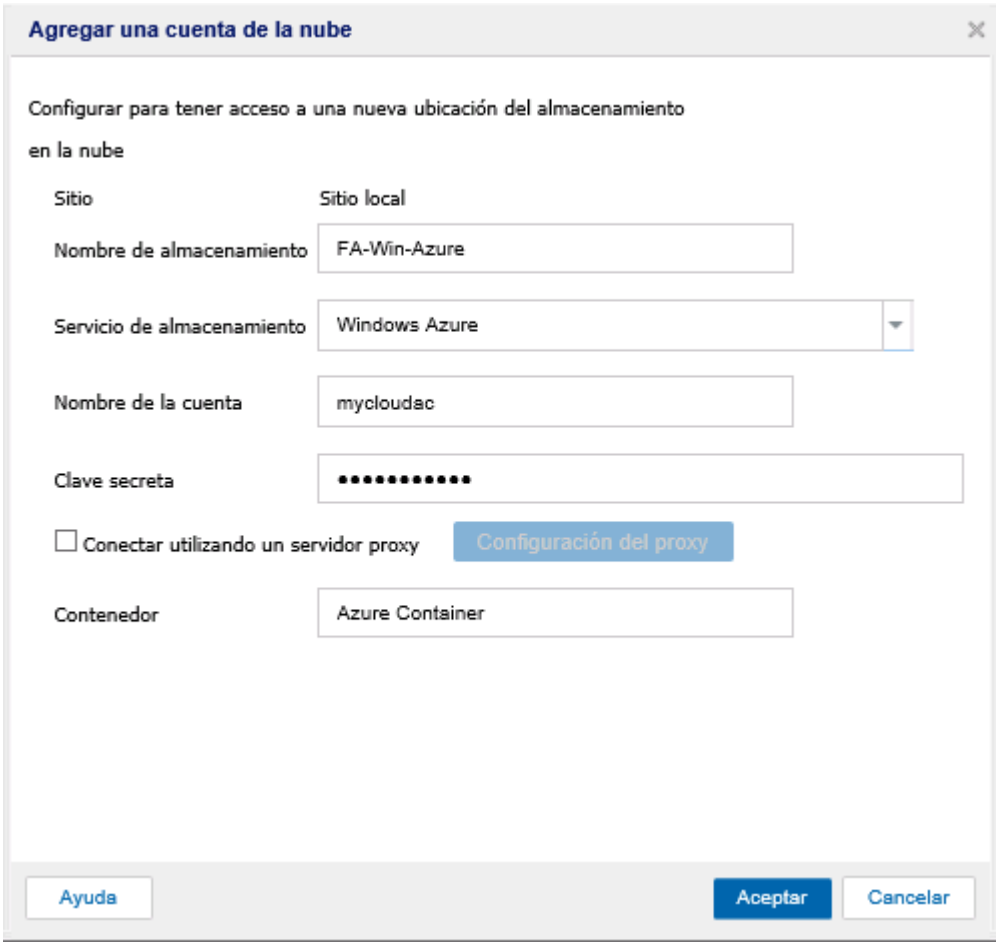
Para Amazon S3 solamente, esta opción permite la selección para activar el almacenamiento de redundancia reducida (RRS). RRS es una opción de almacenamiento de Amazon S3 que facilita la reducción de costes a través del almacenamiento de datos no críticos y reproducibles a niveles de redundancia más bajos que el almacenamiento estándar de Amazon S3. Ambas opciones de almacenamiento de redundancia estándares y reducidas almacenan datos en diferentes funcionalidades y dispositivos, pero con RRS los datos se replican menos veces, de modo que el coste es menor. Se debería esperar la misma latencia y rendimiento mediante el almacenamiento estándar de Amazon S3 o RRS. De forma predeterminada, esta opción no está seleccionada (Amazon S3 utiliza la opción de almacenamiento estándar).

La cuenta de la nube se agrega a la consola.

Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube para el Almacenamiento de blobs de Microsoft Azure

Agregue una cuenta de la nube del Almacenamiento de blobs de Microsoft Azure para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se puede utilizar esta cuenta mientras se crean las tareas Copia de punto de recuperación / Copia de archivo /Archivado de archivos.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.

5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.

6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   Nombre de la cuenta

   Identifica el usuario que solicita acceso a esta ubicación.

   Clave secreta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la clave de acceso no está cifrada.

   Importante: Esta clave secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave secreta en una página Web u otro código de origen accesible públicamente y no la transmita tampoco a través de canales no seguros.

   Configuración proxy

   Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

   Contenedor

   Todos los archivos y las carpetas movidos o copiados al distribuidor de la nube se almacenan y se organizan en los contenedores. Se pueden agrupar y organizar objetos juntos utilizando contenedores. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

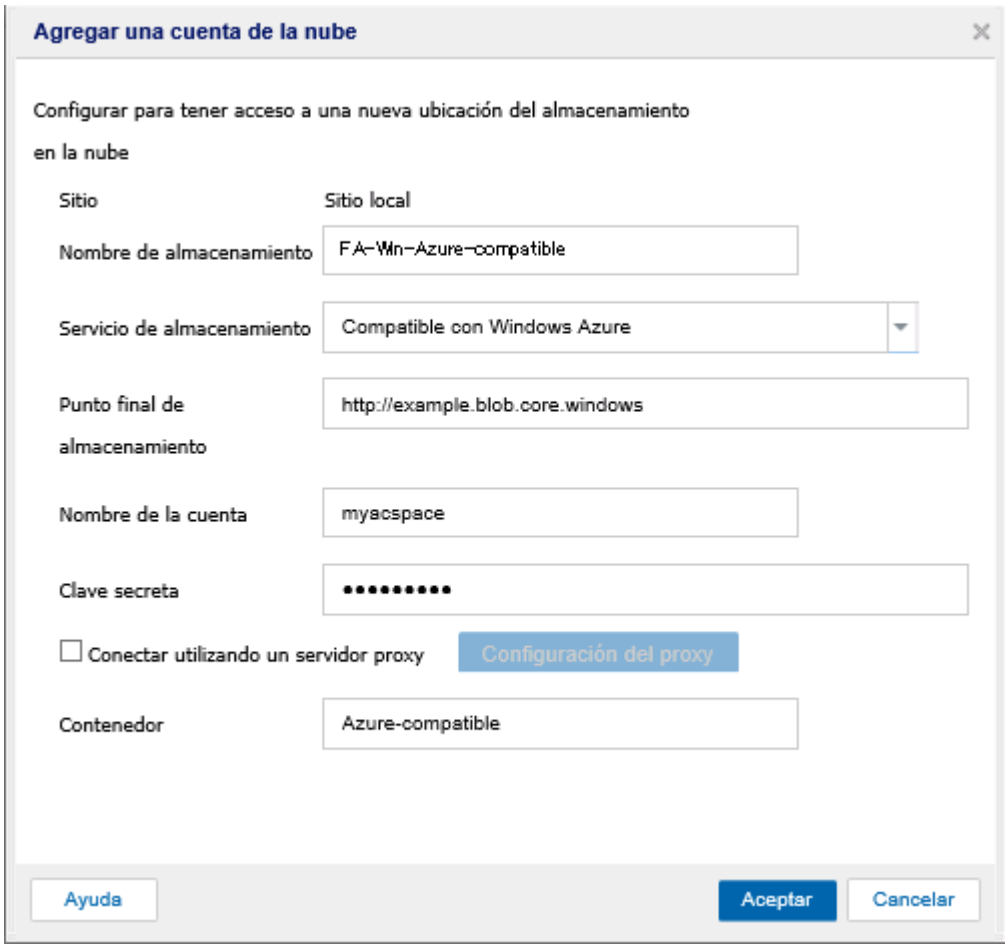
La cuenta de la nube se agrega a la consola.

Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en

la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube compatible con el Almacenamiento de blobs de Microsoft Azure

Agregue una cuenta de la nube compatible con el Almacenamiento de blobs de Microsoft Azure para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se puede utilizar esta cuenta mientras se crean las tareas Copia de punto de recuperación / Copia de archivo /Archivado de archivos.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.

5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.

6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   Punto final del almacenamiento

   Especifica la dirección URL del servicio distribuidor. Por ejemplo, *http:///[nombre servidor]:número puerto*

   Nombre de la cuenta

   Identifica el usuario que solicita acceso a esta ubicación.

   Clave secreta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la clave de acceso no está cifrada.

   Importante: Esta clave secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave secreta en una página Web u otro código de origen accesible públicamente y no la transmita tampoco a través de canales no seguros.

   Configuración proxy

   Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

   Contenedor

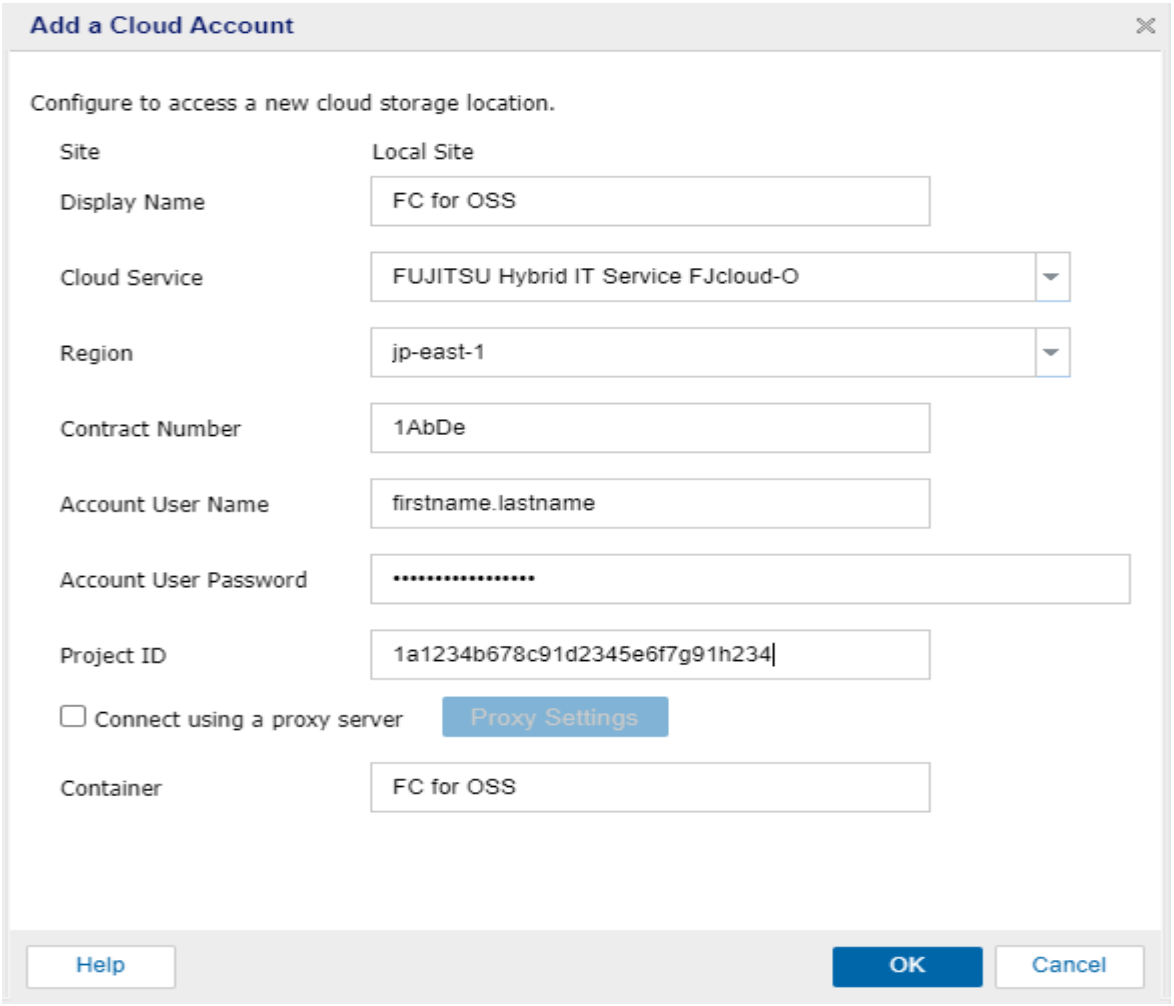
   Todos los archivos y las carpetas movidos o copiados al distribuidor de la nube se almacenan y se organizan en los contenedores. Se pueden agrupar y organizar objetos juntos utilizando contenedores. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

La cuenta de la nube se agrega a la consola.

Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube para FUJITSU Hybrid IT Service FJcloud-O

Agregue una cuenta de la nube de FUJITSU Hybrid IT Service FJcloud-O para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Puede utilizar esta cuenta mientras se crea la tarea de copia de archivo o de archivado de archivos.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.

4. Para el **Nombre para mostrar**, proporcione un nombre único.

   El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.

5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.

6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   Zona de depósito

   Se refiere a la región del depósito en FUJITSU Hybrid IT Service FJcloud-O.

   Nombre de usuario de la cuenta

   Identifica el usuario que solicita acceso a esta ubicación.

   Contraseña de usuario de la cuenta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la contraseña no está cifrada.

   Importante: Esta contraseña es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la contraseña en una página web u otro código de origen accesible públicamente y no la transmita tampoco a través de canales no seguros.

   Configuración proxy

   Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

   Número de contrato

   Hace referencia al número de contrato que proporciona FUJITSU Hybrid IT Service FJcloud-O.

   ID del proyecto

Hace referencia al ID del proyecto que genera FUJITSU Hybrid IT Service FJcloud-O.

Contenedor

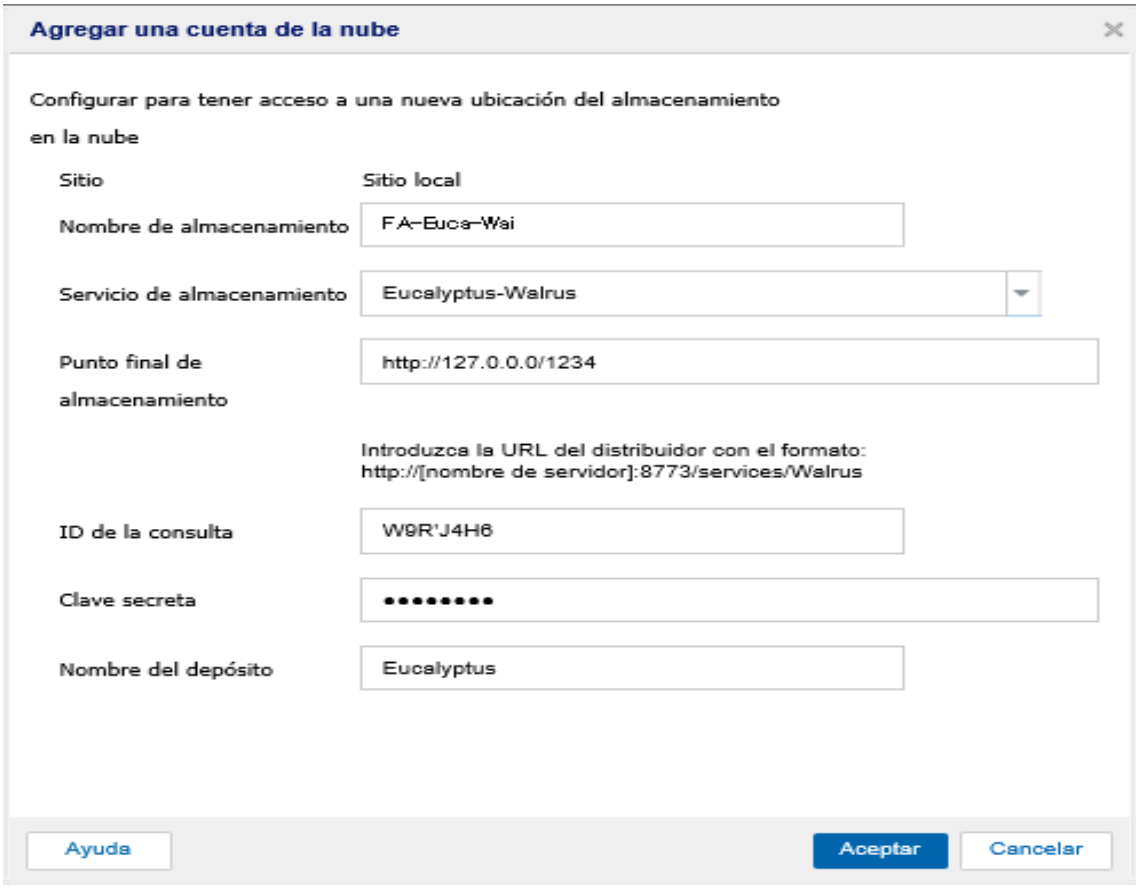
Todos los archivos y las carpetas movidos o copiados al distribuidor de la nube se almacenan y se organizan en los contenedores. Se pueden agrupar y organizar objetos juntos utilizando contenedores. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

La cuenta de la nube se agrega a la consola.

Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube para AppScale Eucalyptus Walrus

Agregue una cuenta de la nube de AppScale Eucalyptus Walrus para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se puede utilizar esta cuenta mientras se crean las tareas Copia de punto de recuperación / Copia de archivo /Archivado de archivos.



Nota: Si utiliza AppScale Eucalyptus Walrus como distribuidor de la nube de copia de archivos, no podrá copiar archivos cuya longitud de la ruta sea mayor de 170 caracteres.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.

5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.

6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   Punto final del almacenamiento

   Especifica la dirección URL del servicio distribuidor. Por ejemplo, *http:///[nombre servidor]:número puerto*

   ID de consulta

   Identifica el usuario que solicita acceso a esta ubicación.

   Clave secreta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la clave de acceso no está cifrada.

   Importante: Esta clave secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave secreta en una página Web u otro código de origen accesible públicamente y no la transmita tampoco a través de canales no seguros.

   Nombre de depósito

   Todos los archivos y las carpetas movidos o copiados al distribuidor de la nube se almacenan y se organizan en los depósitos. Los depósitos son como un contenedor para los archivos y se utilizan para agrupar y organizar objetos conjuntamente. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

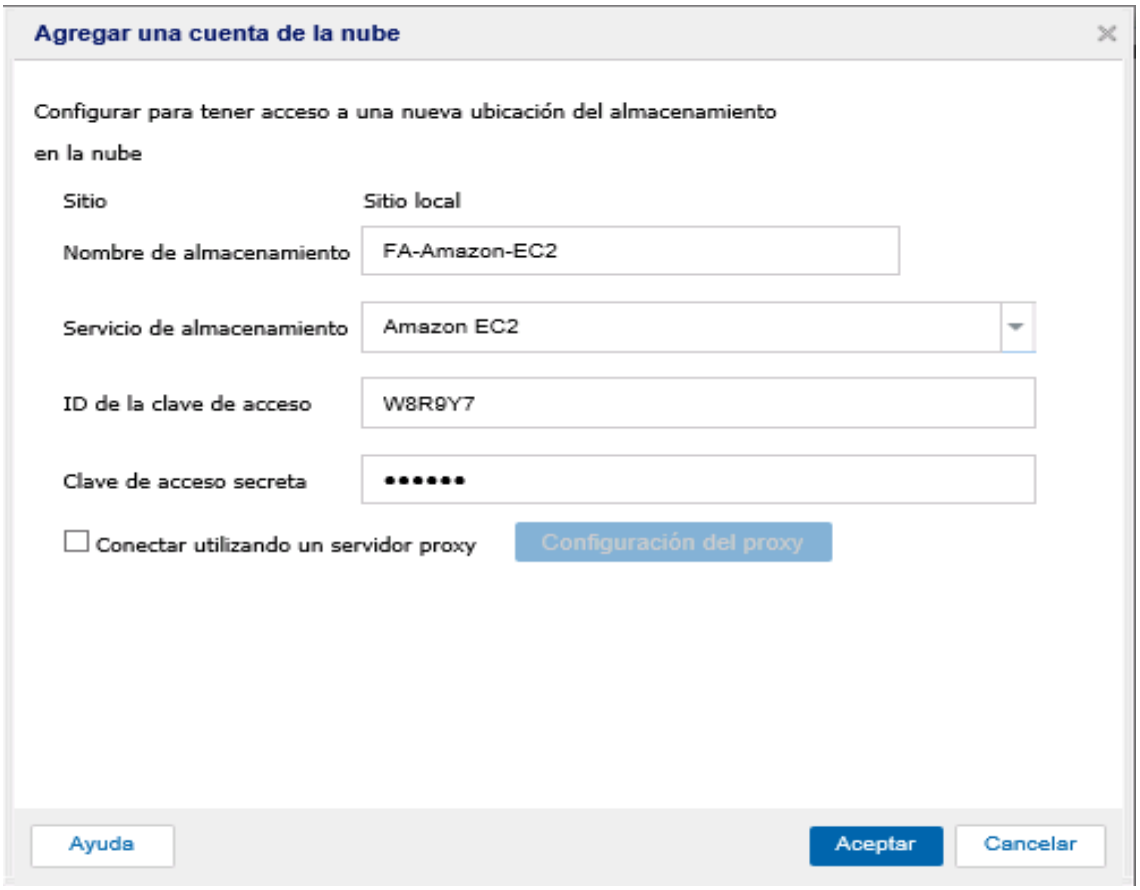
   La cuenta de la nube se agrega a la consola.

   Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube para Amazon EC2

Agregue una cuenta de la nube de Amazon EC2 para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube.

Se puede utilizar esta cuenta mientras se crean tareas para el plan de Virtual Standby a la nube o para el plan de una máquina virtual instantánea en Amazon EC2.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

   El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.

5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.

6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   ID de clave de acceso

   Identifica el usuario que solicita acceso a esta ubicación.

   Clave de acceso secreta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la clave de acceso no está cifrada.

   Importante: Esta clave de acceso secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave de acceso secreta en una página Web ni en otro código de origen accesible públicamente ni la transmita a través de canales no seguros.

   Configuración proxy

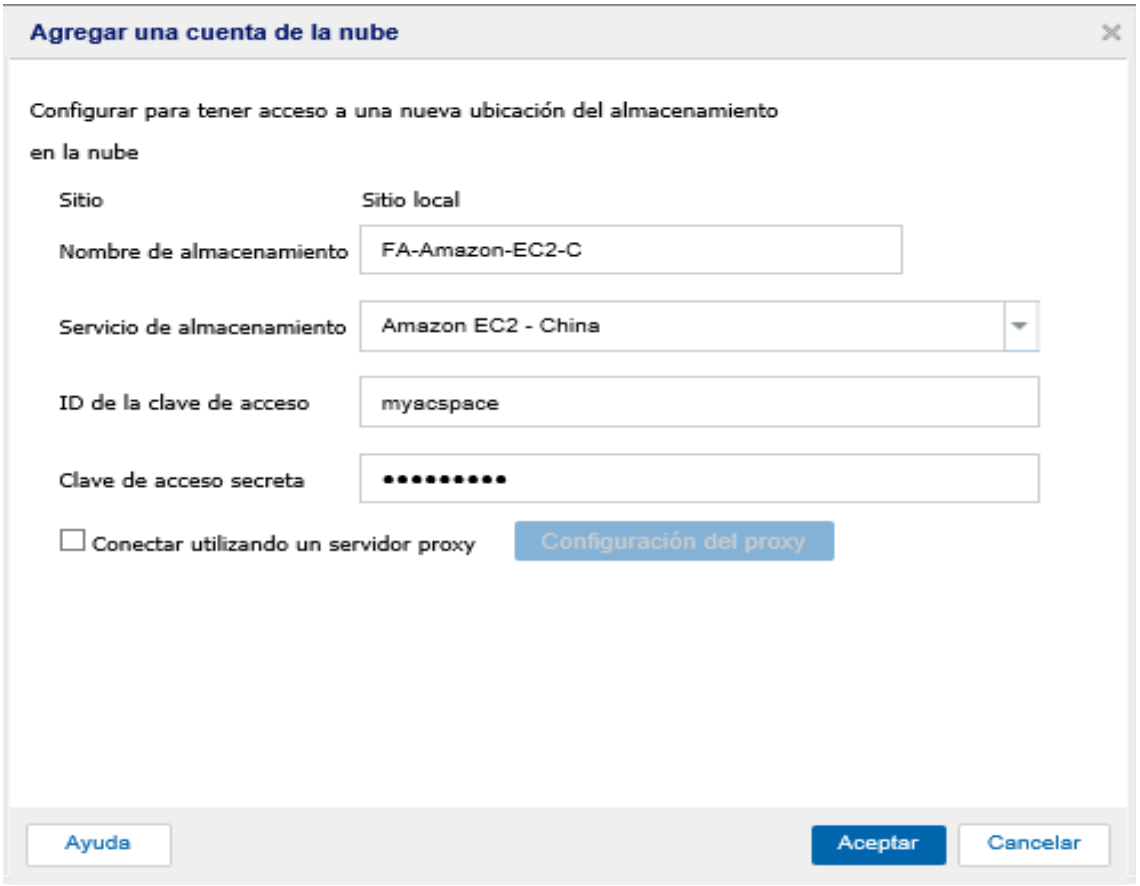
   Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

   La cuenta de la nube se agrega a la consola.

   Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube para Amazon EC2-China

Se debe agregar una cuenta de la nube de Amazon EC2-China para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se puede utilizar esta cuenta mientras se crean tareas para el plan de Virtual Standby a la nube o para el plan de una máquina virtual instantánea en Amazon EC2.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.

5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.

6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   ID de clave de acceso

   Identifica el usuario que solicita acceso a esta ubicación.

   Clave de acceso secreta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la clave de acceso no está cifrada.

   Importante: Esta clave de acceso secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave de acceso secreta en una página Web ni en otro código de origen accesible públicamente ni la transmita a través de canales no seguros.

   Configuración proxy

   Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

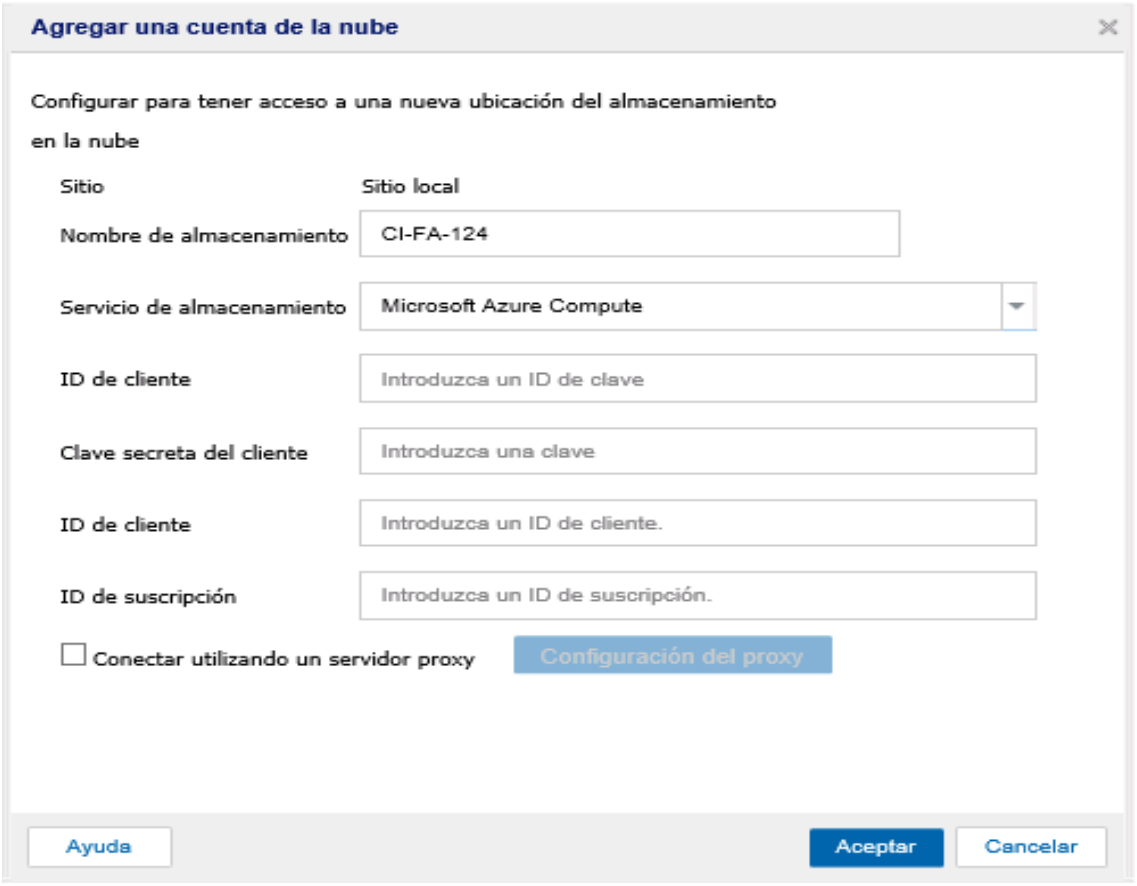
   La cuenta de la nube se agrega a la consola.

   Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube para Microsoft Azure Compute

Agregue una cuenta de la nube de Microsoft Azure Compute para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se puede utilizar esta cuenta mientras se crean tareas para el plan de Virtual Standby a la nube o para el plan de una máquina virtual instantánea en Microsoft Azure.

Nota: Para agregar una cuenta de la nube para Microsoft Azure, se deben cumplir los requisitos previos. Para obtener más información, consulte Requisitos previos.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre de la cuenta**, proporcione un nombre único.

El Nombre de la cuenta especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre de almacenamiento único.

5. Seleccione la opción de la lista desplegable **Servicio de la cuenta**.

   Aparecen varios campos para la configuración.

6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   ID de cliente

   Hace referencia al ID de aplicación de la aplicación de Azure Active Directory. Copie el ID de cliente preparado en el editor de texto.

   Clave secreta del cliente

   Hace referencia a la clave de autenticación generada para la aplicación de Azure Active Directory que se especifica como ID de cliente. Copie la clave secreta del cliente preparada en el editor de texto.

   Importante: Esta clave secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave secreta en una página Web u otro código de origen accesible públicamente y no la transmita tampoco a través de canales no seguros.

   ID de inquilino

   Hace referencia al ID de Azure Active Directory donde se ha creado la aplicación de Azure Active Directory. Copie el ID de inquilino preparado en el editor de texto.

   ID de suscripción

   Hace referencia a un identificador único global (GUID) que identifica de forma exclusiva la suscripción para utilizar los servicios de Azure. Copie el ID de suscripción preparado en el editor de texto.

   Configuración proxy

   Especifica la configuración del servidor proxy. Seleccione **Conectar utilizando un servidor proxy**para activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. Se debe proporcionar la información de autenticación correspondiente necesaria para utilizar el servidor proxy.

La cuenta de la nube se agrega a la consola.

Requisitos previos para agregar una cuenta de la nube para Microsoft Azure

Antes de poder crear una cuenta de la nube para Microsoft Azure, se deben completar las siguientes tareas de requisitos previos obligatorias en el orden especificado:

1. Prepare los servidores para implementar como Consola de Arcserve UDP y servidor de puntos de recuperación. Dichos servidores deben cumplir los requisitos del sistema para cada componente.
2. Asegúrese de que tiene los permisos necesarios para crear una aplicación en Azure Active Directory.

   Para obtener instrucciones, consulte la sección sobre la comprobación de permisos de Azure Active Directory en la documentación de Microsoft.
3. Cree una aplicación de Azure de Active Directory. En un editor de texto (como Bloc de notas), copie el ID de la aplicación y etiquételo como ID de cliente.

   Para obtener instrucciones, consulte la sección sobre la comprobación de permisos de Azure Active Directory en la documentación de Microsoft.
4. Obtenga el ID de la aplicación y genere una clave de autenticación para esta aplicación. Copie la cadena de la clave de autenticación en el editor de texto (como Bloc de notas) y etiquete la cadena como Clave secreta del cliente.

   Para obtener instrucciones, consulte la sección sobre cómo obtener el ID de la aplicación y la clave de autenticación en la documentación de Microsoft.
5. Obtenga el ID de inquilino, que es el ID de Azure Active Directory en el que se ha creado la aplicación. En un editor de texto (como Bloc de notas), copie el ID y etiquételo ID de inquilino.

   Para obtener instrucciones, consulte la sección sobre cómo obtener el ID de inquilino en la documentación de Microsoft.
6. Realice los pasos siguientes para asignar el rol de colaborador a la aplicación.
   a. En el panel izquierdo del menú del portal de Microsoft Azure, seleccione **Suscripciones**.
   b. Seleccione su suscripción.
   c. Seleccione la ficha Control de acceso (IAM).

d. Agregue la aplicación.

e. Asigne el rol de colaborador a la aplicación.

Para obtener más información, consulte la sección sobre cómo asignar aplicaciones a un rol en la documentación de Microsoft.

7. Obtenga su ID de suscripción de Azure.

Nota: El ID de suscripción es un GUID que identifica de forma exclusiva su suscripción para utilizar los servicios de Azure.

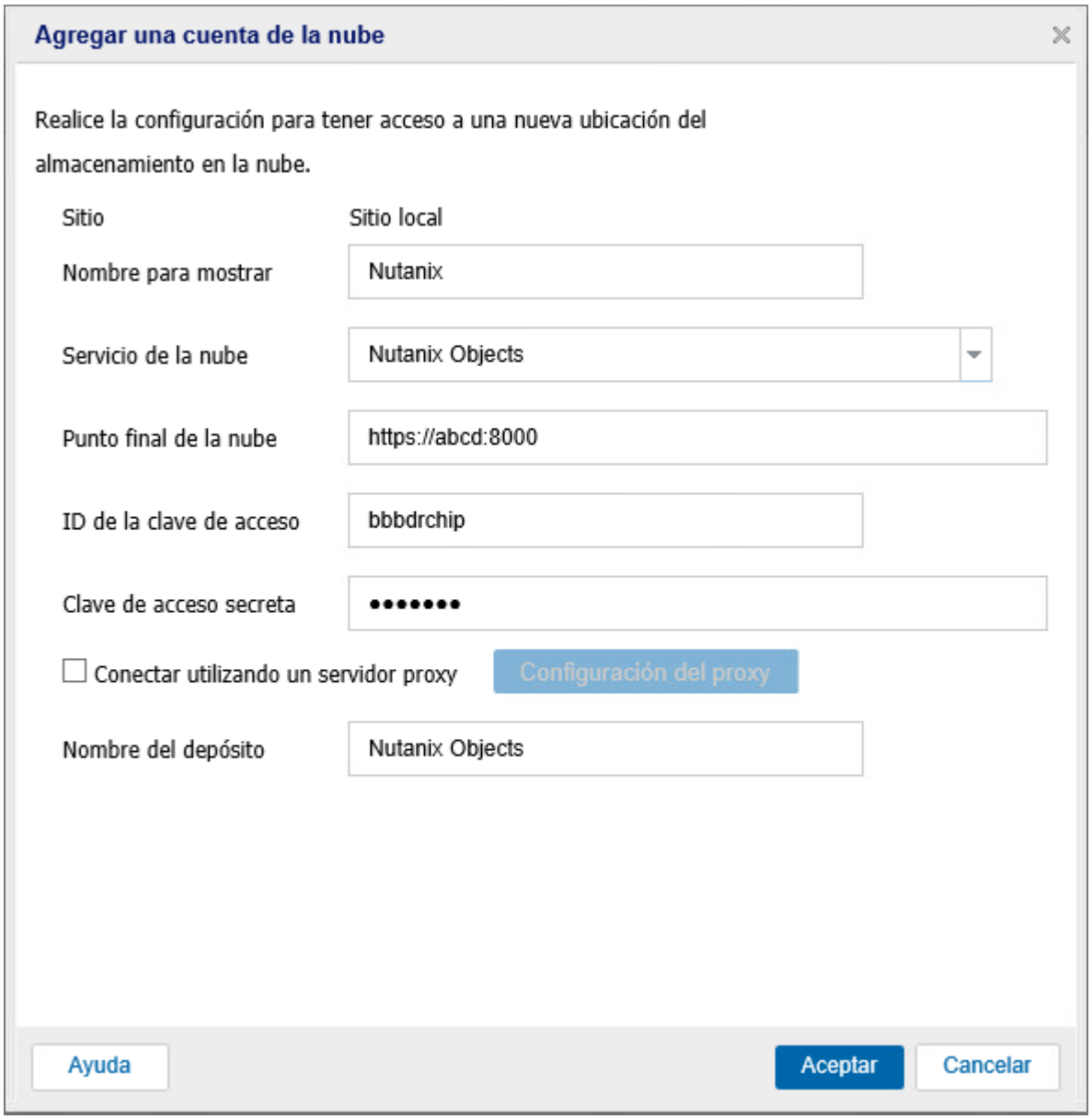
a. Inicie sesión en el portal de Microsoft Azure.

b. En el panel de navegación de la izquierda, haga clic en Suscripciones.

La lista de sus suscripciones se muestra junto con el ID de suscripción.

Adición de una cuenta de la nube para Nutanix Objects

Se debe agregar una cuenta de la nube de Nutanix Objects para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se puede utilizar esta cuenta mientras se crean las tareas Copia de punto de recuperación / Copia de archivo /Archivado de archivos.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

   El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.

5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.

6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   Punto final del almacenamiento

   Especifica la dirección URL del servicio distribuidor. Por ejemplo, *http:///[nombre servidor]:número puerto*

   ID de clave de acceso

   Identifica el usuario que solicita acceso a esta ubicación.

   Clave de acceso secreta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la clave de acceso no está cifrada.

   Importante: Esta clave de acceso secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave de acceso secreta en una página Web ni en otro código de origen accesible públicamente ni la transmita a través de canales no seguros.

   Configuración proxy

   Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

   Nombre de depósito

   Todos los archivos y las carpetas movidos o copiados al distribuidor de la nube se almacenan y se organizan en los depósitos. Los depósitos son como un contenedor para los archivos y se utilizan para agrupar y organizar objetos conjuntamente. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

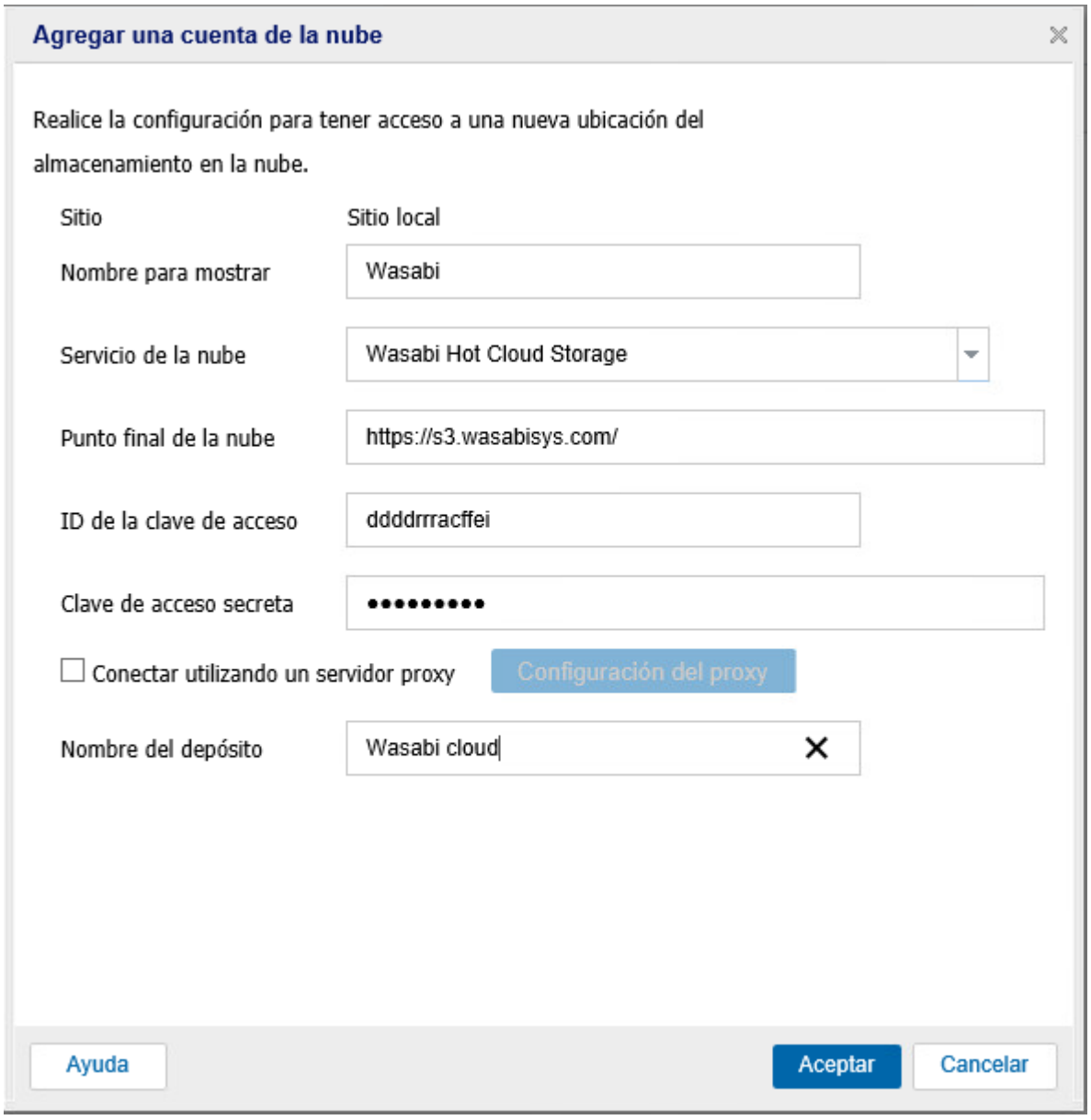
   La cuenta de la nube se agrega a la consola.

   Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de

Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube para Wasabi Hot Cloud Storage

Agregue una cuenta de la nube de Wasabi Hot Cloud Storage para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se puede utilizar esta cuenta mientras se crean las tareas Copia de punto de recuperación / Copia de archivo /Archivado de archivos.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

   El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.
5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.
6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   Punto final del almacenamiento

   Las tres regiones siguientes son compatibles con Wasabi Hot Cloud Storage:

   - Para la región us-east: el punto final es s3.wasabisys.com.
   - Para la región us-west: el punto final es s3.us-west-1.wasabisys.com
   - Para la región eu-central: el punto final es s3.eu-central-1.wasabisys.com

   ID de clave de acceso

   Identifica el usuario que solicita acceso a esta ubicación.

   Clave de acceso secreta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la clave de acceso no está cifrada.

   Importante: Esta clave de acceso secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave de acceso secreta en una página Web ni en otro código de origen accesible públicamente ni la transmita a través de canales no seguros.

   Configuración proxy

   Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor

proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

Nombre de depósito

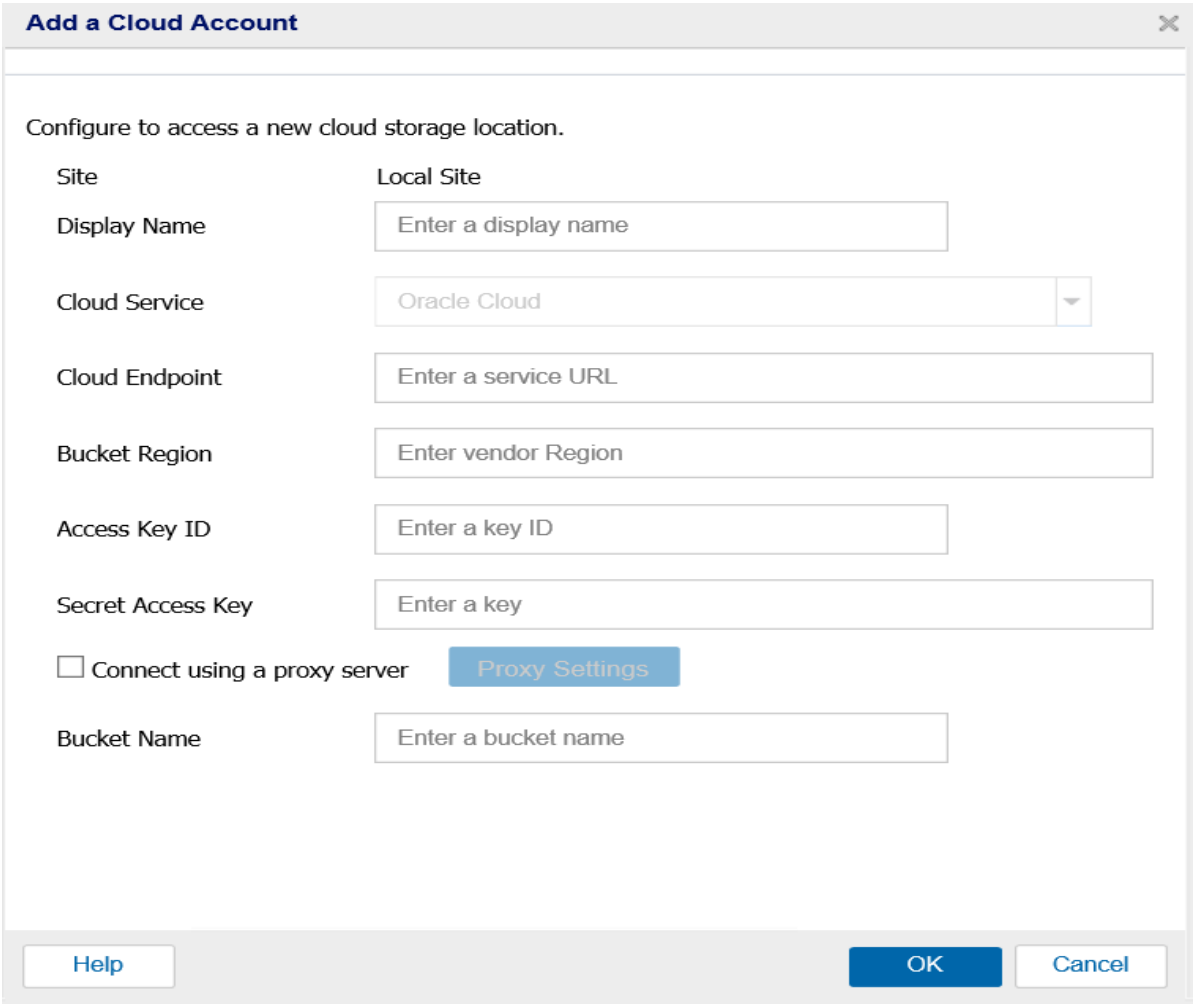
Todos los archivos y las carpetas movidos o copiados al distribuidor de la nube se almacenan y se organizan en los depósitos. Los depósitos son como un contenedor para los archivos y se utilizan para agrupar y organizar objetos conjuntamente. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

La cuenta de la nube se agrega a la consola.

Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube para Oracle Cloud

Se debe agregar una cuenta de la nube de Oracle para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se puede utilizar esta cuenta mientras se crean las tareas Copia de punto de recuperación / Copia de archivo /Archivado de archivos.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre para mostrar**, proporcione un nombre único.

El campo Nombre para mostrar especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre para mostrar único.

5. Seleccione la opción de la lista desplegable **Servicio de la nube**.

   Aparecen varios campos para la configuración.

6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   Punto final de la nube

   Especifica la dirección URL del servicio distribuidor. Por ejemplo, *http-s://namespace.compat.objectstorage.region.oraclecloud.com*

   Zona de depósito

   Se refiere a la región del depósito del distribuidor.

   ID de clave de acceso

   Identifica el usuario que solicita acceso a esta ubicación.

   Clave de acceso secreta

   Hace referencia a una contraseña que se utiliza para comprobar la autenticidad de la solicitud para obtener acceso a esta ubicación porque la clave de acceso no está cifrada.

   Importante: Esta clave de acceso secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave de acceso secreta en una página Web ni en otro código de origen accesible públicamente ni la transmita a través de canales no seguros.

   Configuración proxy

   Especifica la configuración del servidor proxy. Seleccione la casilla de verificación de **Conectar utilizando un servidor proxy** si se desea activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. A continuación, se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

   Nombre de depósito

   Todos los archivos y las carpetas movidos o copiados al distribuidor de la nube se almacenan y se organizan en los depósitos. Los depósitos son como un

contenedor para los archivos y se utilizan para agrupar y organizar objetos conjuntamente. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

La cuenta de la nube se agrega a la consola.

Nota: Si se ha configurado Copia de archivo y Archivado de archivos en Arcserve UDP v6.0 o en versiones anteriores y ahora se actualiza a la versión más reciente de Arcserve UDP, para Archivado de archivos Arcserve UDP crea un nuevo depósito en la nube con el sufijo **-fa**. Copia de archivo utiliza el mismo depósito que se ha utilizado en la versión anterior.

Adición de una cuenta de la nube de Arcserve

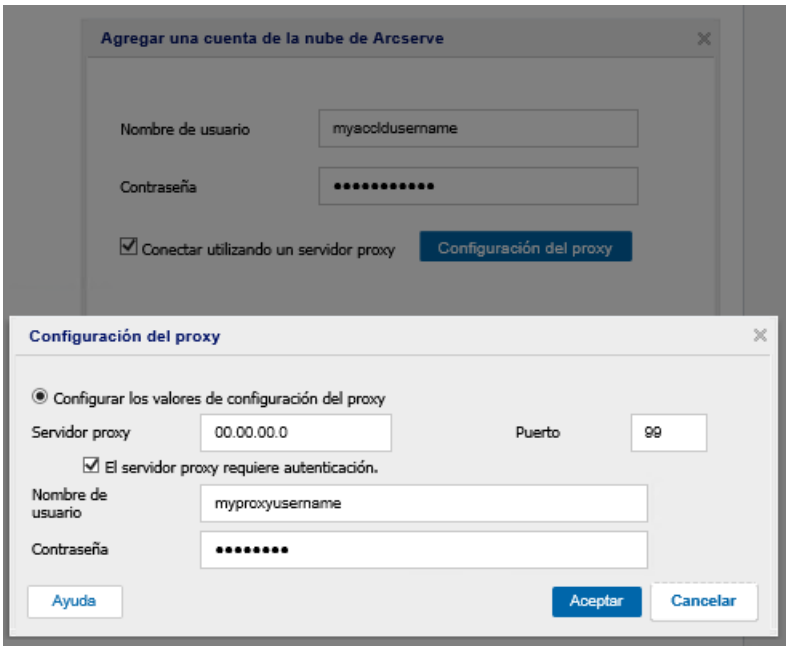
Agregue una cuenta de la nube de Arcserve para copiar archivos o puntos de recuperación a un almacenamiento de la nube.

Siga estos pasos:

1. Inicie sesión en Arcserve UDP y haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Nube de Arcserve**.

   Aparecerá la página Destinos: Nube de Arcserve.
3. Haga clic en **Agregar una cuenta de la nube de Arcserve**.

   Aparecerá la pantalla Adición de una cuenta de la nube de Arcserve.



4. Introduzca los siguientes detalles:

   Nombre de usuario

Especifica el nombre de usuario de la cuenta de la nube de Arcserve que se ha registrado con Arcserve.

Contraseña

Especifica la contraseña de la cuenta de la nube de Arcserve del usuario correspondiente que se ha registrado con Arcserve.

Conectar utilizando un servidor proxy

Seleccione esta opción para conectarse a la nube de Arcserve utilizando un servidor proxy que tiene conexión a Internet.

Configuración proxy

Si se selecciona la opción Conectar utilizando un servidor proxy, haga clic en Configuración proxy.

Aparecerá la ventana Configuración proxy. Introduzca los siguientes detalles y haga clic en **Aceptar**.

Servidor proxy

Especifica la dirección IP del servidor proxy.

Puerto

Especifica el número de puerto que está abierto en el servidor proxy.

El servidor proxy requiere autenticación

Seleccione esta opción si desea que el acceso al servidor proxy requiera autenticación.

Nombre de usuario

Especifica el nombre de usuario que tiene acceso al servidor proxy.

Contraseña

Especifica la contraseña de la cuenta del usuario correspondiente que tiene acceso al servidor proxy.

5. Haga clic en **Aceptar**.

   Se ha agregado correctamente la cuenta de la nube de Arcserve.

Cómo gestionar un almacén de datos

Después de crear un almacén de datos, es posible que sea necesario realizar diversas operaciones como modificar, suprimir, detener e iniciar un almacén de datos.

También se pueden ejecutar tareas de combinación a petición para varios nodos con el objetivo de crear más espacio disponible en un almacén de datos.

¿Qué hacer a continuación?

- Revisión de los requisitos previos
- Modificación de un almacén de datos
- Supresión de un almacén de datos de la consola
- Detención de un almacén de datos
- Inicio de un almacén de datos
- Control de la capacidad de espacio del almacén de datos
- Examen de puntos de recuperación en un almacén de datos
- Supresión de los datos del nodo de un almacén de datos
- Modificación del límite de nodos activos simultáneos para la copia de seguridad manual
- Ejecutar una tarea de combinación manual o a petición
- Solución de problemas: Cómo utilizar un almacén de datos cuando la carpeta de destino de la copia de seguridad está completa

Revisión de los requisitos previos

Para gestionar un almacén de datos, complete los requisitos previos siguientes:

- Se ha agregado ya un almacén de datos.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Modificación de un almacén de datos

Se puede modificar un almacén de datos ya existente, pero hay algunas restricciones y no se pueden modificar los detalles siguientes de un almacén de datos:

- Detalles de compresión
- Almacén de datos de no deduplicación a un almacén de datos de deduplicación o almacén de datos de deduplicación a un almacén de datos de no deduplicación.
- Opciones de deduplicación: Deduplicar datos y Tamaño de bloque de la deduplicación.

Consideraciones antes de modificar un almacén de datos:

- Si se cambia la ruta del almacén de datos o la contraseña de cifrado, se cancelarán todas las tareas que ejecutan en ese almacén de datos, incluyendo las tareas que esperan en cola. Cualquier cambio en el nombre del almacén de datos, el tamaño de la memoria hash o el número de nodos activos simultáneos no afecta a las tareas en ejecución.
- Para un almacén de datos de no deduplicación: para cambiar la ruta del almacén de datos, mantenga vacía la carpeta de destino de la copia de seguridad.
- Para un almacén de datos de deduplicación: para cambiar la ruta del almacén de datos, mantenga vacías las carpetas siguientes:
  - Carpeta de destino de la copia de seguridad
  - Destino de los datos
  - Destino del índice
  - Destino de hash
- Las opciones de **Contraseña de cifrado** solo se pueden editar si se selecciona la opción **Cifrar datos** mientras se crea el almacén de datos.

Siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destinos: servidores de punto de recuperación**, en la que aparecerá la lista de servidores de punto de recuperación disponibles.
3. Expanda un servidor de punto de recuperación.

Se puede ver la lista de almacenes de datos asociada con el servidor de punto de recuperación.

4. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en el nombre del almacén de datos.
   - Seleccione el almacén de datos y en el panel central haga clic en el menú desplegable **Acciones**.

   Aparecerá una lista de opciones.
5. Haga clic en **Modificar**.

   La página **Modificar un almacén de datos** se muestra.
6. Rellene los campos obligatorios y, a continuación, haga clic en **Guardar**:

   Servidor de puntos de recuperación

   Define el servidor de puntos de recuperación en el que se crea el almacén de datos. El servidor de puntos de recuperación ya está agregado de forma predeterminada.

   Nombre del almacén de datos

   Define el nombre del almacén de datos.

   Carpeta del almacén de datos

   Define la ubicación de la ruta para la carpeta donde se crea el almacén de datos. Haga clic en Examinar para seleccionar carpeta de destino.

   Notas:

   - Ahora se puede activar y ver los volúmenes ocultos. Para obtener más información, consulte Cómo activar y ver volúmenes ocultos al crear un almacén de datos.
   - Para el almacén de datos de deduplicación y de no deduplicación, la ruta de destino debe ser una carpeta vacía.

   Límite de nodos activos simultáneos

   Especifica el número máximo de tareas simultáneas en el almacén de datos.

   Valor predeterminado: 4

   hace referencia a un valor del 1 al 9999. El valor indica el número de tareas que se pueden ejecutar simultáneamente. Si las tareas en ejecución cumplen el número, otra tarea se coloca en la cola y la tarea solo puede iniciarse cuando una de las tarea en ejecución se completa. La tarea completada puede significar una tarea finalizada, cancelada o errónea.

El número se aplica a los Tipos de trabajo pero no a los nodos del servidor. Por ejemplo, el número 5 indica que se están ejecutando cinco tareas de copia de seguridad. Cualquier tarea programada para después de estas cinco tareas de copia de seguridad espera en la cola, pero se puede enviar otra tarea, como Catálogo del sistema de archivos.

Si el valor es más de 16 o 32, se muestran mensajes para advertir sobre el aumento de la demanda en el hardware.

Nota: El limitar el número solamente tiene un efecto en la tarea de salida de la replicación, no en la tarea de entrada de la replicación. El límite para contar no impacta en las tareas de restauración o de reconstrucción completa. Estas tareas no se colocan en una cola.

Activación de la deduplicación

Especifica que la deduplicación se activa para este almacén de datos. Arcserve UDP es compatible con los dos tipos de deduplicación: Deduplicación de origen y Deduplicación global. La deduplicación de origen impide que los bloques de datos duplicados se muevan a través de la red desde un agente concreto. La deduplicación global elimina los datos duplicados a través de todos los equipos cliente basándose en el nivel del clúster de volumen.

Tamaño de bloque de la deduplicación

Define el tamaño de bloque de la deduplicación. Las opciones son 4 kB, 8 kB, 16 kB, 32 kB y 64 kB. El tamaño de bloque de la deduplicación también tiene un impacto en la estimación de la capacidad de la deduplicación. Por ejemplo, si se cambia el valor predeterminado de 16 kB a 32 kB, las estimaciones de la capacidad de la deduplicación se doblan. Al aumentar el tamaño de bloque de la deduplicación se puede reducir el porcentaje de deduplicación.

Adjudicación de memoria hash

Especifica la cantidad de memoria física que se adjudica para mantener los hash. Este campo se rellena previamente con un valor predeterminado. El valor predeterminado se basa en el siguiente cálculo:

Si la memoria física del punto de recuperación es inferior a 4 GB (o es idéntica a 4 GB), el valor predeterminado de **Adjudicación de memoria hash** es idéntico al de la memoria física del servidor de puntos de recuperación.

Si la memoria física del servidor de puntos de recuperación es mayor de 4 GB, Arcserve UDP calcula la memoria libre disponible en ese momento. Suponga que la memoria libre disponible asciende a X GB en ese momento. Arcserve UDP también comprueba las siguientes condiciones:

- Si (X * 80 %) > 4 GB, el valor predeterminado de **Adjudicación de memoria hash** es (X * 80 %).
- Si (X * 80 %) ≤ 4 GB, el valor predeterminado de **Adjudicación de memoria hash** es 4 GB.

  Ejemplo: Imagine que el servidor de puntos de recuperación cuenta con 32 GB de memoria física. Asuma que el sistema operativo y otras aplicaciones utilizan 4 GB de memoria a la hora de crear el almacén de datos. Por lo tanto, la memoria libre disponible en este momento es de 28 GB. El valor predeterminado de **Adjudicación de memoria hash** es 22,4 GB (22,4 GB = 28 GB * 80 %).

El destino de hash está en una unidad de estado sólido (SSD)

Especifica si la carpeta de hash está en una unidad de estado sólido.

Nota: Se debe configurar el destino de hash en la unidad de estado sólido (SSD) local si la opción El destino de hash está en una unidad de estado sólido (SSD) está activada.

Destino de los datos

Define la carpeta de destino de los datos para guardar los bloques de datos únicos reales. Use el disco más grande para almacenar datos ya que contiene los bloques de datos originales del origen.

Nota: La ruta de **Destino de los datos** debe ser una carpeta en blanco.

Destino del índice

Define la carpeta de destino del índice para almacenar los archivos de índice. Elija un disco diferente para mejorar el procesamiento de la deduplicación.

Nota: La ruta de **Destino del índice** debe ser una carpeta en blanco.

Destino de hash

Define la ruta para almacenar la base de datos de hash. Arcserve UDP emplea el algoritmo SHA1 para generar el hash de los datos de origen. Los valores de hash se gestionan mediante la base de datos de hash. Si se selecciona una unidad de estado sólido (SSD), se aumentará la capacidad de deduplicación y se reducirá la adjudicación de memoria necesaria. Para mejorar el rendimiento de hash, se recomienda formatear el volumen de SSD como sistema de archivos NTFS con el tamaño del clúster de volúmenes de 4 kB.

Nota: La ruta de **Destino de hash** debe ser una carpeta vacía.

Nota: No se puede especificar la misma ruta para las cuatro carpetas siguientes: **Almacén de datos, Destino de los datos, Destino del índice** y **Destino de hash**.

Activación de la compresión

Especifica que se ha activado la configuración de compresión de datos.

Tipo de compresión

Especifica si se debe utilizar el tipo de compresión estándar o máxima.

La compresión se realiza muchas veces para reducir el uso del espacio en disco, pero también tiene un efecto contrario en la velocidad de la copia de seguridad dado el incremento del uso de la CPU. Basándose en los requisitos, se puede seleccionar una de las tres opciones disponibles.

Nota: Para obtener más información, consulte Tipo de compresión.

Activación del cifrado

Especifica que se han activado los valores de configuración de cifrado. Cuando se selecciona esta opción, se debe especificar y confirmar la contraseña de cifrado.

El cifrado de datos es la traducción de los datos a una forma que resulte ininteligible sin un mecanismo de descifrado. La solución Arcserve Unified Data Protection utiliza algoritmos de cifrado seguros AES (Estándar de cifrado avanzado) para lograr la máxima seguridad y privacidad de los datos. Para los almacenes de datos, se es compatible tanto con el Cifrado como con Sin cifrado. Para Cifrado, solamente AES-256 está disponible.

No será necesaria ninguna contraseña si la restauración se realiza en el equipo desde donde se ha realizado la copia de seguridad. Sin embargo, sí será necesaria una contraseña si se intenta realizar la restauración en otro equipo. De forma predeterminada, solo se necesita una contraseña para el primer inicio de sesión. Para introducir la contraseña incluso después del primer inicio de sesión, el administrador debe detener manualmente el servicio de extensión del explorador del Agente de Arcserve UDP.

Enviar una alerta de correo electrónico cuando un destino se está acercando a su plena capacidad

Al seleccionar esta opción, se configurará el almacén de datos para que envíe alertas de correo electrónico. El servidor de puntos de recuperación envía alertas de correo electrónico a los destinatarios cuando la carpeta de destino del almacén de datos se está acercando a su plena capacidad.

Configurar correo electrónico

Este botón solo aparece cuando se activa la opción *Enviar una alerta de correo electrónico cuando un destino se está acercando a su plena capacidad*. El botón le ayuda a proporcionar un ID de correo electrónico para recibir alertas. Haga clic en el botón **Configurar correo electrónico** para cargar la configuración global de alertas de correo electrónico en Consola > Configuración

> Configuración del correo electrónico y de alertas. Si la configuración global del correo electrónico no está disponible, al hacer clic en el botón **Configurar correo electrónico** se abre el cuadro de diálogo **Configuración del correo electrónico** para establecer los detalles del correo electrónico.

El almacén de datos se actualiza.

Modificación del umbral del almacén de datos

Este tema proporciona información sobre las ubicaciones del registro del umbral, sobre el nombre de clave del umbral y sobre los valores predeterminados, así como también proporciona información sobre cuándo aparece un mensaje de advertencia o error del umbral y sobre cómo modificar el umbral del almacén de datos.

Un almacén de datos tiene la configuración del umbral de capacidad de espacio que ayuda a controlar la información de uso del espacio libre del destino del almacén de datos. En un almacén de datos de deduplicación, el umbral controla la memoria adjudicada al destino del hash y el espacio en disco adjudicado para la carpeta de destino de la copia de seguridad, de destino del índice y de destino de datos. Para un almacén de datos de no deduplicación, el umbral solo controla el espacio de almacenamiento de la carpeta de destino de la copia de seguridad. Los cinco artículos que los umbrales controlan tienen dos tipos de valores:

- Umbral de error
- Umbral de advertencia

El valor del umbral se guarda en el registro del sistema. El valor predeterminado se puede modificar manualmente.

Ubicaciones del registro de los umbrales

1. Carpeta del almacén de datos: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\CommStore]
2. Destino de los datos de la deduplicación:[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\DataRole]
3. Destino de hash de deduplicación y memoria: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\HashRole]

   Nota: El rol del hash controla tanto la memoria como el uso del disco. La ruta representa el uso de disco y Mem representa la memoria.
4. Destino del índice de deduplicación: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\IndexRole]

Nombres de clave del umbral y valores predeterminados

Tipo de ruta	Tipo de umbral	Nombre de la clave de registro	Valor predeterminado	Valor predeterminado (Antes de v6.5 Actualización 1)

Carpeta del almacén de datos	Advertencia	WarnPathThreshold	0,05	0,03
	Error	ErrorPathThreshold	2048	100
Ruta del índice de deduplicación	Advertencia	WarnPathThreshold	0,05	0,03
	Error	ErrorPathThreshold	2048	100
Ruta de hash de deduplicación	Advertencia	WarnPathThreshold	0,05	0,03
	Error	ErrorPathThreshold	2048	100
Ruta del rol de datos de deduplicación	Advertencia	WarnPathThreshold	0,05	0,03
	Error	ErrorPathThreshold	2048	100
Memoria	Advertencia	WarnMemThreshold	0,05	0,03
	Error	ErrorMemThreshold	30	10

- Los valores inferiores a 1 indican el porcentaje de espacio libre. Por ejemplo, 0,05 significa 5 %. Si el espacio libre es inferior al 5 % del tamaño total del espacio, se alcanza el umbral de advertencia.
- Un valor mayor o igual a 1 indica el tamaño real de espacio libre y la unidad es MB. Por ejemplo, el valor predeterminado 2048 significa 2048 MB. Si el espacio libre es inferior a 2048 MB, se alcanza el umbral de error.

El valor del umbral predeterminado está diseñado para mejorar el rendimiento del almacén de datos. Se pueden cambiar los valores del umbral. No se recomienda cambiar estos valores, a menos que se necesite espacio adicional.

Siga estos pasos para modificar el umbral:

1. Vaya a la respectiva ubicación del registro.
2. Modifique manualmente el valor predeterminado del umbral.

Cómo modificar únicamente el destino de hash

Cuando se cambia un almacén de datos de deduplicación, solo el destino de la ruta de hash puede cambiarse a una carpeta vacía. Arcserve UDP vuelve a generar la ruta de hash para el nuevo almacén de datos. Este proceso es útil cuando la carpeta de hash se queda sin espacio y se cancelan todas las tareas. Se puede modificar el almacén de datos y proporcionar una nueva carpeta de destino de hash.

Cómo cambiar los modos de destino de hash

Cuando se crea un almacén de datos de deduplicación, se especifica si el destino de hash está en una unidad de estado sólido (modo SSD) o en una unidad de disco duro (modo RAM). Si se ha configurado el disco duro como el destino de hash, se necesitará más memoria para procesar las claves de hash. Como resultado, cuando el tamaño de la copia de seguridad aumenta, es posible que se agote toda la memoria. En este caso, se puede agregar un SSD para realizar una copia de seguridad de más datos. Del mismo modo, si se ha configurado un SSD como destino de hash, será necesaria menos memoria para procesar las claves de hash. Sin embargo, si se cambia a un equipo con más memoria, será posible cambiar al modo RAM para obtener un procesamiento de hash más rápido.

Para cambiar el destino de hash de RAM a SSD o de SSD a RAM, Arcserve UDP permite modificar un almacén de datos existente y cambiar el modo como sea necesario.

Se puede modificar un almacén de datos existente incluso cuando se encuentra en ejecución, pero el almacén de datos se reinicia después de guardar el cambio.

Cambio del modo RAM al modo SSD

Cuando se cambia del modo RAM al modo SSD, el equipo necesitaría menos memoria. De este modo, Arcserve UDP reduce automáticamente el valor mínimo de adjudicación de memoria hash. Sin embargo, se puede cambiar manualmente la adjudicación de memoria hash. Para este caso, se deben cambiar las carpetas de destino de hash a SSD. Al cambiar el destino de hash, Arcserve UDP copia automáticamente los archivos de hash en la ubicación nueva de SSD.

Cambio del modo SSD al modo RAM

Cuando se cambia del modo SSD al modo RAM, la RAM debería ser suficientemente grande para alojar la base de datos de hash actual. Por ejemplo, antes del cambio, el almacén de datos creó 30 GB de archivos de hash en SSD. Ahora, después del cambio, debería adjudicar como mínimo 30 GB memoria para los archivos de hash. Si la RAM no es suficiente, se producirá un error en el conmutador. En este caso, Arcserve UDP aumenta automáticamente los dos parámetros siguientes:

- Valor mínimo de adjudicación de memoria hash
- Adjudicación de memoria hash

Esto garantiza que el almacén de datos se inicia después de la modificación.

Para este caso, se deben cambiar las carpetas de destino de hash a la unidad de disco duro. Al cambiar el destino de hash, Arcserve UDP copia automáticamente los archivos de hash en la ubicación nueva de la unidad de disco duro.

Inicio de un almacén de datos

Si se ha detenido un almacén de datos en ejecución para cualquier comprobación de mantenimiento rutinaria, se puede iniciar el almacén de datos otra vez después de que la comprobación de mantenimiento se haya acabado. Cuando se inicia el almacén de datos, las tareas pendientes se iniciarán en el punto donde se pausaron.

Nota: Para iniciar un almacén de datos de deduplicación, en función del tamaño de hash, los datos de hash tardan en cargarse desde el disco duro a la memoria. En el panel derecho, el progreso del almacén de datos se muestra con un porcentaje.

Siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destinos: servidores de punto de recuperación**, en la que aparecerá la lista de servidores de punto de recuperación disponibles.
3. Expanda un servidor de punto de recuperación.

   Se puede ver la lista de almacenes de datos asociada con el servidor de punto de recuperación.
4. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en el nombre del almacén de datos.
   - Seleccione el almacén de datos y en el panel central haga clic en el menú desplegable **Acciones**.

   Aparecerá una lista de opciones.
5. Haga clic en **Iniciar**.

   El panel derecho muestra la información de que el almacén de datos se está iniciando. El icono de estado del almacén de datos seleccionado cambia de **Detenido** a **En ejecución**.

Detención de un almacén de datos

Si no se desea que se ejecute un almacén de datos, utilice la opción de deteneción. Al detener el almacén de datos se garantiza que ninguna tarea se está ejecutando en este almacén de datos.

Notas:

- Si se detiene un almacén de datos, se cancelarán todas las tareas en ejecución, incluyendo las tareas que esperan en cola, de ese almacén de datos.
- Si se detiene un almacén de datos mientras una tarea de replicación está en curso, al reiniciar el almacén de datos la tarea de replicación se inicia en el mismo punto en el que se había detenido el almacén de datos.
- Si se detiene el almacén de datos mientras una tarea de replicación (por ejemplo, Job-10) está en curso y durante ese tiempo dos tareas de copia de seguridad más se completan (por ejemplo, Job-11 y Job-12), cuando se reinicia el almacén de datos, las tareas de replicación se completan en secuencia (Job-10, Job-11 y Job-12 respectivamente).

Siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destinos: servidores de punto de recuperación**, en la que aparecerá la lista de servidores de punto de recuperación disponibles.
3. Expanda un servidor de punto de recuperación.

   Se puede ver la lista de almacenes de datos asociada con el servidor de punto de recuperación.
4. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en el nombre del almacén de datos.
   - Seleccione el almacén de datos y en el panel central haga clic en el menú desplegable **Acciones**.

   Aparecerá una lista de opciones.
5. Haga clic en **Detener**.

   Se abre el cuadro de diálogo **Confirmar**.
6. Seleccione **Sí** para detener el almacén de datos.

El panel derecho muestra la información de que el almacén de datos se está deteniendo.

El almacén de datos se detiene y el icono de estado para el almacén de datos seleccionado cambia de **En ejecución** a **Detenido**.

Supresión de un almacén de datos de la consola

Si ya no se desea utilizar un almacén de datos, se puede suprimir el almacén de datos. Cuando se haya suprimido, el almacén de datos se elimina de la consola. Sin embargo, el almacén de datos suprimido existe en el servidor de punto de recuperación.

Notas:

- Se puede importar el almacén de datos suprimido, cuando sea necesario.
- Para suprimir un almacén de datos que está vinculado a planes, se debe suprimir primero el plan vinculado al almacén de datos.

Siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destinos: servidores de punto de recuperación**, en la que aparecerá la lista de servidores de punto de recuperación disponibles.
3. Expanda un servidor de punto de recuperación.

   Se puede ver la lista de almacenes de datos asociada con el servidor de punto de recuperación.
4. Realice una de las acciones siguientes:

   - Haga clic con el botón secundario del ratón en el nombre del almacén de datos.
   - Seleccione el almacén de datos y en el panel central haga clic en el menú desplegable **Acciones**.

   Aparecerá una lista de opciones.
5. Haga clic en **Suprimir**.

   Se abre el cuadro de diálogo **Confirmar**.

   Nota: Si el almacén de datos está vinculado a un plan, en lugar de aparecer el cuadro de diálogo Confirmar, se mostrará un cuadro de diálogo de **Advertencia**.
6. Haga clic en **Sí**.

   El almacén de datos se elimina.

Supresión de los datos del nodo de un almacén de datos

Como administrador de almacenamiento, es posible que se desee suprimir los datos del nodo del que se ha realizado la copia de seguridad de un almacén de datos para liberar espacio y gestionar así, de manera eficaz, el espacio de almacenamiento. Arcserve UDP permite seleccionar los datos del nodo de un almacén de datos y suprímalos. Se pueden seleccionar varios nodos en un almacén de datos. Se puede suprimir cualquier tipo de datos del nodo incluyendo los datos de cifrado y de deduplicación. El almacén de datos debe estar en el estado En ejecución cuando se inicia esta tarea, que se llama tarea de borrado definitivo.

Nota: Solo se puede realizar la tarea de supresión cuando el nodo no está ejecutando ninguna tarea (por ejemplo, una tarea de copia de seguridad, de restauración o de combinación).

Siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. Haga clic en el almacén de datos que contiene los datos de nodo que desee suprimir.
3. Se muestra la página **Resumen de puntos de recuperación**.
4. Seleccione el nodo que desee suprimir.

   Advertencia: Solo seleccione, no haga clic en el nombre del nodo. Al hacer clic en el nombre de nodo se generará otra página desde donde no se podrá realizar la acción de supresión.
5. Haga clic en **Acciones**, **Suprimir**.

   Nota: Si se está utilizando el almacén de datos de deduplicación, después de suprimir los puntos de recuperación de un nodo, es posible que el espacio en disco no se libere inmediatamente. El retraso se produce porque para el almacén de datos de deduplicación:

   - El proceso de borrado definitivo y de reclamación de back-end está programado en el tiempo de inactividad del almacén de datos.
   - Parte de los bloques de datos de los puntos de recuperación suprimidos de ese nodo todavía pueden ser utilizados por puntos de recuperación de otros nodos.

     El volumen de reclamación del espacio en disco depende de la tasa de deduplicación del nodo que se desea suprimir.

6. Confirme que desea suprimir los datos del nodo.

   La tarea de borrado definitivo se inicia y los datos del nodo se suprimen del origen de datos. Se puede ver el estado de la tarea de borrado definitivo en **Eventos recientes** y en los registros.

Control de la capacidad de espacio del almacén de datos

Los almacenes de datos de Arcserve UDP se crean en el volumen o en los discos compartidos remotos del servidor de puntos de recuperación. El mecanismo de control de la capacidad del espacio del almacén de datos ayuda a controlar el uso de la carpeta de destino, cuando el destino está a punto de llegar a la plena capacidad. El espacio libre en la carpeta de destino no es suficiente para la ejecución del almacén de datos. Se puede enviar una alerta de correo electrónico si el almacén de datos ha activado la configuración de alertas de correo electrónico y el registro de actividad proporciona el resultado. Mientras tanto, la ejecución de los almacenes de datos se cambia al estado de solo restauración. Como resultado, las nuevas tareas de copia de seguridad o replicación se bloquean para impedir la copia de seguridad de los nuevos datos de la copia de seguridad.

El control incluye las siguientes opciones:

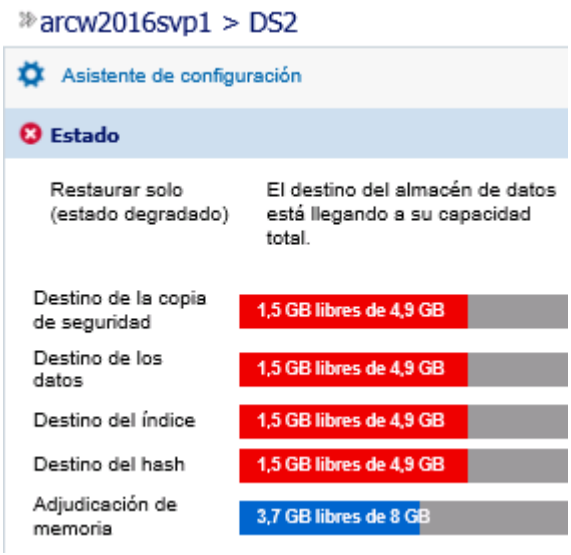
- Modificación del umbral del almacén de datos
- Uso del umbral de error
- Uso del umbral de advertencia
- Activación de la alerta de correo electrónico y funcionamiento del formato de correo electrónico

Uso del umbral de error

El umbral de error indica la ausencia de espacio libre necesario para el almacén de datos de ejecución. Además, algunos componentes del kernel no pueden funcionar correctamente. En esta situación, el almacén de datos se cambia al estado de solo restauración automáticamente si no se ha detenido manualmente el almacén de datos.

Cuando el espacio libre del almacén de datos alcanza el umbral de error:

- El estado del almacén de datos se cambia automáticamente al estado "Restaurar solo (estado degradado)". Mientras tanto, no se puede activar ninguna tarea nueva de copia de seguridad o replicación para este almacén de datos. Pero todavía se puede activar cualquier otro tipo de tarea que no genere datos nuevos. Por ejemplo, las tareas de restauración y combinación.
- La barra de espacio del almacén de datos está marcada con el color rojo.



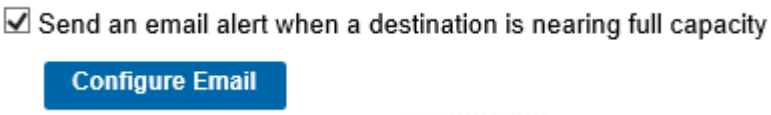
- El estado del almacén de datos está marcado con el icono rojo.



- Aparecen registros de actividad para informar de que la carpeta de destino del almacén de datos se ha quedado sin espacio libre y no podrá guardar los datos nuevos de la copia de seguridad, por lo que alcanzará el nivel de error.



- Si el almacén de datos está configurado para enviar alertas de correo electrónico cuando la carpeta de destino se está acercando a su plena capacidad, el servidor de puntos de recuperación envía alertas de correo electrónico a los destinatarios.



Uso del umbral de advertencia

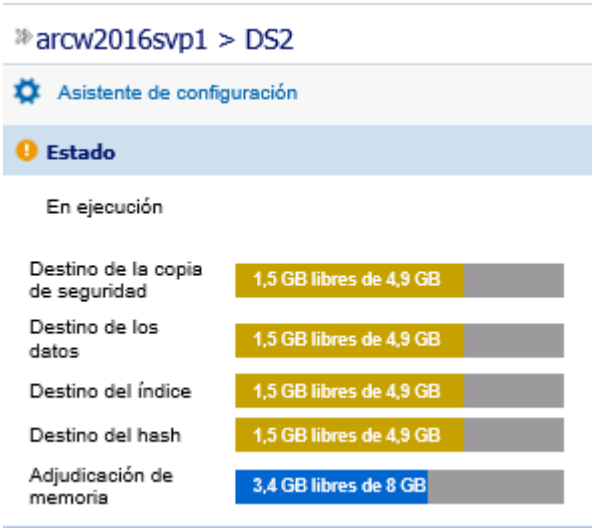
El umbral de advertencia indica que queda libre parte del espacio en el destino. Pero se puede agotar el espacio en poco tiempo si las nuevas tareas de copia de seguridad o replicación siguen funcionando.

Cuando el espacio libre del almacén de datos alcanza el umbral de advertencia:

- El estado del almacén de datos no se ve afectado y mantiene el estado original. Por ejemplo, el estado "en ejecución".
- La programación de la tarea no se ve afectada.
- El estado del almacén de datos está marcado con el signo de exclamación amarillo.



- La barra de espacio del almacén de datos está marcada con el color amarillo.



- Aparece un registro de actividades para informarle de que la carpeta de destino del almacén de datos está cerca de la capacidad máxima y que ha alcanzado el nivel de advertencia.



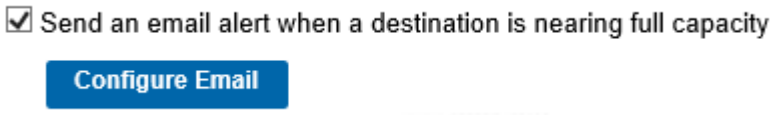
- Si el almacén de datos está configurado para enviar alertas de correo electrónico cuando la carpeta de destino se está acercando a su plena capacidad, el servidor de puntos de recuperación envía alertas de correo electrónico a los destinatarios.

Activación de la alerta de correo electrónico y funcionamiento del formato de correo electrónico

Cuando el destino del almacén de datos se está acercando a su plena capacidad o el espacio libre de la carpeta de destino alcanza el umbral de advertencia o error, se envía una alerta de correo electrónico a los destinatarios especiales para notificarles esta situación. Para recibir una alerta de correo electrónico, se deben configurar las opciones de correo electrónico y activar la opción para recibir alertas de correo electrónico.

Para activar la configuración, siga estos pasos:

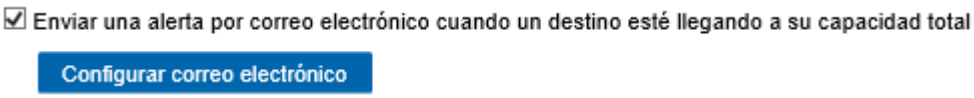
1. Active la casilla de verificación **Enviar una alerta de correo electrónico cuando un destino se está acercando a su plena capacidad** mientras se agrega/modifica/importa el almacén de datos.

   Aparece el botón Configurar correo electrónico.

2. Haga clic en **Configurar correo electrónico**.

   Aparece el cuadro de diálogo Configuración del correo.

3. Especifique los detalles en la configuración del correo electrónico y haga clic en **Aceptar**.

   El correo electrónico se ha configurado para recibir todas las alertas para el almacén de datos.

   Nota: El botón para **probar el correo electrónico** comprueba si el identificador de correo electrónico de los destinatarios está recibiendo correo electrónico. Se recomienda hacer clic en este botón y probar antes de cerrar este cuadro de diálogo.

La alerta de correo electrónico se envía a los destinatarios configurados cuando:

- La capacidad de la ruta del almacén de datos cambia de En buen estado al intervalo de advertencia (alcanza el valor del umbral de advertencia).

- La capacidad de la ruta del almacén de datos cambia del intervalo de advertencia al intervalo de error (alcanza el valor del umbral de error).
- La carpeta de destino del almacén de datos libera espacio (por ejemplo, después de la tarea de combinación del almacén de datos, después de ampliar el espacio del volumen de destino, etc.) y deja el umbral de advertencia o error dentro del intervalo En buen estado.

Formato de la alerta recibida en el correo electrónico

Alerta Error de la capacidad del almacén de datos de Arcserve UD

Servidor de puntos de recuperación de Arcserve UDP	arcw2016svp1	
Nombre del almacén de datos:	DS2	
Ruta del almacén de datos:	E:\Almacén De Datos\Backup Destinazione	
Nivel:	Error	
Destino de la copia de seguridad:	Tamaño total:	4998 MB
	Tamaño libre:	1529 MB (30,59%)
Destino de los datos:	Tamaño total:	4998 MB
	Tamaño libre:	1529 MB (30,59%)
Destino del índice:	Tamaño total:	4998 MB
	Tamaño libre:	1529 MB (30,59%)
Destino del hash:	Tamaño total:	4998 MB
	Tamaño libre:	1529 MB (30,59%)
Adjudicación de memoria:	Tamaño total:	8191 MB
	Tamaño libre:	3767 MB (46,00%)
Tiempo de repetición:	07/12/2017 3:32:07	

Para ver la capacidad actual del almacén de datos, vaya a la dirección: https://arcw2016svp1:8015/management/

Para obtener más información sobre la configuración de la capacidad del almacén de datos, haga clic aquí.

Examen de puntos de recuperación en un almacén de datos

Se puede utilizar la opción **Explorar puntos de recuperación** para ver los detalles relacionados con los puntos de recuperación y los planes asociados con el almacén de datos. Por ejemplo, se pueden ver los detalles relacionados con los valores de configuración del almacén de datos y eventos recientes.

También se pueden examinar los puntos de recuperación desde la vista Carpetas compartidas.

Para suprimir un nodo de un almacén de datos, consulte Supresión de los datos del nodo de un almacén de datos.

Siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destinos: servidores de punto de recuperación**, en la que aparecerá la lista de servidores de punto de recuperación disponibles.
3. Expanda un servidor de punto de recuperación.

   Se puede ver la lista de almacenes de datos asociada con el servidor de punto de recuperación.
4. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en el nombre del almacén de datos.
   - Seleccione el almacén de datos y en el panel central haga clic en el menú desplegable **Acciones**.

   Aparecerá una lista de opciones.

   Nota: También se puede hacer clic en el nombre de un almacén de datos para explorar el almacén de datos.
5. Haga clic en **Explorar puntos de recuperación** de las opciones mostradas después de seleccionar un almacén de datos.

   La página para el almacén de datos seleccionado aparece con el resumen que muestra información sobre los **Puntos de recuperación**. Por ejemplo, la página visualiza la información relacionada con la **Configuración del almacén de datos** y los **Eventos recientes**.

6. Para actualizar información sobre el plan o almacén de datos, seleccione el plan o almacén de datos y haga clic en **Acciones**, **Actualizar**.
7. Para restaurar, seleccione el nodo del agente y haga clic en **Acciones**, **Restaurar**.

   Se puede ver el cuadro de diálogo **Restauración** donde se puede optar por la opción de restauración que se desea realizar para el almacén de datos.

Compatibilidad de FQDN con un almacén de datos

Al crear un almacén de datos en un disco local, Arcserve UDP crea una carpeta compartida para el almacén de datos con el objetivo de que las tareas que se ejecutan en otros servidores puedan acceder a los datos.

En Arcserve UDP versión 5.0, la carpeta se compartía con el nombre de host (por ejemplo, <nombreHost>\nombreRecursoCompartido). Como consecuencia, cuando el servidor remoto podía acceder solo al servidor de puntos de recuperación con FQDN (nombre de dominio totalmente cualificado), no podía acceder al servidor de puntos de recuperación con el nombre de host y se producía un error en las tareas.

Ahora se puede compartir la carpeta del almacén de datos con FQDN o la dirección IP. Esto permite que el servidor remoto tenga acceso al almacén de datos.

Para ello, actualice el servidor de puntos de recuperación de la Consola a FQDN o la dirección IP, y cree un nuevo almacén de datos.

Nota: Para una base de datos existente, detenga el almacén de datos y vuelva a importarlo. Puede sobrescribir el almacén de datos en lugar de eliminarlo. A continuación, vuelva a implementar los planes que utilizan el almacén de datos.

Ejecutar una tarea de combinación manual o a petición

El administrador del almacenamiento puede ejecutar una tarea de combinación a petición y especificar el número de puntos de recuperación que se deben retener. Los valores pueden ser diferentes a la configuración del plan. La tarea de combinación suprime las sesiones de copia de seguridad seleccionadas de un almacén de datos para liberar el espacio y gestiona eficazmente el espacio de almacenamiento. Puede seleccionar varios nodos y ejecutar la tarea de combinación a petición.

Nota: Para la tarea de combinación, cuando se configura una tarea de replicación y se ejecuta una tarea de combinación a petición desde el almacén de datos de origen, la tarea no comprueba si las sesiones se han replicado o no. Como consecuencia, no se pueden replicar las sesiones combinadas al almacén de datos de destino y se acaban replicando más datos. Por ejemplo, supongamos que hay cinco sesiones, s1, s2, s3, s4 y s5 respectivamente. Se han replicado s1 y s2. Ahora, ejecute una tarea de combinación a petición en el origen y retenga dos sesiones. Se retienen las sesiones s4 y s5. La sesión s4 es una sesión completa. Por lo tanto, cuando se inicia la siguiente tarea de replicación, esta necesita replicar una sesión completa.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.
3. En el panel central, haga clic en el almacén de datos que contiene los datos de nodo que desee combinar.

   Se muestra la página **Resumen de puntos de recuperación**.
4. Seleccione el nodo que desee combinar.
5. Haga clic en **Acciones**, **Combinar ahora**.

   Nota: Para combinar varios nodos de un almacén de datos, pulse la tecla Ctrl o la tecla de mayúsculas y seleccione los nodos. A continuación, haga clic en **Acción**, **Combinar ahora**.

   Se abrirá el cuadro de diálogo **Ejecutar ahora una tarea de combinación**.
6. Especifique el número de puntos de recuperación que se desea retener y haga clic en **Aceptar**.

Se iniciará la tarea de combinación a petición y los datos del nodo se suprimirán del origen de datos. Puede ver el estado de la tarea de combinación en Eventos recientes y registros.

Modificación del límite de nodos activos simultáneos para la copia de seguridad manual

Para enviar copias de seguridad manuales simultáneamente para varios nodos, no controladas por la opción *Límite de nodos activos simultáneos*, agregue una clave del registro en el servidor de puntos de recuperación. Se configuran los límites para los nodos activos simultáneos en la interfaz de usuario del almacén de datos.

Siga estos pasos:

1. Se abre el Editor del registro de Windows. Para abrirlo, haga clic en **Inicio**, escriba *regedit* en el campo Buscar programas y archivos y pulse **Intro**.

   Nota: Puede ser necesario proporcionar credenciales administrativas para poder abrir el Editor del registro de Windows.

2. Busque y haga clic en la clave de registro siguiente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

3. En el menú Editar, haga clic en **Nuevo** y, a continuación, haga clic en **Valor de DWORD (32 bits)**.

   Se puede ver la lista de almacenes de datos asociada con el servidor de puntos de recuperación.

4. Especifique ManualJobsIgnoreConcurrentJobLimit como el nombre de la entrada nueva y, a continuación, pulse **Intro**.

5. Haga clic con el botón secundario del ratón en ManualJobsIgnoreConcurrentJobLimit y, a continuación, haga clic en **Modificar**.

6. Especifique 1 en el campo de datos **Valores** y, a continuación, haga clic en **Aceptar**.

7. Salga del Editor del registro.

   Nota: Después de haberse activado con 1, la clave del registro ManualJobsIgnoreConcurrentJobLimit funcionará para todos los almacenes de datos en el servidor de puntos de recuperación.

Solución de problemas: Cómo utilizar un almacén de datos cuando una o varias de las carpetas estén completas.

Síntoma:

Cómo continúo utilizando el almacén de datos cuando una de las siguientes carpetas está completa:

- Destino de la copia de seguridad del almacén de datos
- Índice de deduplicación
- Hash
- Datos

Solución:

Cambie la ruta del destino de la copia de seguridad

1. Detenga el almacén de datos.
2. Modifique los planes que están utilizando este almacén de datos. En la ficha Destino, seleccione el destino que sea una carpeta compartida o un almacén de datos diferente, seleccione la casilla de verificación **Pausar plan** y haga clic en **Guardar** el plan.
3. Suprima el almacén de datos.
4. Copie la carpeta de destino de la copia de seguridad correspondiente en un volumen de gran tamaño. Verifique que el tamaño y el número de archivos de las carpetas de origen y destino sean idénticos.

   Nota: Verifique que, antes de copiar la carpeta, se ha detenido el almacén de datos. Durante la copia, asegúrese de que todos los archivos se copian en las carpetas de destino, sin omitir ningún archivo.

   Advertencia: La omisión de cualquier archivo puede causar la corrupción de datos. Si el número de archivos o el tamaño no coincide entre las carpetas de origen y destino, no continúe con el paso siguiente.
5. Importe el almacén de datos. Especifique la nueva ruta de los datos o del índice mientras se importa el almacén de datos.
6. En la Consola de UDP, vaya a Recursos, Destinos, Servidores de puntos de recuperación.
7. Seleccione Almacén de datos en el Servidor de puntos de recuperación.

8. En los valores de configuración del panel derecho, verifique que la ruta de los datos o la ruta del destino del índice haga referencia a la ubicación correcta.

   Importante: Mientras se llevan a cabo los pasos mencionados anteriormente, NO inicie el almacén de datos hasta que se finalice el paso 8.

9. Inicie el almacén de datos.
10. Modifique los planes que se han pausado y vuelva a configurarlos para utilizar el almacén de datos importado (según el requisito). Seleccione claramente la opción **Pausar plan** y haga clic en **Guardar** el plan.

    Nota: Después de importar el almacén de datos para vincularlo a la nueva ubicación y de iniciarlo, **NO cambie** a la ruta original. Esta acción puede dañar los datos.

Cambio de la ruta de los datos o del destino del índice

1. Detenga el almacén de datos.
2. Copie la carpeta correspondiente (de los datos o del índice según el requisito) en un volumen grande. Verifique que el tamaño y el número de archivos de las carpetas de origen y destino sean idénticos.

   Nota: Verifique que, antes de copiar la carpeta, se ha detenido el almacén de datos. Durante la copia, asegúrese de que todos los archivos se copian en las carpetas de destino, sin omitir ningún archivo.

   Advertencia: La omisión de cualquier archivo puede causar la corrupción de datos. Si el número de archivos o el tamaño no coincide entre las carpetas de origen y destino, no continúe con el paso siguiente.

3. Importe el almacén de datos. Especifique la nueva ruta de los datos o del índice mientras se importa el almacén de datos.
4. En la Consola de UDP, vaya a Recursos, Destinos, Servidores de puntos de recuperación.
5. Seleccione Almacén de datos en el Servidor de puntos de recuperación.
6. En los valores de configuración del panel derecho, verifique que la ruta de los datos o la ruta del destino del índice haga referencia a la ubicación correcta.

   Importante: Mientras se llevan a cabo los pasos mencionados anteriormente, NO inicie el almacén de datos hasta que se finalice el paso 6.

7. Inicie el almacén de datos.

   Nota: Después de importar el almacén de datos para vincularlo a la nueva ubicación y de iniciarlo, **NO cambie** a la ruta original. Esta acción puede dañar los datos.

Cambio de la ruta del destino del hash

Para obtener más detalles, consulte Modificación de la ruta del hash.

Cómo gestionar un servidor de punto de recuperación

Al utilizar Arcserve UDP se pueden realizar varias operaciones en el servidor de punto de recuperación existente, como actualizar, suprimir e importar.

El servidor de punto de recuperación se muestra debajo de **Nombre** en la página **Destinos: Servidor de punto de recuperación.** Haga clic en la ficha **Acciones** o en el nombre del servidor de punto de recuperación en la página **Destinos: Servidor de punto de recuperación** para recibir todas las opciones para gestionar el servidor de punto de recuperación.

¿Qué hacer a continuación?

- Revise de los requisitos previos
- Actualización de un servidor de punto de recuperación
- Supresión de un servidor de punto de recuperación desde la consola
- Importación de un almacén de datos
- Instalación/actualización del servidor de punto de recuperación

Revisión de los requisitos previos

Para gestionar un servidor de punto de recuperación, complete los requisitos previos siguientes:

- Inicie sesión en la Consola.
- Adición de un almacén de punto de recuperación.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Actualización de un servidor de punto de recuperación

Cuando las credenciales o el protocolo se cambian para el servidor de punto de recuperación, se debe actualizar el servidor de punto de recuperación. De lo contrario, el servidor de punto de recuperación no funcionará correctamente.

Nota: Si un nodo sirve tanto de servidor de puntos de recuperación como de agente y se cambian las credenciales o el protocolo de ese nodo, actualice el nodo desde la página **Destinos: servidor de punto de recuperación**. El plan se implementará automáticamente en el agente después de actualizar el servidor de punto de recuperación. Si se actualiza el nodo desde la página **Nodos: todos los nodos**, los planes que implican esos nodos no se implementarán correctamente. Para implementar el plan, actualice otra vez el nodo desde la página **Destinos: servidor de punto de recuperación**.

Siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destinos: servidores de punto de recuperación**.
3. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en un servidor de punto de recuperación.
   - Seleccione un servidor de punto de recuperación y en el menú central haga clic en la lista desplegable **Acciones**.
4. Haga clic en **Actualizar**.

   Se abrirá el cuadro de diálogo **Actualizar nodo**.
5. Modifique los detalles según sea necesario y haga clic en **Aceptar**.

   El servidor de punto de recuperación se actualiza.

Supresión de un servidor de punto de recuperación desde la consola

Para eliminar un servidor de punto de recuperación desde la consola, utilice la opción **Suprimir**.

Nota: Cuando se elimina un servidor de puntos de recuperación, los almacenes de datos asociados no se suprimen. No se puede suprimir ningún servidor de puntos de recuperación que se esté utilizando en algún plan.

Siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destinos: servidores de punto de recuperación**.
3. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en un servidor de punto de recuperación.
   - Seleccione un servidor de punto de recuperación y en el menú central haga clic en la lista desplegable **Acciones**.
4. Haga clic en **Suprimir**.

   Se abre el cuadro de diálogo **Confirmar**.
5. Haga clic en **Sí**.

   El servidor de punto de recuperación se suprime.

Importación de un almacén de datos

La función **Importar almacén de datos** le permite agregar un almacén de datos al servidor de punto de recuperación. Se puede importar cualquier almacén de datos existente a un servidor de punto de recuperación. Los almacenes de datos suprimidos anteriormente de un servidor de punto de recuperación están disponibles para ser importados.

Nota: Cuando se pierden o dañan los datos hash de un almacén de datos de deduplicación, todavía se puede importar el almacén de datos. Proporcione una carpeta vacía como carpeta de hash. A continuación, se inicia el almacén de datos en el estado **restaurar solo** y un mensaje de error muestra que ese rol hash no está funcionando para la carpeta vacía de hash. Con este método, se puede utilizar el almacén de datos solo para las tareas de restauración. Vuelva a generar el hash si se desea ejecutar la tarea de copia de seguridad.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se muestra la página **Destinos: Servidores de punto de recuperación**.
3. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en un servidor de punto de recuperación.
   - Seleccione un servidor de punto de recuperación y en el menú central haga clic en la lista desplegable **Acciones**.
   - Para recibir alertas de correo electrónico, seleccione la casilla de verificación *Enviar una alerta de correo electrónico cuando un destino se está acercando a su plena capacidad*.

     Nota: Si no se ha configurado antes, haga clic en **Configurar correo** para proporcionar la configuración del correo electrónico.
4. Haga clic en **Importar almacén de datos**.

   Se muestra la página **Importación de un almacén de datos**.
5. Realice las acciones siguientes y haga clic en **Siguiente**:
   - Haga clic en **Examinar** para seleccionar la **Carpeta de destino de la copia de seguridad** desde donde se desea importar el almacén de datos.
   - Introduzca la **Contraseña de cifrado**.

Nota: Déjelo vacío si el almacén de datos no está cifrado.

Después de autenticar la **Carpeta de destino de la copia de seguridad**, la página **Importación de un almacén de datos** muestra los detalles del almacén de datos.

6. Modifique los detalles, si es necesario, y haga clic en **Guardar**.

   Si se ha copiado la carpeta Destino de los datos, Destino del índice y Destino de hash para el almacén de datos de deduplicación, cambie la ruta de la carpeta.

   Nota: No se puede activar o desactivar la opción de cifrado para un almacén de datos existente.

   El almacén de datos se agrega al servidor de punto de recuperación y se muestra en el cuadro de diálogo **Destinos: Servidores de puntos de recuperación**.

Instalación/actualización del servidor de punto de recuperación

Se utiliza la opción **Instalar o actualizar el servidor de punto de recuperación** por las siguientes razones:

- Cuando la instalación produce un error.
- Cuando se desea actualizar el producto.

Siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destinos: servidores de punto de recuperación**.
3. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en un servidor de punto de recuperación.
   - Seleccione un servidor de punto de recuperación y en el menú central haga clic en la lista desplegable **Acciones**.
4. Haga clic en **Instalar o actualizar el servidor de punto de recuperación**.

   Los detalles de la ruta de instalación aparecen en la misma página, encima de la lista del servidor de puntos de recuperación agregado.
5. Actualice los detalles como desee.
6. Especifique la programación de instalación/actualización y haga clic en **Aceptar**.

   La instalación o actualización empieza de acuerdo con lo programado. Se puede ver el progreso de la instalación o actualización en el panel derecho.

   Nota: Se puede cancelar una implementación del servidor de punto de recuperación si se programa para un tiempo posterior. Para cancelar una implementación del servidor de punto de recuperación, seleccione el agente y haga clic en Acciones, Cancelar implementación del agente.

Cómo gestionar servidores de Arcserve Backup

Se pueden gestionar servidores de Arcserve Backup desde la Consola de Arcserve UDP. También se puede actualizar y eliminar el servidor de Arcserve Backup desde la Consola.

Actualización del servidor de Arcserve Backup

Si se cambian las credenciales o el puerto de servicio web de Arcserve del servidor de Arcserve Backup, deben actualizarse estos datos en la consola.

Siga estos pasos:

1. Inicie sesión en la consola y haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de Arcserve Backup**.

   Se mostrará la página **Destinos:** Aparece la página **Servidores de Arcserve Backup** en el panel central.
3. Seleccione un servidor de Arcserve Backup, haga clic con el botón secundario del ratón y seleccione **Actualizar**.

   Se abre la página **Actualizar un servidor de Arcserve Backup**.
4. Rellene los campos obligatorios y, a continuación, haga clic en **Guardar**:

   Se cierra la página **Actualizar un servidor de Arcserve Backup**.

   El servidor de Arcserve Backup se ha actualizado correctamente.

Eliminación de un servidor de Arcserve Backup

Si ya no necesita un servidor de Arcserve Backup, puede suprimirse desde la consola. Antes de suprimir un servidor de Arcserve Backup, asegúrese de que el servidor de Arcserve Backup no se incluye en ninguna tarea en un plan. Si el servidor está incluido en cualquier tarea, suprima la tarea o cambie el destino de la copia de seguridad.

Siga estos pasos:

1. Inicie sesión en la consola y haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de Arcserve Backup**.

   Se mostrará la página **Destinos:** Aparece la página **Servidores de Arcserve Backup** en el panel central.
3. Seleccione un servidor de Arcserve Backup, haga clic con el botón secundario del ratón y seleccione **Suprimir**.

   Se abre el cuadro de diálogo de confirmación.
4. Haga clic en **Sí**.

   El servidor de Arcserve Backup se ha suprimido correctamente desde la consola.

Cómo gestionar una carpeta compartida

Se pueden gestionar las carpetas compartidas desde la Consola de Arcserve UDP. También se puede modificar y suprimir la carpeta compartida desde la Consola.

Modificación de una carpeta compartida

Arcserve UDP permite modificar los detalles de una carpeta compartida agregada. Si la información relacionada con la carpeta compartida cambia, se deberá modificar la carpeta compartida que se ha agregado en Arcserve UDP para que los planes funcionen.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Carpetas compartidas**.

   La página **Destinos: Carpetas compartidas** muestra las carpetas compartidas agregadas en el panel central.
3. Para gestionarla, haga clic en una de las carpetas compartidas agregadas o seleccione una carpeta compartida y haga clic en **Acciones**.
4. En las opciones mostradas, haga clic en **Actualizar**.

   Se muestra el cuadro de diálogo **Actualización**.
5. Modifique la información y haga clic en **Aceptar**.

   Ahora se ha actualizado la carpeta compartida.

Supresión de una carpeta compartida

Arcserve UDP permite suprimir una carpeta compartida agregada.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Carpetas compartidas**.

   La página **Destinos: Carpetas compartidas** muestra las carpetas compartidas agregadas en el panel central.
3. Para gestionarla, haga clic en una de las carpetas compartidas agregadas o seleccione una carpeta compartida y haga clic en **Acciones**.
4. En las opciones mostradas, haga clic en **Suprimir**.

   Se muestra un cuadro de diálogo de **Confirmación** o **Error**.
5. Para el mensaje de confirmación, haga clic en **Aceptar** para suprimir.
6. (Opcional) Para el mensaje de error, solucione el error y vuelva a intentar la supresión.

   Ahora se ha actualizado la carpeta compartida.

Cómo gestionar una consola remota

Después de crear una consola remota, es posible que se deban llevar a cabo diversas operaciones como modificar, suprimir o probar la conexión.

¿Qué hacer a continuación?

- Modificación de una consola remota
- Supresión de una consola remota
- Prueba de la conexión de la consola remota

Modificación de una consola remota

Arcserve UDP permite modificar los detalles de una consola remota agregada. Si la información de la conexión ha cambiado para la consola remota, se deberá modificar la cuenta de la consola remota agregada en Arcserve UDP.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Consola remota**.

   Se muestra la página **Destinos: Consola remota** con la consola remota agregada en el panel central.
3. Para gestionarla, haga clic en una de las consolas remotas agregadas o seleccione una consola remota y haga clic en **Acciones**.

   Se muestra la página **Modificación de una consola remota**.
4. Modifique la información y haga clic en **Aceptar**.

   Ahora se ha actualizado la consola remota.

Supresión de una consola remota

Arcserve UDP permite eliminar una consola remota cuando sea necesario.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Consola remota**.

   Se muestra la página **Destinos: Consola remota** con la consola remota agregada en el panel central.
3. Para gestionarla, haga clic en una de las consolas remotas agregadas o seleccione una consola remota y haga clic en **Acciones**.

   Se muestra un mensaje de **Confirmación** o **Error**.

   Mensaje de confirmación

   Aparece cuando la consola remota no se ha agregado a ningún plan.

   Mensaje de error

   Aparece cuando la consola remota forma parte de un plan existente.
4. (Opcional) Cuando aparezca el mensaje de error:
   a. Haga clic en **Aceptar** para cerrar el mensaje de error.
   b. Abra el plan con el que está asociado la consola remota.
   c. Suprima el plan relacionado o modifique el plan para cambiar la consola remota en la ficha de destino del plan **Replicación en un servidor de puntos de recuperación gestionado de forma remota**.

   Después de eliminar la consola remota del plan, vuelva a la página de la consola remota e intente surprimir de nuevo la consola remota.
5. En el mensaje de confirmación, haga clic en **Sí**.

   Ahora, se ha eliminado la consola remota.

Prueba de la conexión de la consola remota

Arcserve UDP le permite probar la conexión de una consola remota agregada. Se necesita una conexión correcta para la conexión de la consola remota para que el plan de replicación funcione porque la cuenta de la consola remota está asociada con el plan.

Se puede producir un error en la conexión de la consola remota por varias razones:

- Cuando la información que se agrega para un destino de la consola remota es incorrecta.
- Cuando la información sobre las credenciales, el puerto, el protocolo o el servidor proxy de la consola remota ha cambiado pero esta información no se actualiza en la Consola de Arcserve UDP.
- Cuando se interrumpe la conexión de red entre esta consola y la consola remota.
- Cuando el servicio de gestión de Arcserve UDP se detiene en la consola remota.

Se puede utilizar la opción de prueba de la conexión de la consola remota para comprobar si una consola remota está conectada y si la información agregada a la cuenta es correcta.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Consola remota**.

   Se muestra la página **Destinos: Consola remota** con la consola remota agregada en el panel central.
3. Para gestionarla, haga clic en una de las consolas remotas agregadas o seleccione una consola remota y haga clic en **Acciones**.

   Aparecen varias opciones.
4. De varias opciones que se muestran, haga clic en **Prueba de la conexión de la consola remota**.

   Aparece un mensaje de **información** si los detalles de la consola remota son correctos.

   Aparece un mensaje de **error** si los detalles de la consola remota no son correctos. Proporcione los detalles correctos para corregir la conexión y vuelva a probar.

5. (Opcional) Si aparece un mensaje de error, corrija la conexión rota comprobando uno o todos de los siguientes motivos:
   - La información de la cuenta es correcta.
   - La conexión de red se ha establecido.
   - El estado del servicio de gestión de Arcserve UDP de la consola remota es no detenido.

   Ahora, se ha probado correctamente la conexión de la consola remota.

Capítulo 10: Creación de planes para proteger datos

Esta sección incluye los siguientes temas:

Funcionamiento del plan y de las tareas

Para proteger un nodo, es necesario crear un plan con una tarea de copia de seguridad. Un plan es un grupo de tareas para gestionar la copia de seguridad, la replicación y la creación de nodos de Virtual Standby. Un plan está formado por una única tarea o por varias. Las tareas son un conjunto de actividades para definir el origen, el destino, la programación y los parámetros avanzados.

Se pueden crear las tareas siguientes:

Tareas de copia de seguridad

Le permite crear una tarea de copia de seguridad para proteger Windows, Linux y los nodos de máquina virtual basados en el host. Basándose en el tipo de nodos que se desea proteger, se debe utilizar una de las tareas de copia de seguridad siguientes:

Copia de seguridad de Windows basada en el agente

Define una tarea de copia de seguridad para proteger nodos de Windows. En un método de copia de seguridad basado en el agente, un componente de agente se utiliza para realizar la copia de seguridad de los datos. El agente está instalado en el nodo de origen.

Copia de seguridad sin agente basada en el host

Define una tarea de copia de seguridad para proteger máquinas virtuales basadas en el host en un servidor de vCenter/ESX de VMware o de Microsoft Hyper-V. En un método de copia de seguridad sin agente, no es necesario instalar un componente de agente en el servidor o en la máquina virtual. Sin embargo, tiene que instalar el agente en un servidor proxy.

Linux, basada en el agente

Define una tarea de copia de seguridad para proteger nodos de Linux. El agente se instala en un servidor de copia de seguridad de Linux y no en los nodos de origen que se desean proteger.

Tarea de replicación desde un servidor de punto de recuperación remoto

Permite la creación de una tarea para recibir datos desde un servidor de punto de recuperación remoto.

Tarea de replicación

Le permite crear una tarea de replicación de los datos de la copia de seguridad desde un servidor de punto de recuperación a otro servidor de punto de recuperación.

Tarea de Virtual Standby

Le permite crear una tarea para crear un nodo de Virtual Standby.

Tarea de copia de archivo

Le permite copiar archivos seleccionados desde el nodo de origen y almacenar los archivos copiados en una carpeta local o compartida. Se pueden almacenar también los archivos en un almacenamiento en la nube.

Tarea de copia de puntos de recuperación

Le permite copiar los puntos de recuperación a una carpeta local o compartida, o a la nube.

Tarea de replicación a un servidor de punto de recuperación remoto

Le permite crear una tarea para replicar o enviar datos a un servidor de puntos de recuperación remoto.

Tarea de archivado de archivos

Permite copiar los puntos de recuperación en un recurso compartido de red, almacenamiento en la nube o volumen de un nodo protegido. Cuando los puntos de recuperación se copian en el destino, se suprimen los archivos de origen.

Tarea de copia en cinta

Permite copiar los puntos de recuperación en una cinta con la capacidad de recuperación granular directamente desde la cinta.

Tarea de recuperación asegurada

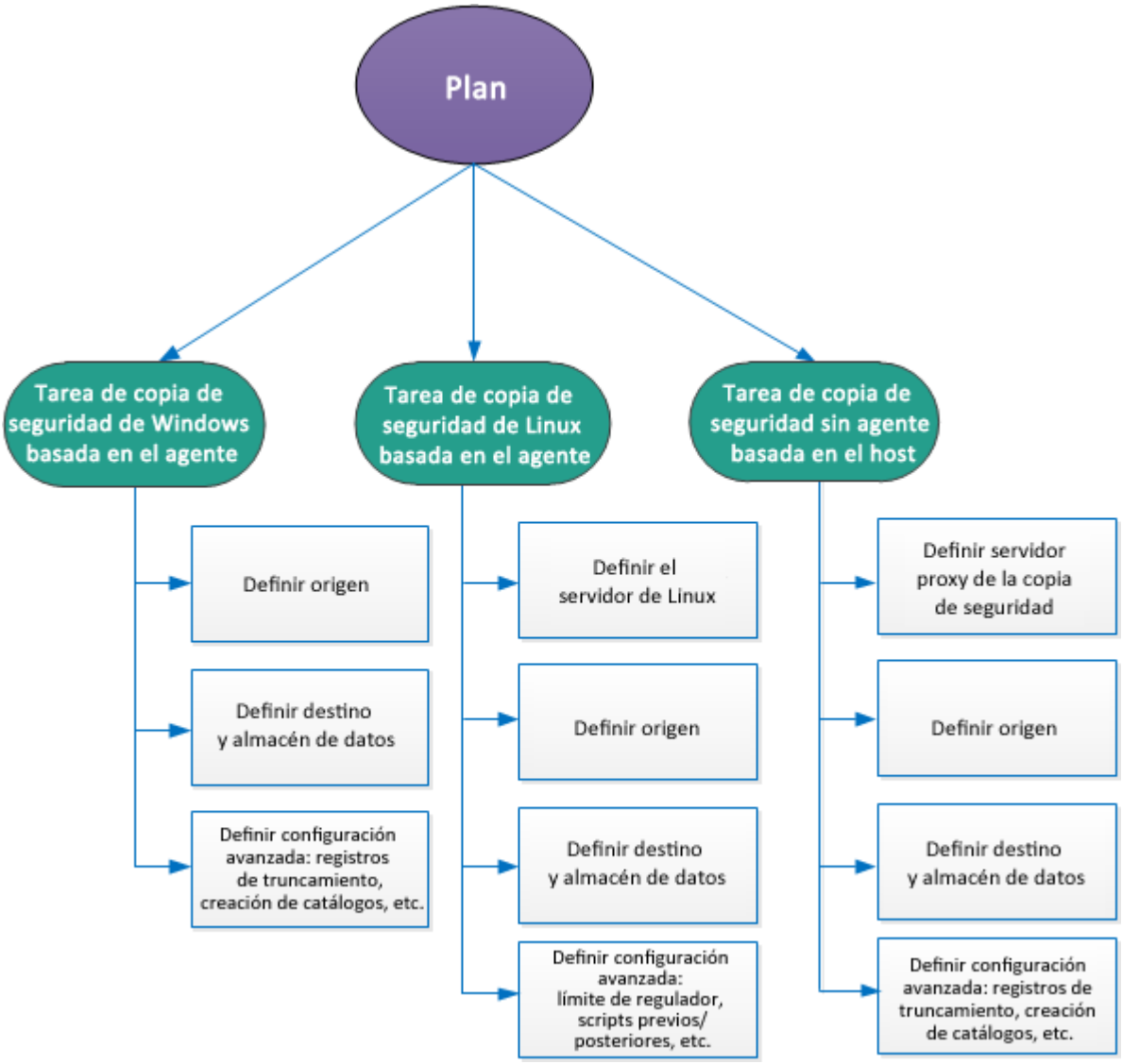
Permite verificar la accesibilidad y asegurar la recuperación de los datos.

La tabla siguiente muestra la lista de tareas de seguimiento que se pueden agregar después de la Tarea 1:

Tarea 1	Tareas de seguimiento
Copia de seguridad: Windows, basada en el agente	■ Replicación ■ Virtual Standby ■ Copia de puntos de recuperación ■ Copia de archivo ■ Replicar a un servidor RPS remoto ■ Archivado de archivos ■ Copia en cinta ■ Prueba de recuperación asegurada
Copia de seguridad: Sin agente basada en el host	■ Replicación ■ Virtual Standby ■ Copia de puntos de recuperación

	■ Replicar a un servidor RPS remoto ■ Copia en cinta ■ Prueba de recuperación asegurada
Copia de seguridad: Linux, basada en el agente	■ Replicación ■ Replicar a un servidor RPS remoto ■ Copia en cinta ■ Prueba de recuperación asegurada
Replicar datos desde un servidor de punto de recuperación remoto	■ Virtual Standby ■ Replicación ■ Prueba de recuperación asegurada
Copia de seguridad: Office 365 Exchange Online	■ Replicación ■ Copia de puntos de recuperación ■ Replicar a un servidor RPS remoto ■ Copia en cinta ■ Prueba de recuperación asegurada
Copia de seguridad: Office 365 OneDrive	■ Replicación ■ Copia de puntos de recuperación ■ Replicar a un servidor RPS remoto ■ Copia en cinta ■ Prueba de recuperación asegurada
Copia de seguridad: Office 365 SharePoint Online	■ Replicación ■ Copia de puntos de recuperación ■ Replicar a un servidor RPS remoto ■ Copia en cinta ■ Prueba de recuperación asegurada
Copia de seguridad: Archivos en una ruta UNC o NFS	■ Replicación ■ Copia de puntos de recuperación ■ Replicar a un servidor RPS remoto ■ Copia en cinta ■ Prueba de recuperación asegurada

El diagrama siguiente ilustra cómo diferentes tareas forman un plan de copia de seguridad. El diagrama también muestra parámetros que se pueden definir en cada tarea.



Cómo crear un plan de copia de seguridad en Windows

Para proteger los nodos o los nodos agrupados en clúster de Windows, es necesario crear un plan. El plan para los nodos de Windows está formado por una tarea de copia de seguridad. Esta tarea de copia de seguridad le permite especificar los nodos que se desean proteger, el destino de la copia de seguridad y la programación de la copia de seguridad. El destino de la copia de seguridad es un servidor de punto de recuperación donde se desea almacenar sus datos de copia de seguridad. El destino también puede ser un destino local o una carpeta de recurso compartido remota.

Se puede realizar una copia de seguridad de la base de datos de Oracle. Antes de crear un plan para realizar una copia de seguridad de una base de datos de Oracle, revise los requisitos previos siguientes:

- Requisito previo para realizar una copia de seguridad de una base de datos de Oracle

Para realizar una copia de seguridad de los nodos agrupados en clúster y de los discos compartidos de Microsoft, revise los requisitos previos siguientes:

- Revisión de los requisitos previos para realizar una copia de seguridad de los nodos agrupados en clúster y de los discos compartidos de Microsoft.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Creación de un plan de copia de seguridad
3. (Opcional) Realización de una copia de seguridad manual
4. Verificación de la copia de seguridad.

Revisión de las consideraciones y requisitos previos

Verifique que se han realizado las siguientes tareas de los requisitos previos:

- Se instala la última versión del Agente de Arcserve UDP (Windows).
- Inicie sesión en la Consola.
- (Opcional) Crear almacén de datos para almacenar los datos de copia de seguridad.
- Revisión de los requisitos previos para la base de datos de Oracle con el Agente de Windows de UDP.
- Revise los requisitos previos para realizar una copia de seguridad de los nodos agrupados en clúster y de los discos compartidos de Microsoft.
- (Para la copia de seguridad de SQL cuando la base de datos está en modo completo) Revise Cómo activar truncamientos del registro cuando la base de datos SQL está en modo de recuperación completa.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Los requisitos previos siguientes son para las instantáneas de hardware:

- Instale a un proveedor de hardware VSS compatible con la instantánea de hardware en los Agentes de Arcserve UDP. Una configuración habitual de un proveedor de hardware VSS incluye:
  - Especificación de un servidor que controle el LUN.
  - Especificación de las credenciales de la matriz de discos para acceder a la matriz de discos.

  Nota: Para obtener más información sobre cómo configurar el proveedor de hardware VSS, póngase en contacto con el distribuidor del hardware.

Los siguientes requisitos previos son para una copia de seguridad de red específica:

- El Agente de Windows y el servidor de puntos de recuperación deben estar en la misma red.
- El nodo de protección de Windows está programado.
- El servidor de puntos de recuperación local está conectado con varios NIC.

Revisión de los requisitos previos para la base de datos de Oracle con el Agente de Windows de UDP

Para realizar la copia de seguridad de una base de datos de Oracle con datos coherentes, se debe verificar que el modo ARCHIVELOG esté activado para permitir el archivado de los registros de rehacer.

Nota: El volumen de datos debe incluir archivos de datos de Oracle, archivos de control, archivos de parámetros del servidor y registros de rehacer en línea. Los registros de rehacer archivados deben estar ubicados físicamente en un volumen independiente.

Siga estos pasos para verificar si el modo ARCHIVELOG está activado:

a. Inicie sesión en el servidor de Oracle como usuario de Oracle con privilegios de SYSDBA.

b. En el símbolo del sistema SQL*Plus introduzca el siguiente comando:

   ARCHIVE LOG LIST;

   Aparecen los valores de configuración del registro de archivado para la instancia actual.

c. Defina la configuración siguiente:

   Modo de registro de la base de datos: modo de archivado

   Archivado automático: activado

d. Inicie el modo ARCHIVELOG.

   Nota: Si el modo ARCHIVELOG no está activado, inicie el modo ARCHIVELOG para hacer copias de seguridad de la base de datos.

Siga estos pasos para reiniciar el modo ARCHIVELOG:

a. Cierre Oracle Server.

b. Ejecute las siguientes instrucciones en Oracle:

   CONNECT SYS/SYS_PASSWORD AS SYSDBA

   STARTUP MOUNT;

   ALTER DATABASE ARCHIVELOG;

   ALTER DATABASE OPEN;

   De forma predeterminada, los registros de archivado se escriben en el área de recuperación de flash. Si no desea escribir registros de archivado en el área de recu-

peración de flash, establezca el parámetro LOG_ARCHIVE_DEST_n en la ubicación donde se desea escribir los registros de archivado.

SQL>ALTER SYSTEM SET LOG_ARCHIVE_DEST_
1='LOCATION=e:\app\administrator\oradata\<nombre_base_datos_oracle>\arch'
SCOPE= BOTH;

System altered.

SQL> ARCHIVE LOG LIST;

Aparecen los valores de configuración del registro de archivado para la instancia actual.

c. Defina la configuración siguiente:

Modo de registro de la base de datos: modo de archivado

Archivado automático: activado

Destino del archivo de archivado: E:\app\oracle\oradata\<nombre_basededatos_oracle>\arch

Secuencia de registro en línea más antigua: 21

Secuencia de registro actual: 23

El servicio del editor de Oracle VSS se ha iniciado y funciona correctamente.

Nota: Si no se ejecuta el servicio del editor VSS de Oracle, el Agente de Arcserve UDP (Windows) lo iniciará automáticamente antes de tomar la instantánea.

- Se instala el Agente de Arcserve UDP (Windows) y se programa un plan.

  Garantice que se han seleccionado los volúmenes que incluyen todos los archivos de datos de Oracle, el archivo de parámetros del servidor, los archivos de control, los registros de rehacer archivados y los registros de rehacer en línea para la copia de seguridad.

- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Si desea realizar una reconstrucción completa para una recuperación de desastres, asegúrese de seleccionar los volúmenes del sistema y los volúmenes que incluyen todos los archivos de instalación de Oracle.

Revisión de los requisitos previos para realizar una copia de seguridad de los nodos agrupados en clúster y de los discos compartidos de Microsoft.

Revise los siguientes pasos de los requisitos previos cuando se esté realizando una copia de seguridad de nodos agrupados en clúster y discos compartidos de Microsoft:

- Instale el Agente de Arcserve UDP en todos los nodos agrupados en clúster.
- Agregue todos los agentes o nodos en el mismo plan de la copia de seguridad.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Nota: Se realizará la copia de seguridad de los discos compartidos junto con el agente que posee los discos de recursos compartidos. Si el disco compartido se mueve del Nodo A al Nodo B durante una conmutación por error, para la tarea de copia de seguridad siguiente en el Nodo B se realizará una copia de seguridad del disco como disco completo incluso si la misma tarea aparece como una tarea incremental. Después de otra conmutación por error, si el disco compartido se vuelve a mover al Nodo A, incluso entonces se realizará una copia de seguridad del disco como disco completo aunque la misma tarea aparezca como una tarea incremental.

Cómo activar truncamientos del registro cuando la base de datos SQL está en modo de recuperación completa

Síntoma

Cuando la base de datos está en el modo completo y se realiza una copia de seguridad completa de la base de datos, no se puede truncar el registro de truncamiento de SQL.

Solución

Para solucionar este problema, agregue dos valores de registro para permitir que Arcserve UDP pueda ejecutar el comando BACKUP LOG para realizar la copia de seguridad del registro de transacciones. Este comando marca como reutilizable el espacio que ya se ha escrito en el archivo de la base de datos.

Siga estos pasos para agregar el valor del registro:

1. Abra el editor de tablas de registro en el equipo del agente mediante el comando siguiente:

   ```
   regedit
   ```

2. Vaya a las claves siguientes dependiendo de si la copia de seguridad es basada en el agente o sin agente:

   Para la copia de seguridad basada en el agente para sistemas operativos de 32 bits y 64 bits, vaya a la clave siguiente en el equipo del agente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Si se utiliza una versión anterior a Arcserve UDP v6.5 Actualización 2, para la copia de seguridad sin agente vaya a la siguiente clave. Cree el valor de la tabla de registro en la máquina virtual de la que se desea realizar una copia de seguridad en el servidor proxy. Si la clave de la tabla del registro no está disponible, cree la ruta completa de la clave.

   - **Sistema operativo de 32 bits:**

     HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   - **Sistema operativo de 64 bits:**

     HKEY_LOCAL_MACHINE\SOFTWARE\WoW6432Node\Arcserve\Unified Data Protection\Engine\AFBackupDll

3. Cree los siguientes dos valores de registro y establezca sus valores en 1:

- valor de DWORD llamado BackupSQLLog4Purge
- valor de DWORD llamado ForceShrinkSQLLog

  Se agrega el valor del registro.

La solución se aplicará cuando se produzca la siguiente tarea de borrado definitivo.

Creación de un plan de copia de seguridad con una tarea de copia de seguridad

Un plan de copia de seguridad incluye una tarea de copia de seguridad que realiza una copia de seguridad de un nodo físico y almacena los datos en un destino especificado. Cada tarea está formada por parámetros que definen el origen, destino, programación y otros detalles de la copia de seguridad.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Vaya a **recursos** > **Planes** > **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre la página Agregar un plan.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable Tipo de tarea seleccione **Copia de Seguridad: Windows, basada en el agente**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

La página Origen le permite especificar los nodos de origen que se desean proteger. Se pueden seleccionar más de un nodo del plan. Si no se ha agregado ningún nodo a la consola, se podrán agregar nodos al crear o modificar un plan en la página Origen. Se puede guardar un plan sin agregar ningún nodo de origen. El plan se implementa solamente después de agregar nodos de origen.

Siga estos pasos:

1. En la ficha Origen, haga clic en **Agregar**.
2. Seleccione una de las opciones siguientes:

   Seleccionar los nodos para proteger en Arcserve UDP

   Abre el cuadro de diálogo Seleccionar los nodos para proteger en Arcserve UDP. Seleccione los nodos de la lista que se muestra. Seleccione esta opción si ya se han agregado los nodos a la consola.

   Agregar nodo de Windows

   Se abre el cuadro de diálogo Agregar nodos a un plan. Seleccione esta opción si no se han agregado los nodos y desea agregarlos manualmente para la protección.

   Detectar nodos desde Active Directory

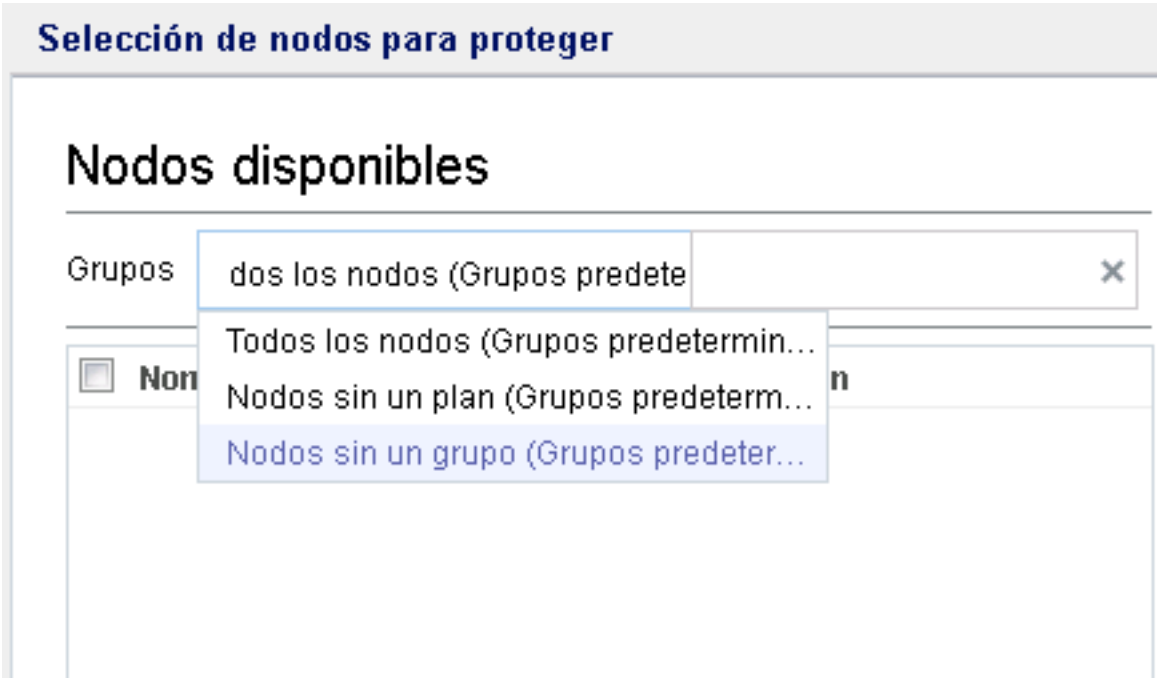
   Se abre el cuadro de diálogo Agregar nodos a la Consola de Arcserve UDP. Seleccione esta opción si desea detectar y agregar nodos en Active Directory.
3. Si ha seleccionado la opción **Seleccionar nodos para proteger en Arcserve UDP**, haga lo siguiente en el cuadro de diálogo Seleccionar nodos para proteger:
   a. (Opcional) Seleccione un filtro en la lista desplegable Grupos para filtrar nodos. Se pueden especificar palabras clave para filtrar más detalladamente los nodos.

      Los nodos se muestran en la columna Nodos disponibles.

   b. Seleccione los nodos en la columna Nodos disponibles y, a continuación, haga clic en la flecha simple hacia la derecha (>) o en la flecha doble hacia la derecha (>>) para mover los nodos seleccionados o todos los nodos respectivamente a la columna Nodos seleccionados.

      Los nodos se muestran en la columna Nodos seleccionados.

   c. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.



4. Para elegir el Tipo de El Protección, seleccione una de las opciones siguientes:

   Realizar copia de seguridad de todos los volúmenes

   Prepara una instantánea de copia de seguridad de todos los volúmenes.

   Realizar copia de seguridad de los volúmenes seleccionados

   Prepara una instantánea de copia de seguridad del volumen seleccionado.

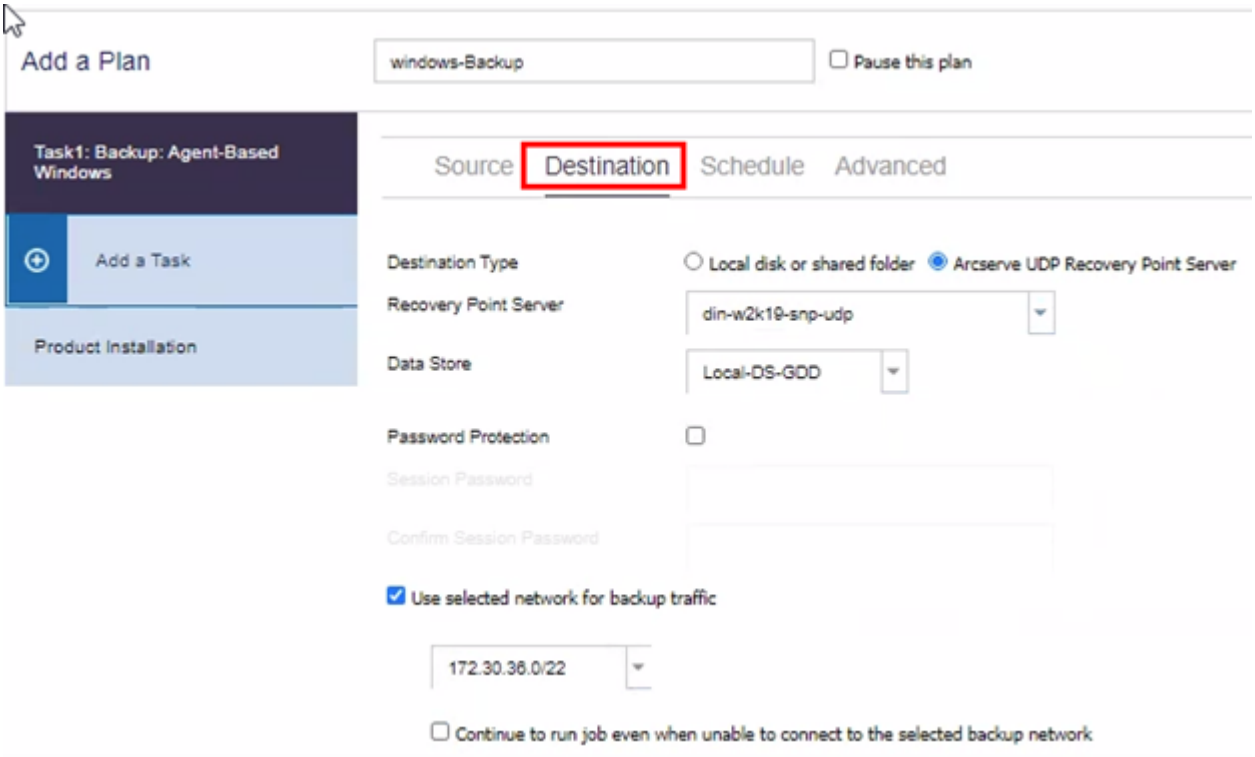
   Se especifica el origen.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Haga clic en la ficha **Destino**.



2. Seleccione uno de los siguientes tipos de destino:

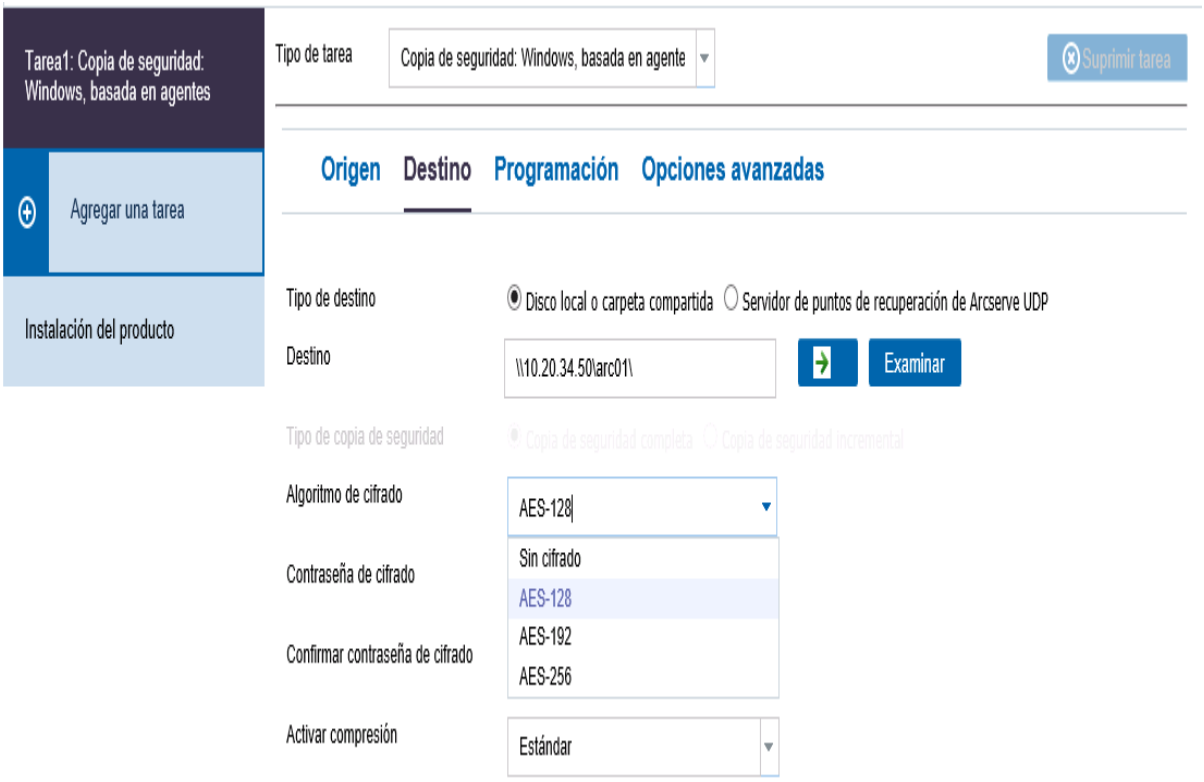
   Disco local o carpeta compartida

   Especifica que el destino de la copia de seguridad es un destino local o una carpeta compartida. Si se selecciona esta opción, se pueden guardar datos como puntos de recuperación o como conjuntos de recuperación. Las opciones Puntos de recuperación y Conjuntos de recuperación están disponibles en la ficha Programación.

   Servidor de puntos de recuperación de Arcserve UDP

   Especifica que el destino de la copia de seguridad es un servidor de puntos de recuperación. Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.

3. Si selecciona el **disco local o la carpeta compartida** como tipo de destino, proporcione los siguientes detalles:



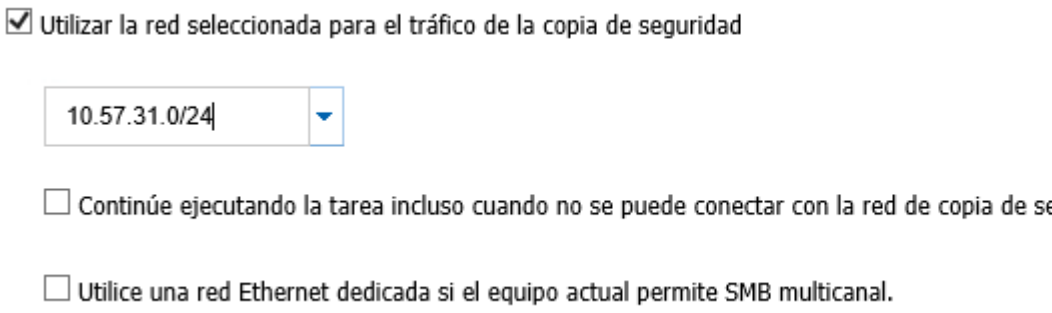
- Destino: Proporcione la ruta completa del destino local o de red. Para el destino de la red, especifique las credenciales con acceso de escritura. Haga clic en **Examinar** para buscar el destino o haga clic en el icono de flecha hacia adelante para probar la conexión y proporcione las credenciales de la carpeta de destino proporcionada.
- Algoritmo de cifrado: En la lista de opciones de la lista desplegable, seleccione el algoritmo de cifrado. Para obtener más información, consulte Configuración de cifrado.
- (Opcional) Contraseña de cifrado: Proporcione una contraseña de cifrado.
- Confirmar contraseña de cifrado: Vuelva a especificar la contraseña de cifrado para confirmarla.
- Activar compresión: Seleccione un tipo de compresión en la lista desplegable. Para obtener más información, consulte Tipo de compresión.

Nota: Si se almacenan los datos a un disco local o a una carpeta compartida, no se pueden replicar los datos a otro servidor de puntos de recuperación.

Solo se admite la replicación si se almacenan los datos en un servidor de puntos de recuperación.

4. Si selecciona **Servidor de puntos de recuperación de Arcserve UDP** como tipo de destino, haga lo siguiente:
   - Servidor de puntos de recuperación: En la lista desplegable, seleccione el servidor de puntos de recuperación (RPS).
   - Almacén de datos: En la lista desplegable, seleccione el almacén de datos de destino.
   - Protección con contraseña: Seleccione la casilla de verificación **Protección con contraseña**, proporcione la contraseña de sesión y, a continuación, vuelva a especificarla para confirmarla.

     Nota: La contraseña de la sesión es opcional cuando el destino de copia de seguridad es un almacén de datos del servidor de puntos de recuperación no cifrado..
   - (Opcional) Seleccione la casilla de verificación **Utilizar la red seleccionada para el tráfico de la copia de seguridad** y siga estos pasos:
     a. Para activar la comunicación entre el Agente de Windows y el servidor de puntos de recuperación, seleccione la red CIDR en la lista desplegable.



     Nota: Si no se puede acceder a la red de copia de seguridad seleccionada y para continuar la tarea con la red disponible o con la red predeterminada, haga clic en la casilla de verificación **Continuar ejecutando la tarea incluso cuando no se pueda conectar con la red de copia de seguridad seleccionada**.

     b. Para desactivar la función SMB multicanal para que los datos se transfieran solo a través de la red seleccionada, seleccione la casilla de verificación **Utilizar una red Ethernet dedicada si el equipo actual permite SMB multicanal**.

Notas:

- Esta opción no se encuentra disponible de forma determinada. Para activar esta opción, vaya a la siguiente ubicación de la carpeta: C:\Archivos de programa\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. A continuación, modifique el valor de *useDedicatedEthernet* como True.

```
- <SpecifyNetwork>
      <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

  La función Especificar red se desactiva en caso de almacén de datos remoto, que utilizaba la carpeta compartida de la red como destino.

- Cuando se reinician los servicios de gestión de Arcserve UDP, se activa la función SMB multicanal.
- La función SMB multicanal está activada en Windows de forma predeterminada.

Se especifica el destino.

Especificación de la programación

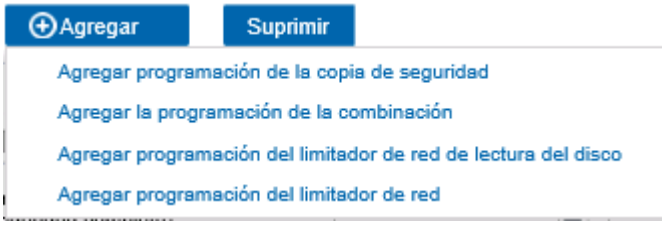
La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y se pueden proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

Siga estos pasos:

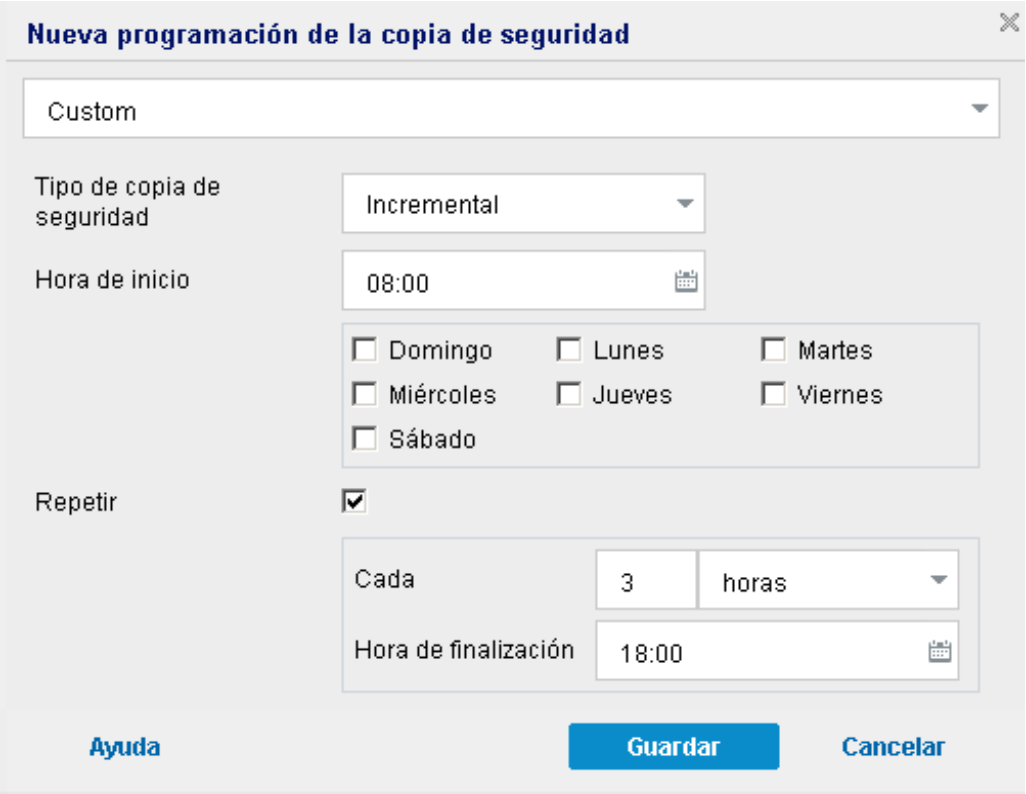
1. Agregue la programación de la copia de seguridad, de la combinación, del regulador de la lectura del disco y del regulador de la red.



Agregar programación de la copia de seguridad

a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

   Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Verificar

Especifica la programación de la copia de seguridad para las copias de seguridad de verificación.

Arcserve UDP verifica que los datos protegidos sean válidos y estén completos mediante una comprobación de confianza de la imagen de copia de seguridad almacenada en el origen de la copia de seguridad. Si es necesario, volverá a sincronizar la imagen. Una copia de seguridad de verificación se fijará en la copia de seguridad más reciente de cada bloque individual y comparará el contenido y la información con la de origen. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad de un bloque no coincide con la del origen (posiblemente por cambios en el sistema desde la última copia de seguridad), Arcserve UDP actualiza (resincroniza) la copia de seguridad del bloque que no coincide. Se puede utilizar también una copia de seguridad de verificación (aunque poco frecuentemente) para obtener la garantía de copia de seguridad completa sin utilizar el espacio necesario para una copia de seguridad completa.

Ventajas: produce una pequeña imagen de copia de seguridad si se compara con la copia de seguridad completa porque solamente se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventajas: el tiempo durante el cual se realiza la copia de seguridad es considerable puesto que todos los bloques de origen se comparan con los bloques de la última copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad

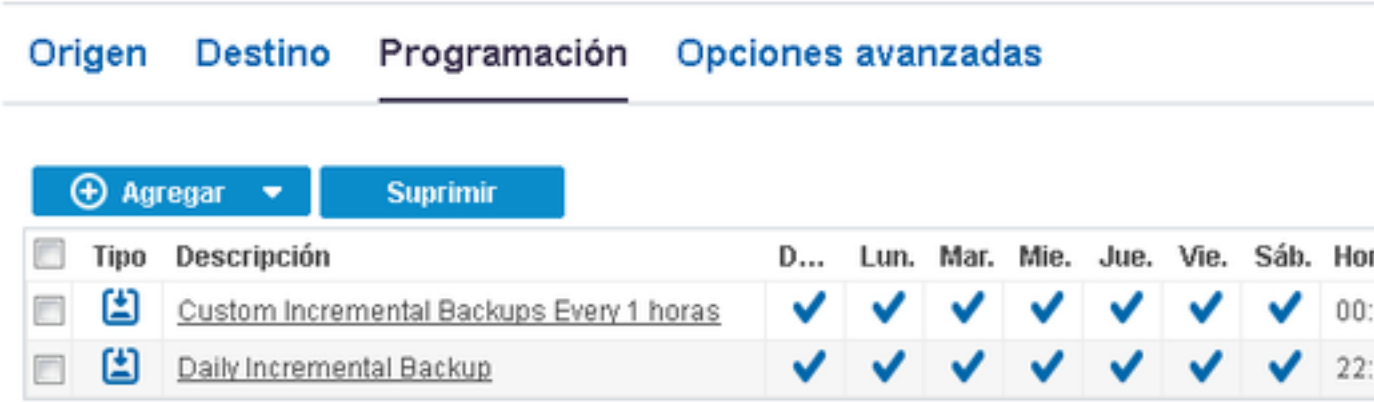
rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

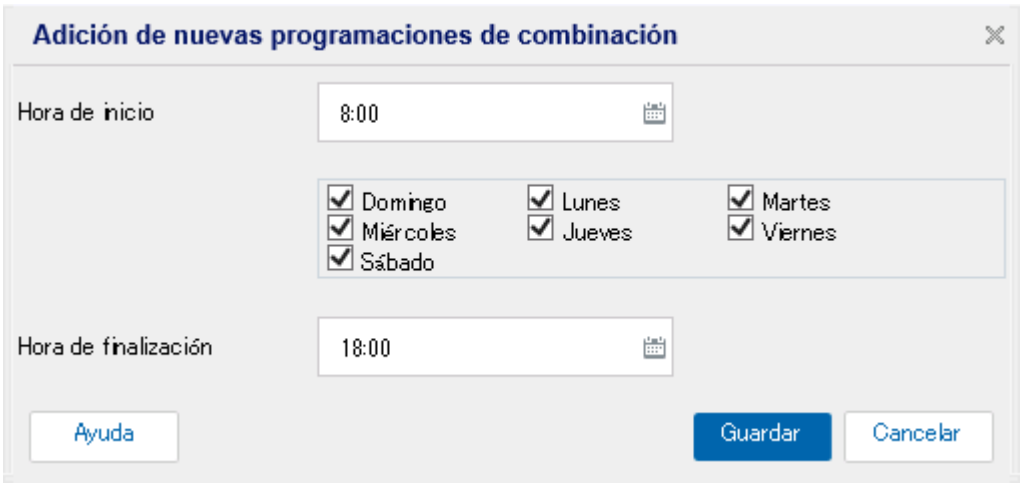
La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en **Agregar** y seleccione **Agregar programación de la combinación**.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.



b. Especifique la hora de inicio para iniciar la tarea de combinación.

c. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

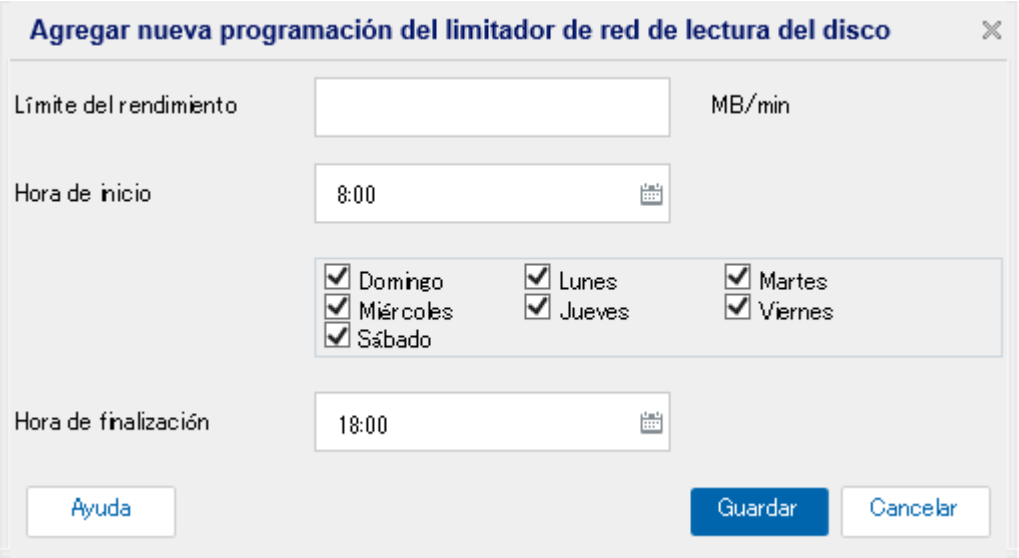
d. Haga clic en **Guardar**.

La Programación de la combinación se especifica y se muestra en la página **Programación**.

Adición de la programación del regulador de la lectura de disco

a. Haga clic en **Agregar** y seleccione **Agregar programación del regulador de la lectura de disco**.

   Se abre el cuadro de diálogo **Agregar nueva programación del regulador de la lectura de disco**.



b. Especifique el límite de rendimiento en MB por minuto.

c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

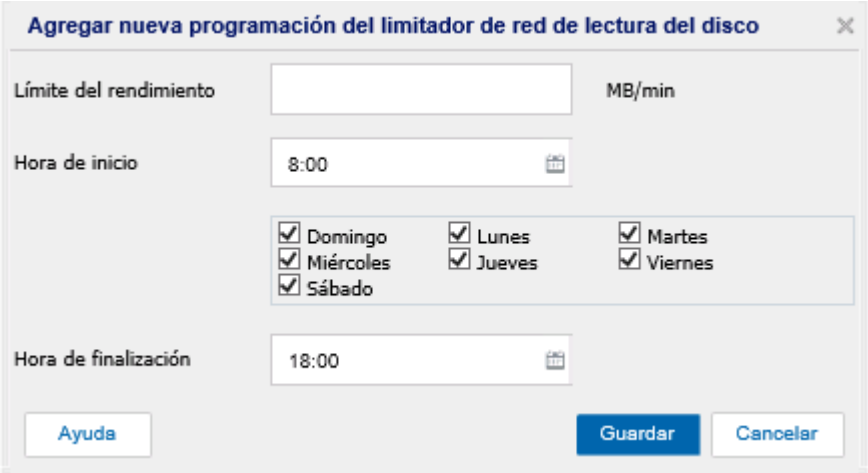
La programación del regulador de la lectura de disco se especifica y se muestra en la página **Programación**.

Adición de la programación del regulador de la red

Nota: La programación del regulador de la red solo aparece para la copia de seguridad basada en el Agente de Windows al definir un almacén de datos con la deduplicación activada como destino para el plan.

a. Haga clic en **Agregar** y seleccione **Agregar programación del regulador de la red**.

   Se abre el cuadro de diálogo **Agregar programación del regulador de la red**.



b. Especifique el límite del rendimiento en MB o kB por segundo.

   Nota: El valor mínimo predeterminado es de 500 kbps. Para cambiar el valor predeterminado, siga estos pasos:

   i. En la ruta del registro SOFTWARE\Arcserve\Unified Data Protection\Management\Console, agregue la clave MinNetworkThrottleValueInKpbs, cuyo tipo es REG_SZ, y establezca el valor.

   ii. Reinicie el servicio de gestión de Arcserve UDP.

   iii. Modifique el plan o cree uno nuevo.

   Se aplica el valor personalizado.

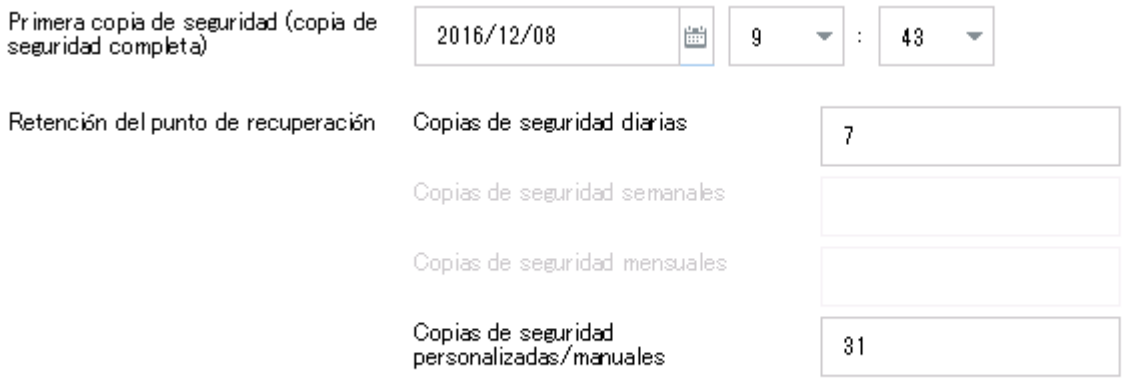
c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

La programación del regulador de la red se especifica y se muestra en la página **Programación**.

2. Especifique la hora de inicio para la copia de seguridad programada.



3. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

   Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo Programación de la copia de seguridad.

   Se especifica la programación.

Funcionamiento de la programación avanzada y de la retención

La opción de programación le permite especificar una programación personalizada, una programación diaria/semanal/mensual o ambas. En la programación personalizada, se puede configurar la programación de la copia de seguridad durante cada día de la semana y se pueden agregar hasta cuatro programaciones de copia de seguridad cada día. Se puede seleccionar un día específico de una semana y crear un período de tiempo para definir cuando se desea ejecutar la copia de seguridad y con qué frecuencia.

Programación	Tarea compatible	Comentarios
Copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para ejecutar las tareas de copia de seguridad.
Regulación de la copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para controlar la velocidad de la copia de seguridad.
Combinar	Tarea de combinación	Defina cuando se deben ejecutar las tareas de combinación.
Programación diaria	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad diarias.
Programación semanal	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad semanales.
Programación mensual	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad mensuales.

Se pueden especificar también los valores de configuración de retención para los puntos de recuperación.

Nota: Establezca la configuración de la retención en cada plan para controlar cómo se retienen los datos para los nodos asignados a ese plan en el almacén de datos de destino.

Las programaciones para las copias de seguridad diarias/semanales/mensuales son independientes de la programación personalizada y de las unas a las otras. Se puede configurar solamente ejecutar una copia de seguridad diaria, una copia de seguridad semanal o una copia de seguridad mensual sin configurar la programación personalizada.

Programación de la tarea de copia de seguridad

Se pueden agregar cuatro períodos de tiempo por día en la programación de la copia de seguridad. Un período de tiempo válido es desde las 12:00 horas hasta las 23:59 horas. No se puede especificar un período de tiempo como, por

ejemplo, de las 18:00 horas a las 06:00 horas. En tales casos, se debe especificar manualmente dos períodos de tiempo diferentes.

Para cada período de tiempo, la hora de inicio está incluida y, en cambio, no se incluye la hora de finalización. Por ejemplo, se ha configurado ejecutar una copia de seguridad incremental ejecutada todas las horas entre las 06:00 horas y las 09:00 horas y la copia de seguridad se iniciará a las 06:00 horas. Esto significa que la copia de seguridad se ejecuta a las 06:00 horas, a las 07:00 horas y a las 08:00 horas, pero NO a las 09:00 horas.

Nota: Si desea ejecutar la tarea de copia de seguridad reiteradamente hasta el final del día, configure la programación hasta las 12:00 horas. Por ejemplo, para ejecutar la tarea de copia de seguridad cada 15 minutos durante todo el día, configure la programación de las 12:00 a las 12:00, cada 15 minutos.

Programación del regulador de la copia de seguridad

La programación del regulador de la copia de seguridad le permite controlar la velocidad del rendimiento de la copia de seguridad, que a su vez controla el uso de recursos (E/S del disco, CPU, ancho de banda de la red) del servidor del que se está realizando la copia de seguridad. Esto es útil si no se desea afectar al rendimiento del servidor durante el horario comercial. Se pueden agregar cuatro períodos de tiempo por día en la programación del regulador de la copia de seguridad. Para cada período de tiempo, se puede especificar un valor en MB por minuto. Este valor se utiliza para controlar el rendimiento de la copia de seguridad. Los valores válidos van desde 1 MB/minuto a 99999 MB/minuto.

Si una tarea de copia de seguridad excede el tiempo especificado, el límite del regulador se ajusta según el período de tiempo especificado. Por ejemplo, se ha definido el límite del regulador de la copia de seguridad en 500 MB/minuto desde las 08:00 horas a las 20:00 horas y en 2500 MB/minuto de las 20:00 horas a las 22:00 horas. Si una tarea de copia de seguridad se inicia a las 19:00 horas y se ejecuta durante tres horas, el límite del regulador es de 500 MB/minuto de las 19:00 horas a las 20:00 horas y de 2500 MB/minuto de las 20:00 horas a las 22:00 horas.

Si no se define ninguna programación de la copia de seguridad ni ninguna programación del rendimiento de la copia de seguridad, la copia de seguridad se ejecuta tan deprisa como pueda.

Programación de la combinación

Le permite combinar puntos de recuperación basándose en la programación proporcionada.

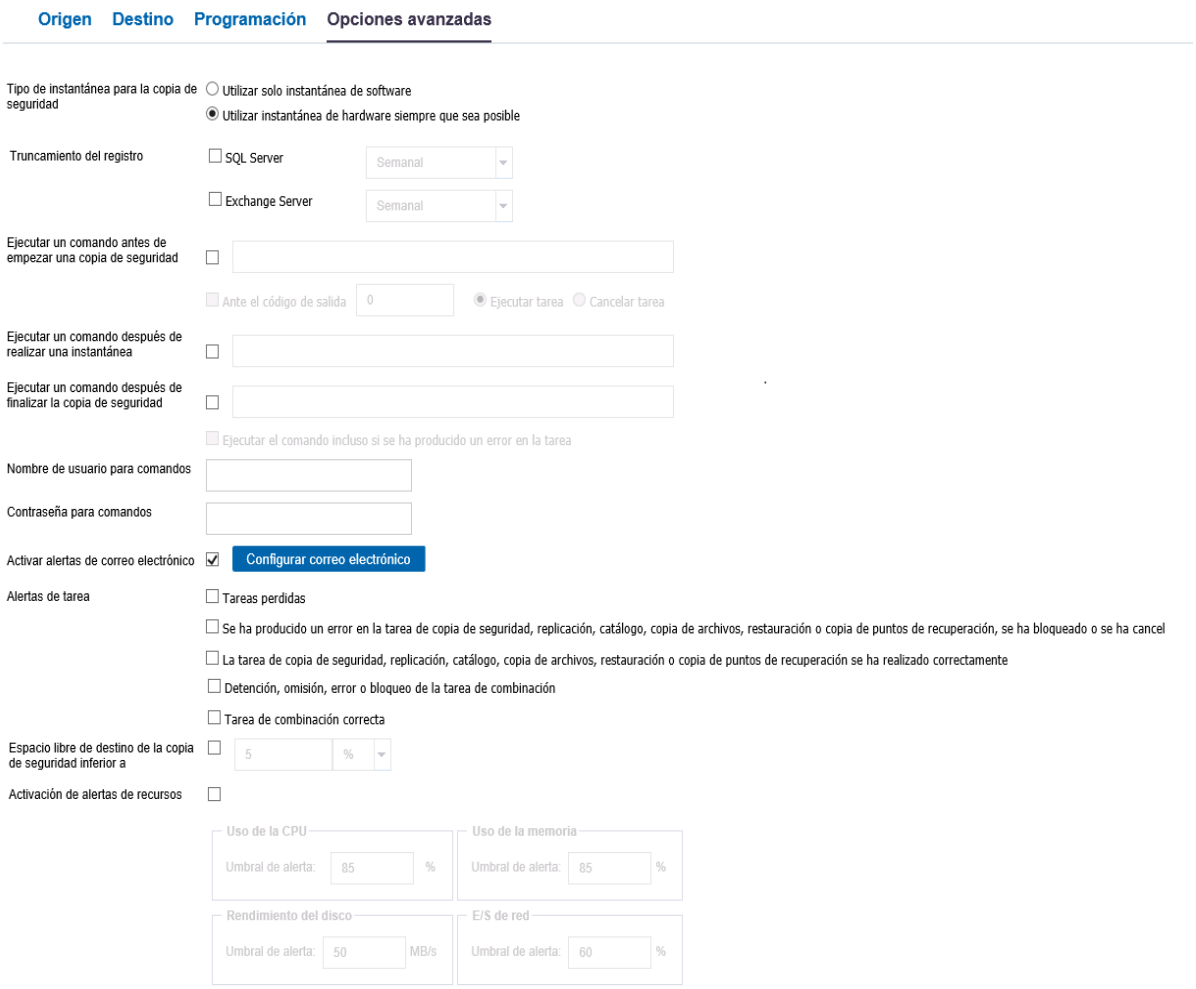
Tenga en cuenta los puntos siguientes para la tarea de combinación:

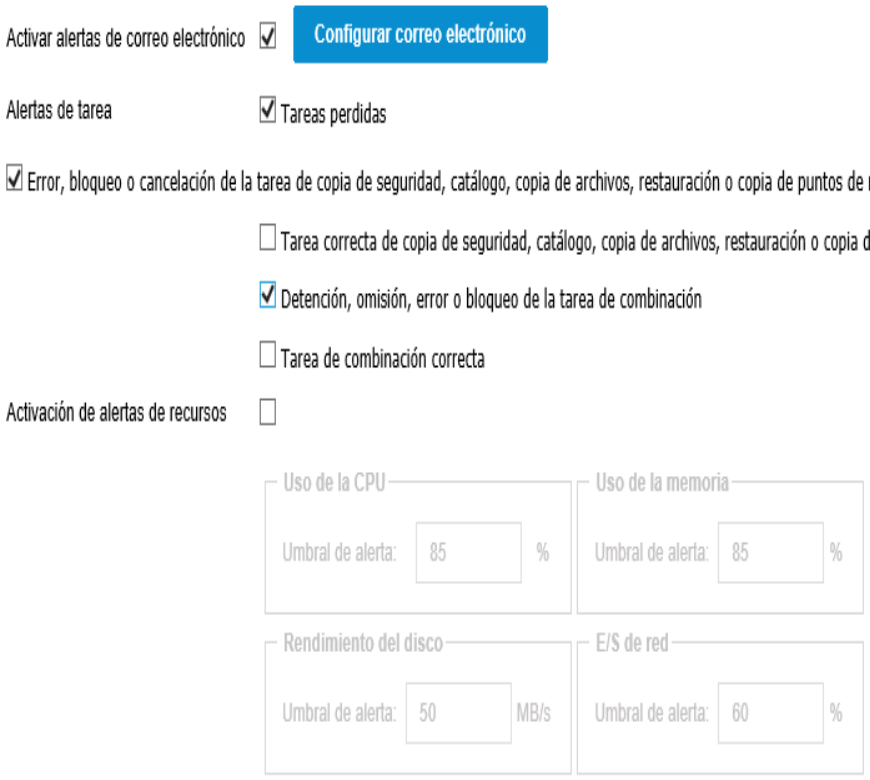
- Solamente una tarea de combinación puede ejecutarse para un nodo en cualquier momento proporcionado.
- Si se inicia una tarea de combinación, se tiene que completar antes de que la siguiente tarea de combinación se pueda iniciar. Esto no significa que, si uno o más conjuntos de puntos de recuperación se combinan, no se pueda agregar un punto de recuperación nuevo a este proceso de combinación hasta que el proceso de combinación del conjunto actual de puntos de recuperación se complete.
- Si una tarea de combinación está procesando más de un conjunto de puntos de recuperación (por ejemplo, el conjunto [1~4], el conjunto [5~11] y el conjunto [12~14] son tres conjuntos), el servidor de puntos de recuperación procesará estos conjuntos uno a uno.
- Si una tarea de combinación se reanuda después de una pausa, la tarea detecta en qué punto se ha pausado y reanuda la combinación a partir del punto de pausa.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye la configuración de registros de truncamiento, proporcionar la ubicación de los scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha Avanzada:


Origen
Destino
Programación
Opciones avanzadas
Tipo de instantánea para la copia de seguridad
Utilizar solo instantánea de software
Utilizar instantánea de hardware siempre que sea posible
Truncamiento del registro
SQL Server
Semanal
Exchange Server
Semanal
Ejecutar un comando antes de empezar una copia de seguridad
Ante el código de salida
0
Ejecutar tarea
Cancelar tarea
Ejecutar un comando después de realizar una instantánea
Ejecutar un comando después de finalizar la copia de seguridad
Ejecutar el comando incluso si se ha producido un error en la tarea
Nombre de usuario para comandos
Contraseña para comandos
Activar alertas de correo electrónico
Configurar correo electrónico
Alertas de tarea
Tareas perdidas
Se ha producido un error en la tarea de copia de seguridad, replicación, catálogo, copia de archivos, restauración o copia de puntos de recuperación, se ha bloqueado o se ha cancel
La tarea de copia de seguridad, replicación, catálogo, copia de archivos, restauración o copia de puntos de recuperación se ha realizado correctamente
Detención, omisión, error o bloqueo de la tarea de combinación
Tarea de combinación correcta
Espacio libre de destino de la copia de seguridad inferior a
5
%
Activación de alertas de recursos
Uso de la CPU
Umbral de alerta:
85
%
Uso de la memoria
Umbral de alerta:
85
%
Rendimiento del disco
Umbral de alerta:
50
MB/s
E/S de red
Umbral de alerta:
60
%



Siga estos pasos:

1. Especifique los siguientes detalles:

   Tipo de instantánea para la copia de seguridad

   Seleccione una de las opciones siguientes para la instantánea de copia de seguridad:

   Utilizar solo instantánea de software

   Especifica que el tipo de copia de seguridad utiliza solo la instantánea de software. Arcserve UDP no buscará la instantánea de hardware. La instantánea de software utiliza menos recursos en las máquinas virtuales. Se puede utilizar esta opción si el servidor tiene una velocidad de configuración y procesamiento menor.

   Utilice la instantánea de hardware siempre que sea posible

   Especifica que el tipo de copia de seguridad primero busca una instantánea de hardware. Si se cumplen todos los criterios, el tipo de copia de seguridad utiliza la instantánea de hardware.

   Nota: Para obtener más información sobre los criterios de instantánea de hardware, consulte los requisitos previos.

   Cómo truncar un registro

Le permite especificar la programación para truncar los registros de SQL Server y Exchange Server. Se puede especificar la programación como **Diaria**, **Semanal** o **Mensual**.

Activación del borrado definitivo de los registros cada hora para SQL a través de un conmutador de registro

- Configure la configuración del plan. Seleccione la opción SQL Server en la sección Truncar registro en la ficha Avanzadas y, a continuación, seleccione Diariamente.
- Establezca la clave de registro en el equipo de SQL Server en los hosts del Agente de UDP. PurgeSqlLogPerHour es el intervalo en horas para borrar definitivamente el registro de SQL.

  Ruta: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

  Nombre del valor: PurgeSqlLogPerHour (indica el intervalo en horas para borrar definitivamente el registro de SQL).

  Tipo de valor: REG_DWORD

Nombre de usuario

Le permite especificar el usuario que se autoriza para ejecutar un script.

Contraseña

Le permite especificar la contraseña del usuario autorizado para ejecutar el script.

Ejecutar un comando antes de empezar una copia de seguridad

Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta completa donde está almacenado el script. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de seguridad continuará cuando el script devuelva el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detendrá cuando el script devuelva el código de salida.

Ejecutar un comando después de realizar una instantánea

Le permite ejecutar un script después de realizar la instantánea de la copia de seguridad. Especifique la ruta completa donde está almacenado el script.

Para ejecutar el script posterior a la instantánea incluso durante un error de instantánea, seleccione **Ejecutar el comando incluso se ha producido un error en la instantánea**.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta completa donde está almacenado el script.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y se pueden especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy. Para obtener más información sobre cómo configurar el correo electrónico, consulte la sección Configuración de la configuración del correo electrónico y alertas.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de tareas que se desea recibir.

Cómo activar las alertas de recurso

Le permite especificar un umbral para el Uso de CPU, Uso de memoria, Rendimiento del disco y E/S de la red. Se puede proporcionar el valor en porcentaje. Se recibirá un correo electrónico cuando se exceda el valor de Umbral de alerta.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en Guardar.

Los cambios se guardan y se muestra una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **Recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar.

El plan de copia de seguridad se crea y se implementa automáticamente en el nodo de origen. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

(Opcional) Realización de una copia de seguridad manual

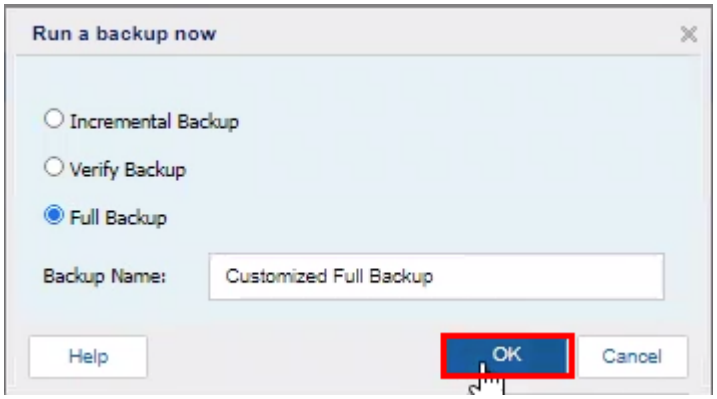
Normalmente se realizan copias de seguridad automáticamente y las controlan los valores de configuración de programación. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario. Por ejemplo, si tiene una programación de repetición para las copias de seguridad completas, incrementales y de resincronización y desea hacer cambios importantes en el equipo, se deberá realizar una copia de seguridad manual inmediata sin necesidad de esperar a la siguiente copia de seguridad programada.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Vaya a **recursos** > **Plan** > **Todos los planes**.

   La lista de todos los planes se muestra en el panel central.
3. Haga clic con el botón secundario del ratón en el plan y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
4. En el cuadro de diálogo Ejecutar una copia de seguridad ahora, seleccione el tipo de copia de seguridad que desea realizar y, a continuación, especifique el nombre de la copia de seguridad si es necesario.



A continuación se especifican las opciones disponibles:

Copia de seguridad incremental

Inicia una copia de seguridad incremental del equipo. Una copia de seguridad incremental sólo hará una copia de seguridad de los bloques que han cambiado desde la copia de seguridad anterior.

Nota: Si está realizando una copia de seguridad por primera vez, la copia de seguridad completa se iniciará automáticamente aunque haya seleccionado la opción Copia de seguridad incremental.

Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Ésta es la manera más óptima de realizar copias de seguridad.

Copia de seguridad de verificación

Inicia una copia de seguridad de verificación de su equipo examinando la copia de seguridad más reciente de cada bloque individual y comparando el contenido y la información con la original. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad para un bloque no coincide con la de origen, el Agente de Arcserve UDP (Windows) actualizará (resincronizará) la copia de seguridad del bloque que no coincida.

Ventaja: Una imagen de copia de seguridad muy pequeña se produce cuando se compara con una copia de seguridad completa porque solo se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventaja: El tiempo de copia de seguridad es lento porque todos los bloques del disco de origen se comparan con los bloques de la última copia de seguridad.

Copia de seguridad completa

Inicia una copia de seguridad completa del equipo o los volúmenes seleccionados.

Notas:

- Si se agrega un nuevo volumen al origen de la copia de seguridad, se realizará una copia de seguridad completa del nuevo volumen agregado, independientemente del método de copia de seguridad general seleccionado.
- Si no se especifica ningún nombre de copia de seguridad, de forma predeterminada se denominará Copia de seguridad completa/incremental/de verificación personalizada.

5. Haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.

6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.

7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   Nota: Solamente se puede restaurar una tarea cada vez. Si intenta iniciar una tarea de copia de seguridad manualmente cuando se está ejecutando otra tarea al mismo tiempo, aparecerá un mensaje de alerta para informar de que otra tarea está en ejecución y solicitará intentarlo de nuevo más tarde.

   La copia de seguridad manual se realiza correctamente.

Verificación de la copia de seguridad.

Para verificar la tarea de copia de seguridad, confirme que se ha creado correctamente el plan de copia de seguridad. Después de verificar que el plan se ha creado correctamente, confirme si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Se puede verificar el estado de las tareas de copia de seguridad en la ficha **Tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga uno de estos métodos para verificar las tareas de copia de seguridad:

Método 1

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas finalizadas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Método 2

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Tareas correctas**.

   La lista de tareas de copia de seguridad completadas aparecerá en el panel central.
3. Haga clic en la tarea que desea verificar.

   Se actualiza el panel derecho.
4. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
5. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Cómo crear un plan de copia de seguridad de Nutanix

Para proteger los nodos de Nutanix, es necesario crear un plan. Los nodos del plan consisten en una tarea de copia de seguridad. Esta tarea de copia de seguridad le permite especificar los nodos que se desean proteger, el destino de la copia de seguridad y la programación de la copia de seguridad. El destino de la copia de seguridad es un servidor de punto de recuperación donde se desea almacenar sus datos de copia de seguridad. El destino también puede ser un destino local o una carpeta de recurso compartido remota.

Para explorar las funciones disponibles para la función Nutanix en Arcserve UDP, consulte Cómo funcionan Nutanix con Arcserve UDP.

Cómo crear un plan de Virtual Standby a Nutanix AHV

Para proteger Virtual Standby en Nutanix AHV, consulte Protección de Virtual Standby en Nutanix AHV.

Cómo crear una máquina virtual instantánea en Nutanix AHV

Para crear una máquina virtual instantánea en Nutanix AHV, consulte Cómo crear una máquina virtual instantánea en Nutanix AHV.

Cómo crear un plan de recuperación asegurada para proteger Nutanix AHV para el nodo de Linux

Para crear un plan de recuperación asegurada para proteger Nutanix AHV para el nodo de Linux, consulte Cómo crear un plan de recuperación asegurada para proteger Nutanix AHV para el nodo de Linux.

Cómo realizar la copia de seguridad del volumen compartido de clúster

Arcserve UDP es compatible con la copia de seguridad de los volúmenes compartidos del clúster (CSV) desde v6.5 Actualización 4. Los volúmenes CSV se crean en el espacio de almacenamiento y son transparentes para el Agente de Arcserve UDP (Windows). El volumen CSV siempre se considera para la copia de seguridad completa a nivel del volumen, sin tener en cuenta el tipo de tarea de copia de seguridad (completa o incremental). La copia de seguridad del volumen CSV protege los datos de todos los sistemas de archivos populares como, por ejemplo, NTFS, deduplicación de NTFS, ReFS y CSVFS.

Se puede crear un plan basado en el agente o actualizar un plan existente basado en el agente de la Consola de Arcserve UDP para realizar la copia de seguridad del volumen CSV especificado.

Siga estos pasos:

1. Seleccione el volumen compartido de clúster en el equipo del agente. Para obtener más información, consulte Modificación de la configuración del equipo del agente para realizar la copia de seguridad del volumen CSV.

   Nota: También se puede ejecutar la tarea de copia de seguridad desde el equipo del Agente de Windows. Para obtener más información, consulte Cómo realizar la copia de seguridad desde el equipo del Agente de Windows.

2. Para realizar la copia de seguridad desde la Consola de Arcserve UDP, vaya a la ficha **Recursos**.
3. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.
4. En el panel central, haga clic en **Agregar un plan** y especifique un nombre de plan.
5. En la lista desplegable **Tipo de tarea** seleccione **Copia de Seguridad: Windows, basada en el agente**.
6. En la ficha **Origen** del plan, seleccione la casilla de verificación **Realizar copia de seguridad de todos los volúmenes** como **Tipo de protección**.
7. Especifique los detalles de los campos Destino, Programación y Avanzada. Para obtener más información, consulte Cómo crear un plan de copia de seguridad en Windows.

   Ahora, después de guardar el plan cuando se ejecuta la tarea de copia de seguridad, se realiza la copia de seguridad del volumen CSV especificado para el Agente de Windows.
8. Compruebe el estado de las tareas de copia de seguridad. Para obtener más información, consulte Verificación de la copia de seguridad.

   Notas:

   - El registro de actividad del nodo de propietario muestra el progreso de la tarea de copia de seguridad y registra el mensaje de confirmación tras la finalización correcta de la copia de seguridad. El registro de actividad del nodo miembro (que no es el propietario) muestra un mensaje de advertencia tal y como se muestra a continuación, pero el estado de la copia de seguridad se muestra como correcto.

     Advertencia: Se ha producido un error al buscar la ubicación física del volumen compartido del clúster [C:\ClusterStorage\Volume1]. Este volumen se excluirá de la copia de seguridad.
   - Si se desea excluir el volumen CSV durante la copia de seguridad, realice los pasos siguientes:

     a. En el nodo del Agente de UDP, abra el registro en la ruta siguiente:

        HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

     b. Cree un valor DWORD como BackupCSV.

c. Establezca el valor en 0.

   El volumen CSV ahora se excluye durante la copia de seguridad.

Modificación de la configuración del equipo del agente para realizar la copia de seguridad del volumen CSV

Antes de realizar la primera copia de seguridad, se deben establecer los valores de configuración de la copia de seguridad que se aplican a cada tarea de copia de seguridad. Estos valores de configuración se pueden conservar para las copias de seguridad futuras o se pueden modificar en cualquier momento desde la página principal del Agente de Arcserve UDP (Windows).

Siga estos pasos:

1. En la página principal del Agente de Arcserve UDP (Windows) o del monitor del Agente de Arcserve UDP (Windows), haga clic en **Configuración**.

   Aparecerá la ventana Configuración.

2. Haga clic en la ficha **Configuración de la copia de seguridad**.

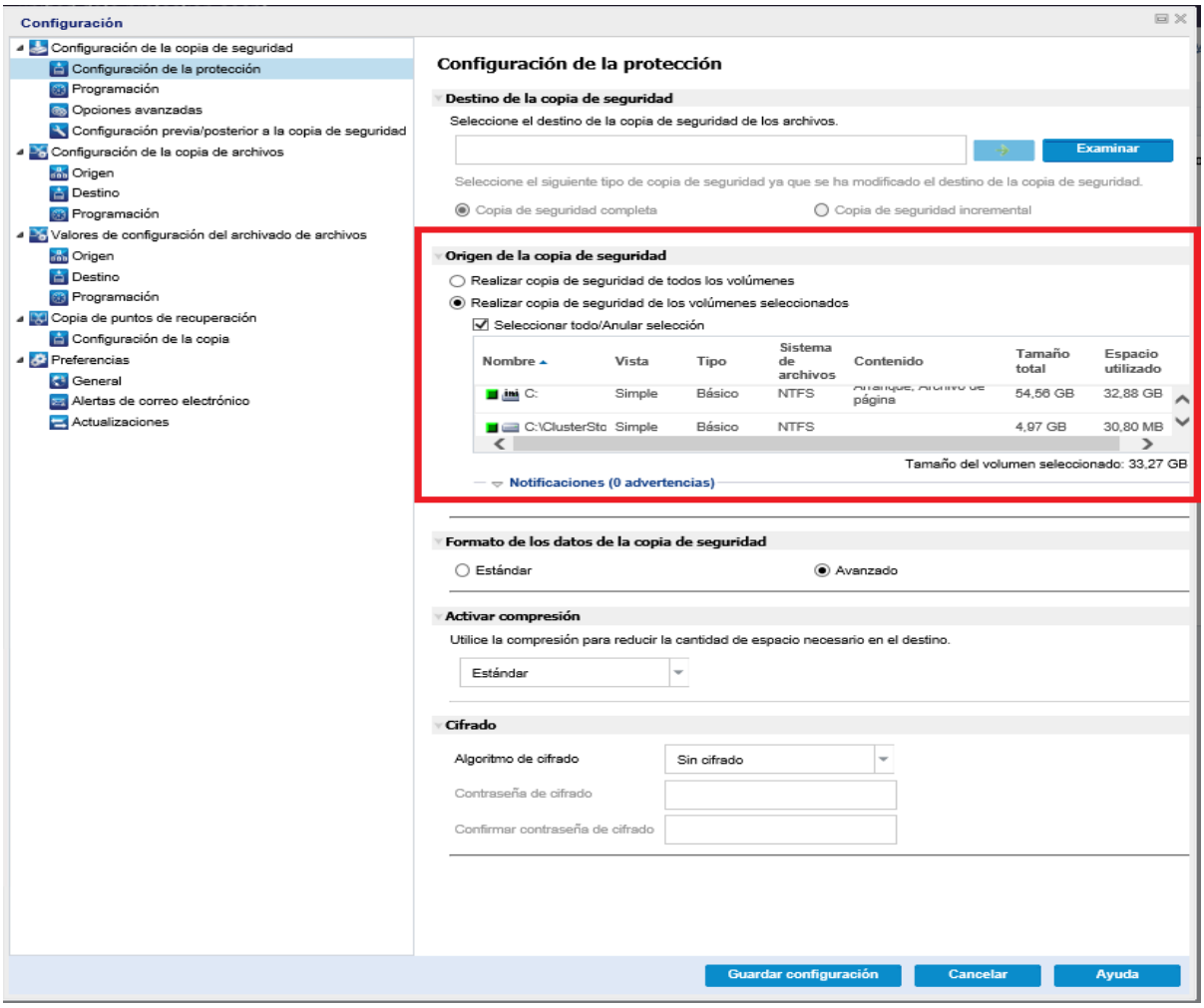
   Se abre la ventana Configuración de la copia de seguridad.

3. Haga clic en Configuración de la protección.

4. Se abre la ventana Configuración de la protección.

   Notas:

   - Cuando la Consola gestiona el Agente de Arcserve UDP (Windows), no todos los valores de configuración están disponibles y se muestran como información de solo lectura.
   - Cuando la Consola gestiona el Agente y no está protegido en un plan, todos los valores de configuración todavía estarán disponibles excepto el panel Preferencia > Actualizaciones.



5. En el grupo de **origen de la copia de seguridad**, seleccione **Copia de seguridad de los volúmenes seleccionados**.

   Aparecerá la lista de volúmenes disponibles en el equipo del agente.

6. Seleccione el volumen CSV del que se desea realizar la copia de seguridad y haga clic en **Guardar configuración**.

   La configuración de la protección de copia de seguridad se guardará.

Cómo realizar la copia de seguridad de volúmenes sin la letra de unidad

A partir de Arcserve UDP v6.5 Actualización 4, se pueden proteger los volúmenes sin letra de unidad utilizando la opción **Montado en los volúmenes de la carpeta NTFS** en **Realizar copia de seguridad de los volúmenes seleccionados**. Antes de seleccionar la opción **Montado en los volúmenes de la carpeta NTFS** en la Consola de Arcserve UDP, se debe montar el volumen de la carpeta NTFS. También puede realizar una personalización en más profundidad y solo realizar copias de seguridad

de algunos volúmenes sin letra de unidad en lugar de realizar la copia de seguridad de todos ellos.

Para obtener más información, consulte lo siguiente:

- Revisión de los requisitos previos
- Montaje del volumen sin letra de unidad en la carpeta NTFS
- Especificación del volumen sin letra de unidad en el registro

Revisión de los requisitos previos

Revise lo siguiente:

- Para que el almacén de datos esté el estado en ejecución en los reinicios del servidor de puntos de recuperación, active el montaje automático en el servidor de puntos de recuperación. Se puede activar el montaje automático utilizando el comando diskpart - automount.

  Siga estos pasos:

  1. Abra un símbolo del sistema con privilegios elevados.
  2. En el símbolo del sistema con privilegios elevados, haga lo siguiente:
  3. Escriba *diskpart* y, a continuación, pulse la tecla **Intro**.
  4. Escriba *automount enable* y pulse **Intro**.
  5. Cierre el símbolo del sistema con privilegios elevados.
  6. Para aplicar los cambios, reinicie el equipo.

Montaje del volumen sin letra de unidad en la carpeta NTFS

Se debe montar el volumen sin letra de unidad en la carpeta NTFS para realizar la copia de seguridad del volumen y del contenido del punto de montaje.

Siga estos pasos:

1. En **Administrador de discos de Windows**, seleccione el disco nuevo que no tiene una letra de unidad asignada.
2. Haga clic con el botón secundario del ratón y haga clic en **Cambiar la letra y rutas de acceso de unidad**.

   Se abre el cuadro de diálogo Agregar la letra y rutas de acceso de unidad.
3. Haga clic en **Cambiar**.

Se abre el diálogo Cambiar la letra y rutas de acceso de unidad.

4. Seleccione **Montar en la siguiente carpeta NTFS vacía**, especifique la ruta siguiente y haga clic en **Aceptar**.

   C:\MountPoint

   Aparecerá el punto de montaje en el Explorador de Windows. Se ha montado correctamente el volumen sin letra de unidad

Especificación del volumen sin letra de unidad en el registro

Se debe especificar el volumen sin letra de unidad en el registro para proteger el volumen y el contenido del punto de montaje.

Siga estos pasos:

1. En **Administrador de discos de Windows**, seleccione el disco nuevo que no tiene una letra de unidad asignada.
2. Haga clic con el botón secundario del ratón y haga clic en **Propiedades**.

   Se abrirá la ventana de propiedades del disco.
3. En la ficha **Seguridad**, copie el **Nombre de objeto**.
4. En la máquina del **Agente de Windows**, vaya a su respectivo **Nodo del agente** y abra el **Registro**.

   Se abre la ventana del registro.
5. Vaya a la siguiente ruta y haga clic en **BackupVolumesWIthMountedVolumes**.

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Aparecerá el cuadro de diálogo Modificar cadenas múltiples.
6. En el campo **Información del valor**, agregue el nombre del objeto que se ha copiado.
7. Haga clic en **Aceptar**.

   El volumen sin letra de unidad se especifica en el registro.

   Cuando se realiza la copia de seguridad desde la Consola de Arcserve UDP, solo se consideran los volúmenes especificados en el registro para la copia de seguridad.

Cómo realizar la copia de seguridad del volumen seleccionado

Este tema describe cómo realizar la copia de seguridad solo de los volúmenes seleccionados en lugar de realizar la copia de seguridad completa. Para realizar la copia de seguridad de un volumen específico, debe seleccionar la casilla de verificación **Realizar copia de seguridad de los volúmenes seleccionados** de la opción Origen mientras se crea un plan.

Siga estos pasos:

1. Durante la creación o modificación de un plan, seleccione la ficha Origen.
2. Seleccione la casilla de verificación Realizar copia de seguridad de los volúmenes seleccionados como Tipo protegido.

   Aparecen varios campos para seleccionar la unidad y otras opciones relacionadas con el volumen.
3. Seleccione una o más unidades en la lista de unidades.
4. Seleccione una o más opciones en la siguiente lista de volúmenes:

   Volumen reservado del sistema

   Se refiere al volumen necesario para arrancar el sistema operativo. Seleccione la opción si desea realizar una reconstrucción completa para el nodo de copia de seguridad o si desea realizar la copia de seguridad para una unidad determinada.

   Volumen de recuperación

   Se refiere al volumen necesario para el entorno de recuperación de Windows. Seleccione la opción si desea realizar la copia de seguridad del volumen de recuperación.

   Volumen de arranque

   Se refiere al volumen necesario cuando se arranca el sistema operativo de Windows. Seleccione la opción si desea realizar una reconstrucción completa para el nodo de copia de seguridad o si desea realizar la copia de seguridad para una unidad determinada.

   Montado en los volúmenes de la carpeta NTFS

   Se refiere a la opción Montado en los volúmenes de la carpeta NTFS. Seleccione esta opción si puede realizar la copia de seguridad de los volúmenes sin letra de unidad. Antes de seleccionar la opción en el plan, debe montar el volumen de la carpeta NTFS. También puede realizar una

personalización en más profundidad y solo realizar copias de seguridad de algunos volúmenes sin letra de unidad en lugar de realizar la copia de seguridad de todos ellos. Para obtener más información, consulte Cómo realizar la copia de seguridad de volúmenes sin la letra de unidad

5. Introduzca los detalles en las otras fichas del plan y guarde el plan.

   Se ha especificado la unidad o volumen. Solo se realiza la copia de seguridad del volumen o unidad seleccionados cuando se ejecuta una tarea de copia de seguridad.

Cómo crear un plan de copia de seguridad en Linux

Para proteger los nodos de Linux, es necesario crear un plan. Un plan de copia de seguridad para los nodos de Linux está formado por una tarea de copia de seguridad. Esta tarea de copia de seguridad le permite especificar los nodos que se desean proteger, el destino de la copia de seguridad y la programación de la copia de seguridad. El destino de la copia de seguridad puede ser un destino local, una carpeta de recurso compartido remota o un almacén de datos de un servidor de puntos de recuperación.

El diagrama siguiente ilustra el proceso para proteger los nodos de Linux:



¿Qué hacer a continuación?

1. Revisión de las consideraciones y requisitos previos
2. Creación de un plan de copia de seguridad
3. (Opcional) Realización de una copia de seguridad manual
4. Verificación de la copia de seguridad.
5. Solución de problemas

Revisión de las consideraciones y requisitos previos

Complete los siguientes requisitos previos:

- Inicie sesión en la Consola.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Creación de un plan de copia de seguridad

Un plan de copia de seguridad incluye una tarea de copia de seguridad que realiza una copia de seguridad del nodo físico o virtual y almacena los datos en el destino especificado.

Siga estos pasos:

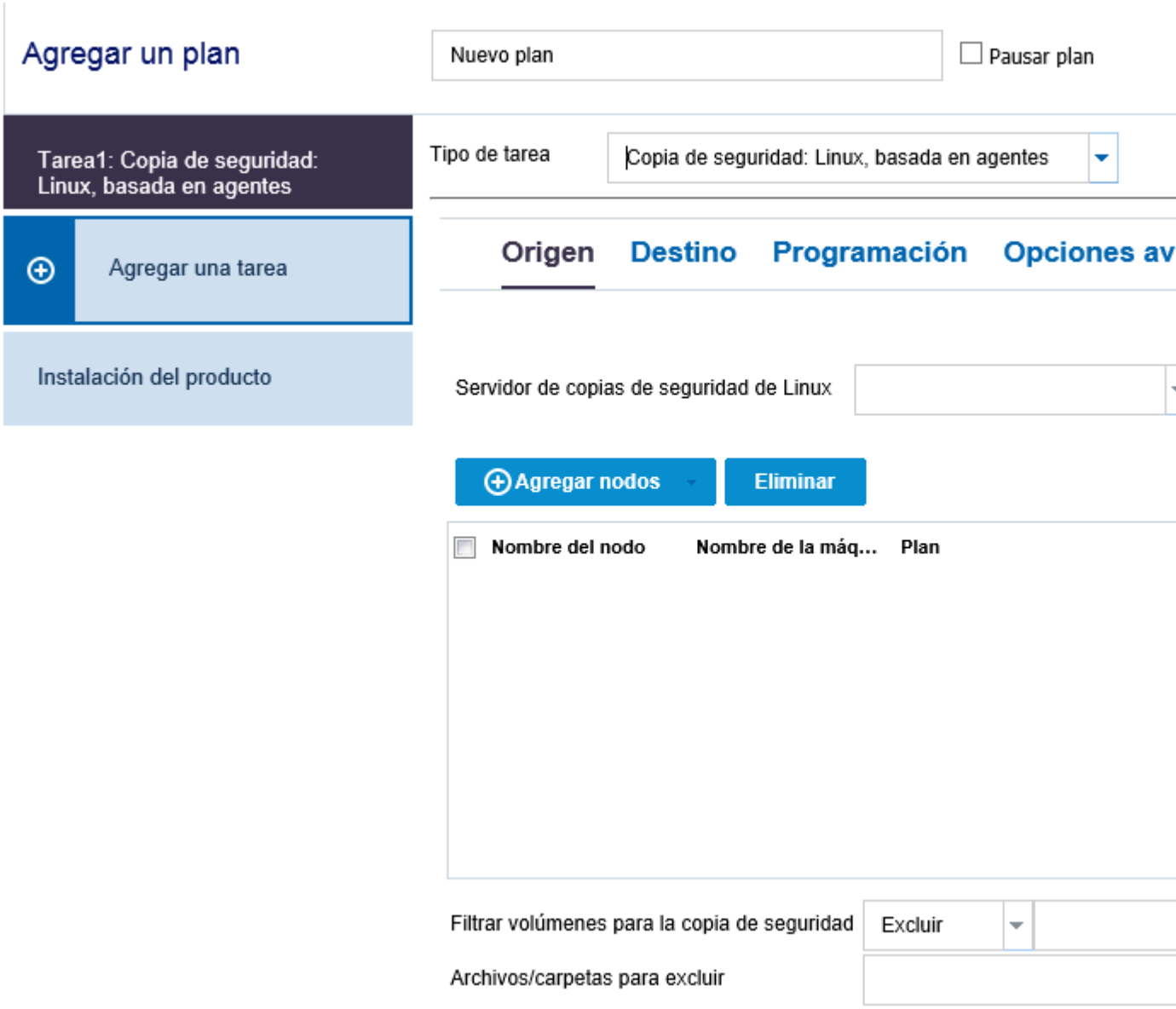
1. Inicie sesión en la Consola de Arcserve UDP.
2. Vaya a la ficha **recursos** > **Plan** > **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre la página Agregar un plan.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable Tipo de tarea seleccione **Copia de Seguridad: Linux, basada en el agente**.



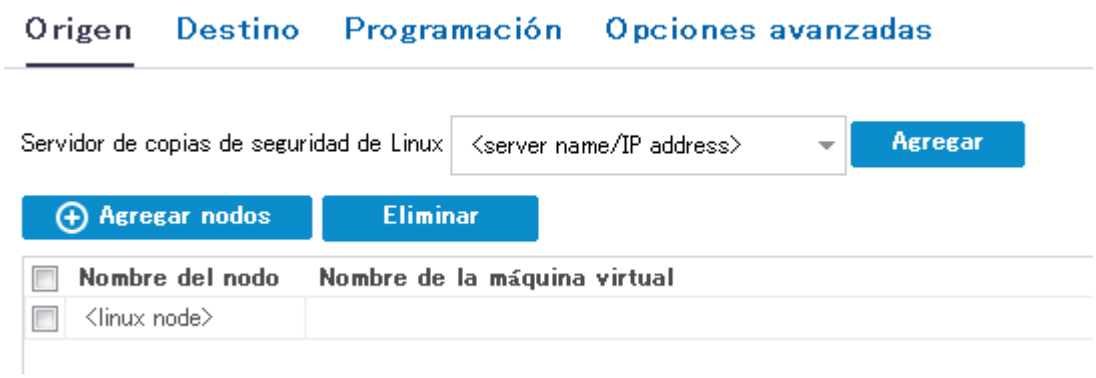
Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

La página Origen le permite especificar los nodos de origen que se desean proteger. Se pueden seleccionar más de un nodo del plan. Si no se han agregado nodos a la Consola, se pueden agregar nodos desde la página Origen. Se puede guardar un plan sin agregar nodos de origen pero el plan no se implementará a menos que se agreguen nodos.

Siga estos pasos:

1. Haga clic en la ficha Origen.
2. En la lista desplegable del servidor de copia de seguridad de Linux, seleccione el servidor de copia de seguridad de Linux.



3. (Opcional) Haga clic en **Agregar** para agregar un servidor de copia de seguridad de Linux nuevo a la lista.
4. Haga clic en **+ Agregar** y, a continuación, seleccione una de las opciones siguientes:

Seleccionar los nodos para proteger en Arcserve UDP

Se abre el cuadro de diálogo Seleccionar nodos para proteger. Seleccione los nodos de la lista que se muestra. Seleccione esta opción si ya se han agregado los nodos a la consola.

Agregar nodo de Linux

Se abre el cuadro de diálogo Agregar nodos de Linux a la Consola de Arcserve UDP. Seleccione esta opción si no se han agregado los nodos y desea agregarlos manualmente para la protección.

Si se selecciona, la copia de seguridad del nodo de Archivado de UDP la realiza el servidor de copia de seguridad de Linux instalado en el mismo nodo, incluso si se selecciona manualmente otro servidor de copia de seguridad de Linux. Para realizar la copia de seguridad del nodo mediante otro servidor de copia de seguridad de Linux, se puede agregar este nodo como nodo de Linux en lugar

de agregarlo como nodo de Archivado de UDP. Para obtener más información, consulte Cómo agregar nodos.

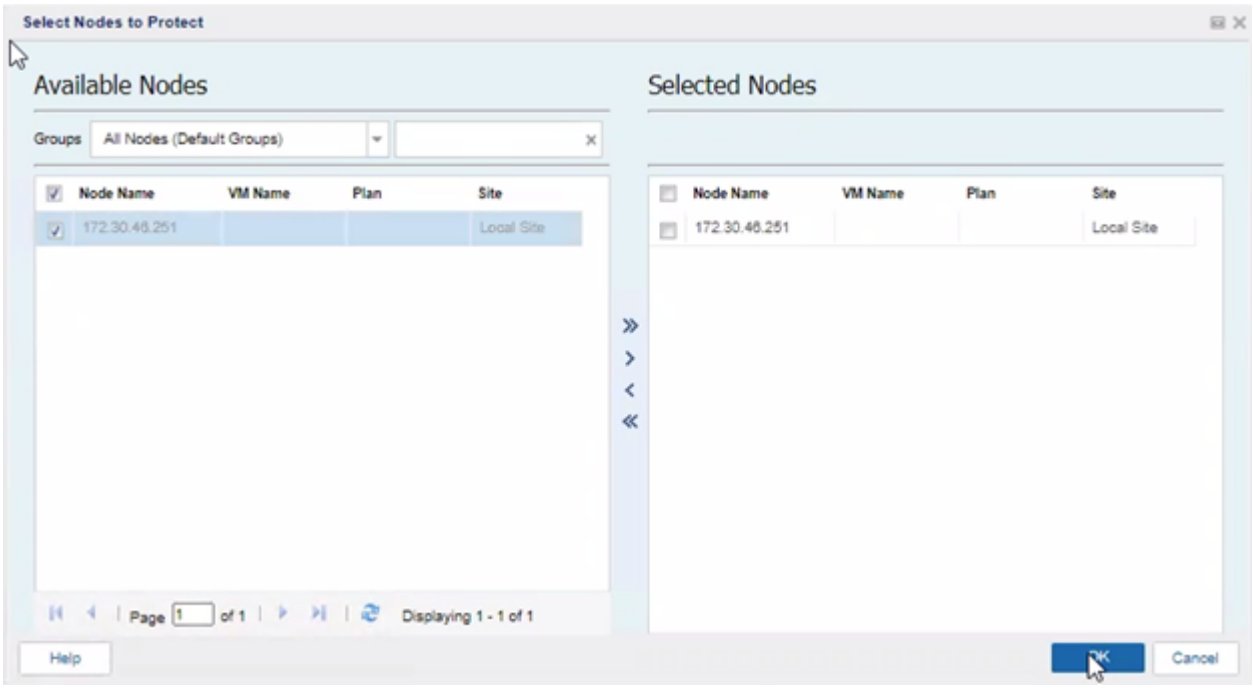
5. En el cuadro de diálogo Seleccionar nodos para proteger, haga lo siguiente:

   a. (Opcional) Seleccione un filtro en la lista desplegable Grupos para filtrar nodos. Se pueden especificar palabras clave para filtrar más detalladamente los nodos.

      Los nodos se muestran en la columna Nodos disponibles.

   b. Seleccione los nodos de la columna Nodos disponibles, haga clic en la flecha hacia la derecha y, a continuación, haga clic en **Aceptar**.

      Los nodos seleccionados se muestran en la columna Nodos seleccionados.



6. (Opcional) Proporcione los detalles para las opciones siguientes:

   Filtrado de los volúmenes para la copia de seguridad

   Seleccione **Incluir** o **Excluir** en la lista desplegable. Incluir especifica que solo se incluirán los volúmenes especificados para la copia de seguridad. No se realizará la copia de seguridad de cualquier volumen que no se haya especificado. Excluir especifica que los volúmenes se excluyen de la copia de seguridad.

   Archivos/carpetas para excluir

   Especifique los archivos y las carpetas de los que no desea realizar la copia de seguridad para todos los nodos listados. Si no se desea realizar la copia de seguridad de varios archivos y carpetas, separe cada archivo y carpeta mediante el

signo de los dos puntos (:). Proporcione la ruta completa del archivo y carpeta que se desea excluir.

7. Para Red de copia de seguridad designada, para seleccionar la red entre el servidor de copia de seguridad de Linux (LBS) y el nodo de Linux, haga clic en la casilla de verificación **Utilizar la red seleccionada para el tráfico de copia de seguridad** y, a continuación, seleccione la red en la lista desplegable.

   Nota: Si no se puede acceder a la red de copia de seguridad seleccionada y para continuar la tarea con la red disponible o con la red predeterminada, haga clic en la casilla de verificación **Continuar ejecutando la tarea incluso cuando no se pueda conectar con la red de copia de seguridad seleccionada**.

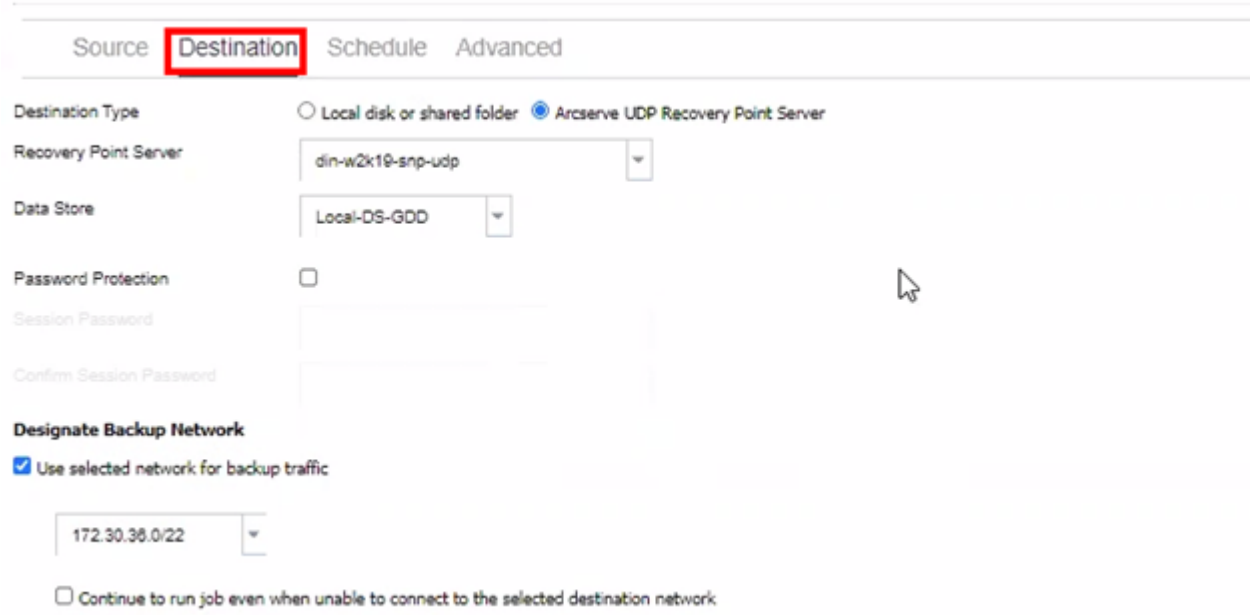
   Se especifica el origen.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Haga clic en la ficha **Destino**.



2. Seleccione uno de los siguientes tipos de destino:

   Disco local o carpeta compartida

   Especifica que los datos de copia de seguridad se almacenan en un disco local o en una carpeta compartida.

   Servidor de puntos de recuperación de Arcserve UDP

   Especifica que el destino de la copia de seguridad es un servidor de puntos de recuperación. Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.

3. Si se selecciona **Disco local o carpeta compartida** como Tipo de destino, proporcione los siguientes detalles:

   - Si se ha seleccionado **Recurso compartido de NFS**, escriba los detalles de Destino de la copia de seguridad en el formato siguiente:

     Dirección IP del uso compartido de NFS:/ruta completa de la ubicación de almacenamiento

- Haga clic en el botón de flecha para validar la información Destino de copia de seguridad.

  Si el destino de copia de seguridad no es válido, aparecerá un mensaje de error.

Nota: Algunas versiones del NAS de dominio de datos no son compatibles con el mecanismo de bloqueo del archivo de NFS. Como resultado, estos recursos compartidos de NFS no se pueden utilizar como destino de la copia de seguridad. Para obtener más información sobre este problema, consulte Problemas de compatibilidad con el Agente de Arcserve Unified Data Protection para Linux.

- Si se ha seleccionado **Recurso compartido de CIFS**, escriba los detalles de Destino de copia de seguridad en el formato siguiente:

  //hostname/share_folder

  - Haga clic en el botón de flecha para validar la información Destino de copia de seguridad.

    Si el destino de copia de seguridad no es válido, aparecerá un mensaje de error.

  Nota: Asegúrese de que el nombre de la carpeta compartida no tenga espacios.

- Si se ha seleccionado **Origen local**, siga estos pasos:

  a. Proporcione la ruta del destino local.

     Por ejemplo: /root

  b. Seleccione un nivel de compresión en la lista desplegable Compresión para especificar un tipo de compresión que se utiliza para la copia de seguridad.

     Las opciones disponibles para la Compresión son:

     Compresión estándar

     Especifica un nivel de compresión en la lista desplegable Compresión para especificar un tipo de compresión que se utiliza para la copia de seguridad.

     Compresión máxima

     Esta opción utiliza la mayor cantidad de CPU (velocidad más baja) pero también utiliza el menor espacio en disco para la imagen de copia de seguridad.

c. Seleccione un algoritmo en la lista desplegable Algoritmo de cifrado y escriba la contraseña de cifrado si es necesario.

d. Seleccione el tipo de algoritmo de cifrado que desea utilizar para las copias de seguridad.

El cifrado de datos es la traducción de los datos a una forma que resulte ininteligible sin un mecanismo de descifrado. La solución de protección de datos del Agente de Arcserve UDP (Linux) usa algoritmos seguros de cifrado AES (Estándar de cifrado avanzado) para lograr la mayor seguridad y privacidad de los datos especificados.

Para obtener las opciones de formato disponibles de cifrado, consulte Configuración de cifrado.

- Todas las copias de seguridad completas y sus copias de seguridad incrementales relacionadas deben utilizar el mismo algoritmo de cifrado.
- Si el algoritmo de cifrado para una copia de seguridad incremental ha cambiado, se deberá realizar una copia de seguridad completa.

Por ejemplo, si se cambia el formato del algoritmo y, a continuación, se ejecuta una copia de seguridad incremental, el tipo de copia de seguridad se convertirá automáticamente en una copia de seguridad completa.

e. Cuando se selecciona un algoritmo de cifrado, se debe proporcionar, y confirmar, la contraseña de cifrado.

- La contraseña de cifrado puede tener un máximo de 23 caracteres.
- Una copia de seguridad completa y todas las copias de seguridad incrementales y de verificación relacionadas deben utilizar la misma contraseña para cifrar los datos.

- Si desea realizar una copia de seguridad en Amazon S3, haga lo siguiente:

a. Seleccione **Recurso compartido de CIFS** y especifique el almacenamiento de Amazon S3 con el formato siguiente:

s3://S3 Region/S3 bucket name

b. Haga clic en la flecha y proporcione la información de acceso de Amazon S3.

4. Si selecciona **Servidor de puntos de recuperación de Arcserve UDP** como tipo de destino, haga lo siguiente:

- Servidor de puntos de recuperación: En la lista desplegable, seleccione el servidor de puntos de recuperación de destino.
- Almacén de datos: En la lista desplegable, seleccione el almacén de datos de destino.
- Protección con contraseña: Seleccione la casilla de verificación **Protección con contraseña**, proporcione la contraseña de la sesión y, a continuación, vuelva a especificarla para confirmarla.

  Nota: La contraseña de la sesión es opcional cuando el destino de copia de seguridad es un almacén de datos del servidor de puntos de recuperación no cifrado.
- Para Red de copia de seguridad designada, para seleccionar la red entre el servidor de copia de seguridad de Linux (LBS) y el servidor de puntos de recuperación, haga clic en la casilla de verificación **Utilizar la red seleccionada para el tráfico de copia de seguridad** y, a continuación, seleccione la red en la lista desplegable.

  Nota: Si no se puede acceder a la red de copia de seguridad seleccionada y para continuar la tarea con la red disponible o con la red predeterminada, haga clic en la casilla de verificación **Continuar ejecutando la tarea incluso cuando no se pueda conectar con la red de copia de seguridad seleccionada**.

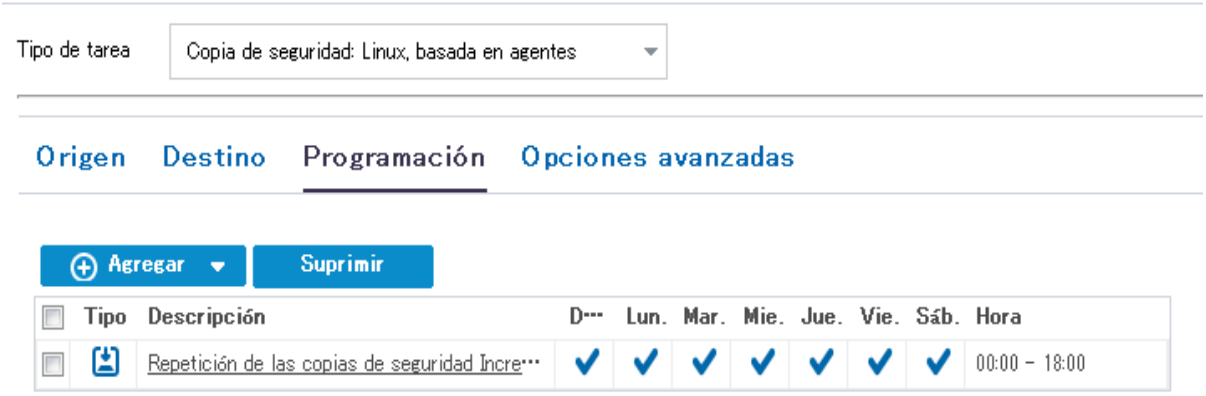
  Cuando el destino de la copia de seguridad es un almacén de datos de deduplicación, el tráfico se produce directamente entre el origen de Linux y el servidor de puntos de recuperación (RPS), incluso cuando la opción Especificar red esté configurada entre el origen de Linux y el servidor de copia de seguridad de Linux (LBS). Sin embargo, cuando el destino de la copia de seguridad es un almacén de datos de no deduplicación, el tráfico pasa por el servidor de copia de seguridad de Linux (LBS).

Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación de copia de seguridad para que se repita en intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y proporcionar valores de configuración de retención. Si el destino de la copia de seguridad es un disco local o una carpeta compartida, el valor predeterminado es una copia de seguridad incremental personalizada a las 22:00 horas. Si el destino de la copia de seguridad es un servidor de puntos de recuperación, el valor predeterminado es una copia de seguridad incremental diaria a las 22:00 horas.

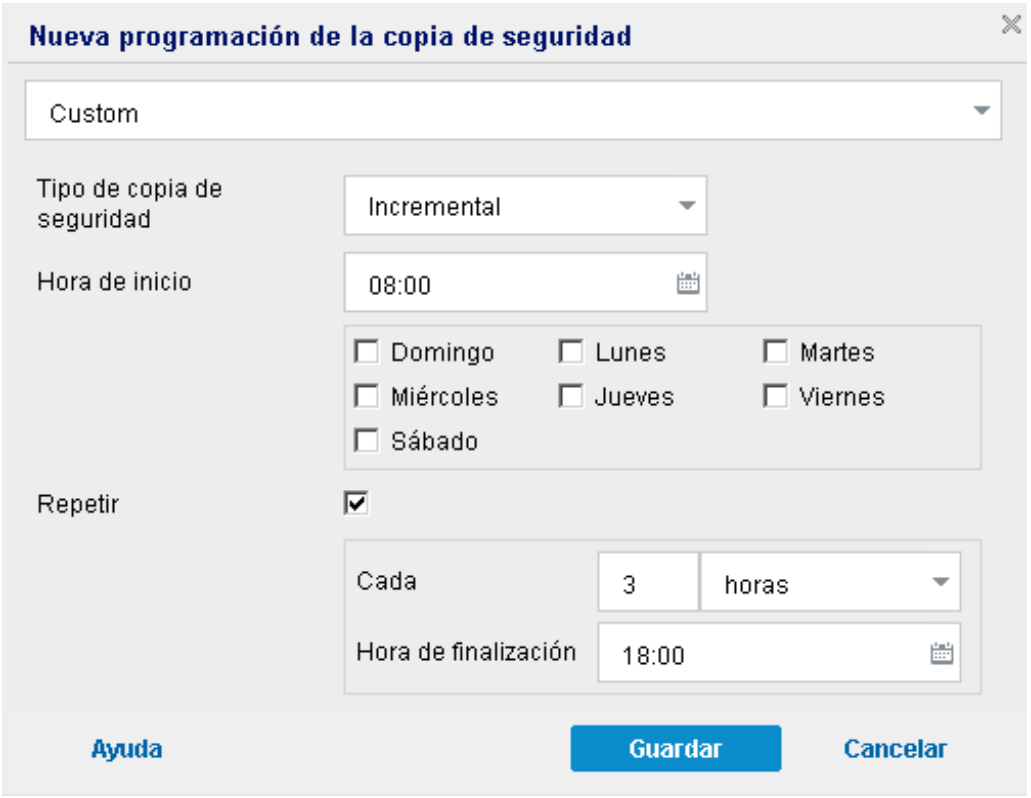
Se puede editar o suprimir una programación de la tarea de copia de seguridad.



Siga estos pasos:

1. Haga clic en la ficha **Programación**.
2. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

   Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



a. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

b. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Verificar

Especifica la programación de la copia de seguridad para las copias de seguridad de verificación.

Arcserve UDP verifica que los datos protegidos sean válidos y estén completos mediante una comprobación de confianza de la imagen de copia de seguridad almacenada en el origen de la copia de seguridad. Si es necesario, volverá a sincronizar la imagen. Una copia de seguridad de verificación se fijará en la copia de seguridad más reciente de cada bloque individual y comparará el contenido y la información con la de origen. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad de un bloque no coincide con la del origen (posiblemente por cambios en el sistema desde la última copia de seguridad), Arcserve UDP actualiza (resincroniza) la copia de seguridad del bloque que no coincide. Se puede utilizar también una copia de seguridad de verificación (aunque poco frecuentemente) para obtener la garantía de copia de seguridad completa sin utilizar el espacio necesario para una copia de seguridad completa.

Ventajas: produce una pequeña imagen de copia de seguridad si se compara con la copia de seguridad completa porque solamente se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventajas: el tiempo durante el cual se realiza la copia de seguridad es considerable puesto que todos los bloques de origen se comparan con los bloques de la última copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que

produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

c. Especifique la hora de inicio de la copia de seguridad.

d. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

e. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.

3. Si el destino es una carpeta compartida o de red, especifique los valores de configuración de la retención.

Nota: Para obtener más información acerca de los conjuntos de recuperación, consulte Funcionamiento de los conjuntos de recuperación.

Especifique el número de conjuntos de recuperación que deben retenerse.

Especifica el número de conjuntos de recuperación retenidos.

Inicie un nuevo conjunto de recuperación cada:

Día seleccionado de la semana

Especifica el día de la semana seleccionado para iniciar un nuevo conjunto de recuperación.

Cada día seleccionado del mes

Especifica el día del mes seleccionado para iniciar un nuevo conjunto de recuperación. Seleccione del 1 al 31, o bien el último día del mes.

Nota: El servidor de copia de seguridad de Linux comprueba cada 15 minutos el número de conjuntos de recuperación en el almacenamiento de la copia de seguridad configurado y suprime cualquier conjunto de recuperación adicional de la ubicación de almacenamiento de la copia de seguridad.

4. Si ha seleccionado Servidor de puntos de recuperación de Arcserve como destino, realice los pasos adicionales siguientes:

Adición de la programación de la combinación

a. Haga clic en **Agregar** y seleccione **Agregar programación de la combinación**.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

b. Especifique la hora de inicio para iniciar la tarea de combinación.

c. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

d. Haga clic en **Guardar**.

La Programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

Se abre el cuadro de diálogo Agregar nueva programación del limitador.

b. Especifique el límite de rendimiento en MB por minuto.

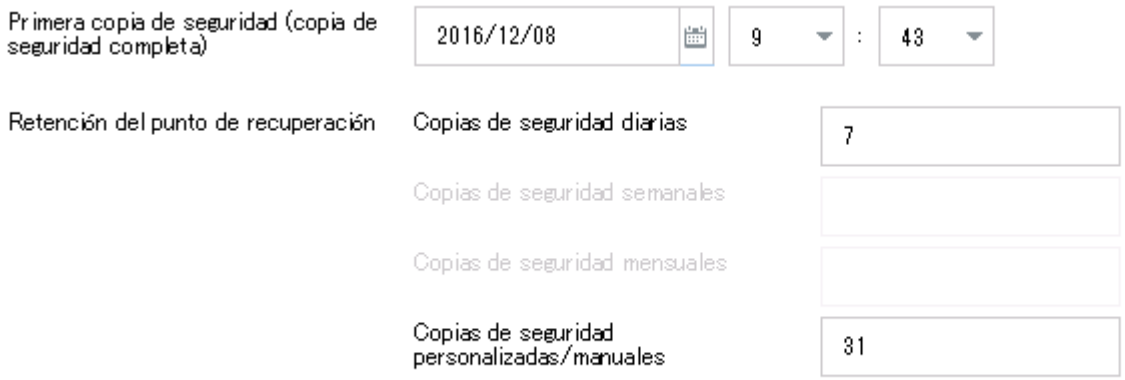
c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

La Programación del regulador se especifica y se muestra en la página **Programación**.

5. Especifique la hora de inicio para la copia de seguridad programada.



6. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo Programación de la copia de seguridad.

Se especifica la programación de la copia de seguridad.

Información general de los conjuntos de recuperación

Un conjunto de recuperación es una configuración de almacenamiento donde se realiza copia de seguridad de un grupo de puntos de recuperación y se almacena en un período especificado como un conjunto. Un conjunto de recuperación es una serie de copias de seguridad, empezando con una copia de seguridad completa y seguida, a continuación, por un número determinado de copias de seguridad incrementales, completas o de verificación. Especifique el número de conjuntos de recuperación que deben retenerse.

La configuración de los conjuntos de recuperación garantiza el mantenimiento periódico de los conjuntos de recuperación. Cuando el límite especificado se sobrepasa, el conjunto de recuperación más antiguo se suprimirá. Los siguientes valores definen los conjuntos de recuperación predeterminados, mínimos y máximos en el Agente de Arcserve Unified Data Protection para Linux:

Predeterminado: 2

Mínimo: 1

Número máximo de conjuntos de recuperación: 100

Nota: Si se desea suprimir un conjunto de recuperación para guardar espacio de almacenamiento de copia de seguridad, reduzca el número de conjuntos retenidos y el servidor de copia de seguridad suprimirá automáticamente el conjunto de recuperación más antiguo. No intente suprimir el conjunto de recuperación manualmente.

Conjunto de ejemplo 1:

- Completa
- Incremental
- Incremental
- Verificar
- Incremental

Conjunto de ejemplo 2:

- Completa
- Incremental
- Completa
- Incremental

Se requiere una copia de seguridad completa para iniciar un nuevo conjunto de recuperación. La copia de seguridad que inicia el conjunto se convertirá

automáticamente en una copia de seguridad completa, incluso si no hay ninguna copia de seguridad completa configurada o programada para que se lleve a cabo en ese momento. Después de cambiar la configuración del conjunto de recuperación (por ejemplo, cambiando el punto de partida del conjunto de recuperación de la primera copia de seguridad realizada el lunes a la primera copia de seguridad realizada el jueves), el punto de partida de los conjuntos de recuperación existentes no se cambiará.

Nota: No se cuenta ningún conjunto de recuperación incompleto al calcular un conjunto de recuperación existente. Un conjunto de recuperación se considera completo solamente cuando se crea la copia de seguridad inicial del siguiente conjunto de recuperación.

Ejemplo 1 - Retener 1 conjunto de recuperación:

- Especifique el valor del número de conjuntos de recuperación que deben retenerse como 1.

  El servidor de copia de seguridad siempre mantiene dos conjuntos para mantener un conjunto completo antes de iniciar el siguiente conjunto de recuperación.

Ejemplo 2 - Retener 2 conjuntos de recuperación:

- Especifique el valor del número de conjuntos de recuperación que deben retenerse como 2.

  El servidor de copia de seguridad suprime el primer conjunto de recuperación en el momento en que va a iniciarse el cuarto conjunto de recuperación. De esta manera se asegura que cuando la primera copia de seguridad se suprima y la cuarto se está iniciando, todavía habrá dos conjuntos de recuperación (el conjunto de recuperación 2 y el conjunto de recuperación 3) disponibles en disco.

  Nota: Aunque se seleccione el mantenimiento de un único conjunto de recuperación, se necesitará espacio para como mínimo dos copias de seguridad completas.

Ejemplo 3 - Retener 3 conjuntos de recuperación:

- La hora de inicio de la copia de seguridad es a las 06:00, 20 de agosto de 2012.
- Una copia de seguridad incremental se ejecuta cada 12 horas.
- Un conjunto de recuperación nuevo empieza el viernes. De forma predeterminada, la primera tarea de copia de seguridad del viernes será el inicio del nuevo conjunto de recuperación.

- Se desea retener 3 conjuntos de recuperación.

  Con la configuración anterior, se ejecutará una copia de seguridad incremental a las 06:00 y a las 18:00 cada día. El primer conjunto de recuperación se crea cuando se realiza la primera copia de seguridad (debe ser una copia de seguridad completa). A continuación, la primera copia de seguridad completa se marca como la copia de seguridad de partida del conjunto de recuperación. Cuando la copia de seguridad programada a las 6:00 del viernes se ejecuta, se convertirá en una copia de seguridad completa y se marcará como la copia de seguridad de partida del conjunto de recuperación.

  Nota: Si desea ejecutar la tarea de copia de seguridad reiteradamente hasta el final del día, configure la programación hasta las 12:00 horas. Por ejemplo, para ejecutar la tarea de copia de seguridad cada 15 minutos durante todo el día, configure la programación de las 12:00 a las 12:00, cada 15 minutos.

Especificación de la configuración avanzada

Utilizando la ficha Opciones avanzadas, especifique algunas opciones adicionales para la tarea de copia de seguridad, incluida la configuración de los scripts anteriores/posteriores y del rendimiento de la copia de seguridad.

Siga estos pasos:

1. Haga clic en la ficha **Opciones avanzadas**.
2. Especifique el valor de regulación de la copia de seguridad.

   Solo es aplicable cuando el destino de la copia de seguridad es un disco local o una carpeta compartida.

   Se puede especificar la velocidad máxima de escritura (MB/min) para las copias de seguridad. Es posible regular la velocidad de la copia de seguridad para reducir el uso de la CPU o de la red. Sin embargo, la limitación de la velocidad de las copias de seguridad puede tener efectos adversos en la ventana de copia de seguridad. A medida que se reduzca la velocidad máxima de la copia de seguridad, aumentará la cantidad de tiempo necesario para realizar la copia de seguridad.

   Nota: De forma predeterminada, la opción Regular copia de seguridad no aparece activada y no se controla la velocidad de la copia de seguridad.
3. Especifique los valores de configuración anteriores y posteriores a la realización de la copia de seguridad en **Configuración previa o posterior al script**.

   Estos scripts ejecutan comandos de script para realizar acciones antes del inicio de la tarea o cuando esta se finalice.

   Nota: Los campos de Configuración previa o posterior al script se rellenan solamente si ya se ha creado un archivo de script y se ha colocado en la siguiente ubicación del servidor de copia de seguridad de Linux:

   /opt/Arcserve/d2dserver/usr/prepost

   Nota: Para obtener más información acerca de cómo crear los scripts anteriores/posteriores, consulte *Gestión de scripts anteriores/posteriores para la automatización*.
4. Haga clic en Activar alertas de correo electrónico para especificar los valores de configuración del correo electrónico y seleccionar alertas de tarea.

   Solo es aplicable cuando el destino de la copia de seguridad es el servidor de puntos de recuperación de Arcserve.
5. Haga clic en **Guardar**.

   Se guardan los cambios.

El plan de copia de seguridad se crea y se implementa automáticamente en el nodo de origen. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

Ahora se pueden agregar las tareas siguientes al plan:

- Replicación
- Replicar a un servidor RPS remoto
- Copia en cinta

(Opcional) Gestión de scripts anteriores/posteriores para la automatización

Los scripts previos/posteriores permiten ejecutar su propia lógica empresarial en las etapas específicas de una tarea en ejecución. Se puede especificar cuando se ejecutan los scripts en **Configuración previa/posterior** de los scripts del **Asistente de copia de seguridad** y el **Asistente de restauración** en la consola. Los scripts se pueden ejecutar en el servidor de copia de seguridad en función de la configuración.

La gestión de scripts anteriores/posteriores constituye un proceso de dos partes que consta de la creación del script anterior/posterior y la colocación de dicho script en la carpeta prepost.

Creación de scripts anteriores/posteriores

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un archivo de script mediante el uso de las variables de entorno en el lenguaje de generación de scripts preferido.

   Variables de entorno de scripts anteriores/posteriores

   Para crear un script, utilice las variables de entorno siguientes:

   D2D_JOBNAME

   Indica el nombre de la tarea.

   D2D_JOBID

   Identifica el ID de la tarea. El ID de la tarea es un número que se proporciona a la tarea cuando esta se ejecuta. Si se ejecuta la misma tarea de nuevo, obtendrá un nuevo número de tareas.

   D2D_TARGETNODE

   Identifica el nodo del cual se realiza copia de seguridad o que se restaura.

   D2D_JOBTYPE

   Identifica el tipo de tarea en ejecución. Los valores siguientes identifican la variable D2D_JOBTYPE:

   backup.full

   Identifica la tarea como copia de seguridad completa.

   backup.incremental

   Identifica la tarea como copia de seguridad incremental.

backup.verify

Identifica la tarea como copia de seguridad de verificación.

restore.bmr

Identifica la tarea como reconstrucción completa. Esta tarea es de restauración.

restore.file

Identifica la tarea como una restauración de nivel de archivo. Esta tarea es de restauración.

D2D_SESSIONLOCATION

Identifica la ubicación donde se almacenan los puntos de recuperación.

D2D_PREPOST_OUTPUT

Identifica un archivo temporal. El contenido de la primera línea del archivo temporal aparecerá en el registro de actividades.

D2D_JOBSTAGE

Indica la etapa de la tarea. Los valores siguientes identifican la variable D2D_JOBSTAGE:

pre-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad antes de que se inicie la tarea.

post-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad después de que se complete la tarea.

pre-job-target

Identifica el script que se ejecuta en el equipo de destino antes de que se inicie la tarea.

post-job-target

Identifica el script que se ejecuta en el equipo de destino después de que se complete la tarea.

pre-snapshot

Identifica el script que se ejecuta en el equipo de destino antes de capturar la instantánea.

post-snapshot

Identifica el script que se ejecuta en el equipo de destino después de capturar la instantánea.

D2D_TARGETVOLUME

Identifica el volumen del cual se realiza copia de seguridad durante una tarea de copia de seguridad. Esta variable es aplicable para los scripts de instantáneas previas y posteriores para una tarea de copia de seguridad.

D2D_JOBRESULT

Identifica el resultado para un script de tarea de publicación. Los valores siguientes identifican la variable D2D_JOBRESULT:

success

Identifica el resultado como correcto.

fail

Identifica el resultado como incorrecto.

D2DSVR_HOME

Identifica la carpeta donde se instala el servidor de copia de seguridad. Esta variable es aplicable para los scripts que se ejecutan en el servidor de copia de seguridad.

El script se crea.

Nota: En todos los scripts, un valor de retorno de cero indica que se ha realizado correctamente, mientras que un valor de retorno distinto a cero indica que se han producido errores.

Colocación del script en la carpeta prepost y verificación

Todos los scripts previos/posteriores para un servidor de copia de seguridad se gestionan centralmente desde la carpeta prepost en la ubicación siguiente:

/opt/Arcserve/d2dserver/usr/prepost

Siga estos pasos:

1. Coloque el archivo en la siguiente ubicación del servidor de copia de seguridad:

   /opt/Arcserve/d2dserver/usr/prepost

2. Proporcione los permisos de ejecución al archivo de script.
3. Inicie sesión en la interfaz web del Agente de Arcserve Unified Data Protection para Linux.
4. Abra el **Asistente de copia de seguridad** o el **Asistente de restauración** y vaya a la ficha **Configuración avanzada**.

5. Seleccione el archivo de script en la lista desplegable **Configuración de scripts anteriores/posteriores** y, a continuación, envíe la tarea.
6. Haga clic en **Registro de actividad** y verifique que el script se ejecute en la tarea de copia de seguridad especificada.

   El script se ejecuta.

   Los scripts anteriores/posteriores se crean correctamente y se colocan en la carpeta prepost.

(Opcional) Realización de una copia de seguridad manual

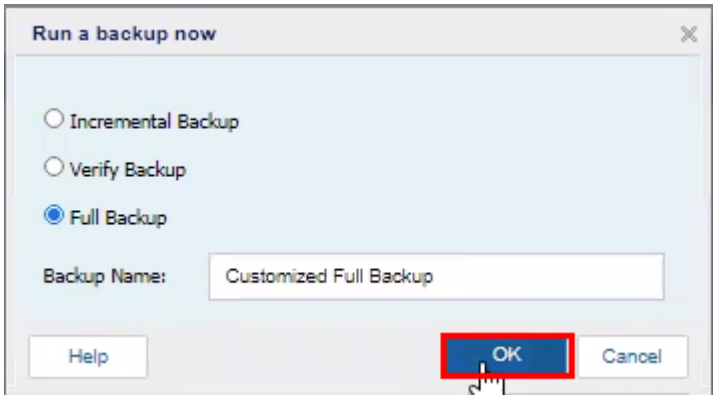
Normalmente se realizan copias de seguridad automáticamente y las controlan los valores de configuración de programación. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario. Por ejemplo, si tiene una programación de repetición para las copias de seguridad completas, incrementales y de resincronización y desea hacer cambios importantes en el equipo, se deberá realizar una copia de seguridad manual inmediata sin necesidad de esperar a la siguiente copia de seguridad programada.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Vaya a **recursos** > **Plan** > **Todos los planes**.

   La lista de todos los planes se muestra en el panel central.
3. Haga clic con el botón secundario del ratón en el plan y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
4. En el cuadro de diálogo Ejecutar una copia de seguridad ahora, seleccione el tipo de copia de seguridad que desea realizar y, a continuación, especifique el nombre de la copia de seguridad si es necesario.



A continuación se especifican las opciones disponibles:

Copia de seguridad incremental

Inicia una copia de seguridad incremental del equipo. Una copia de seguridad incremental sólo hará una copia de seguridad de los bloques que han cambiado desde la copia de seguridad anterior.

Nota: Si está realizando una copia de seguridad por primera vez, la copia de seguridad completa se iniciará automáticamente aunque haya seleccionado la opción Copia de seguridad incremental.

Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Ésta es la manera más óptima de realizar copias de seguridad.

Copia de seguridad de verificación

Inicia una copia de seguridad de verificación de su equipo examinando la copia de seguridad más reciente de cada bloque individual y comparando el contenido y la información con la original. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad para un bloque no coincide con la de origen, el Agente de Arcserve UDP (Windows) actualizará (resincronizará) la copia de seguridad del bloque que no coincida.

Ventaja: Una imagen de copia de seguridad muy pequeña se produce cuando se compara con una copia de seguridad completa porque solo se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventaja: El tiempo de copia de seguridad es lento porque todos los bloques del disco de origen se comparan con los bloques de la última copia de seguridad.

Copia de seguridad completa

Inicia una copia de seguridad completa del equipo o los volúmenes seleccionados.

Notas:

- Si se agrega un nuevo volumen al origen de la copia de seguridad, se realizará una copia de seguridad completa del nuevo volumen agregado, independientemente del método de copia de seguridad general seleccionado.
- Si no se especifica ningún nombre de copia de seguridad, de forma predeterminada se denominará Copia de seguridad completa/incremental/de verificación personalizada.

5. Haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.

6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.

7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   Nota: Solamente se puede restaurar una tarea cada vez. Si intenta iniciar una tarea de copia de seguridad manualmente cuando se está ejecutando otra tarea al mismo tiempo, aparecerá un mensaje de alerta para informar de que otra tarea está en ejecución y solicitará intentarlo de nuevo más tarde.

   La copia de seguridad manual se realiza correctamente.

Verificación de la copia de seguridad.

Para verificar la copia de seguridad, confirme que se ha creado correctamente el plan de copia de seguridad. Después de verificar que el plan se ha creado correctamente, confirme si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Se puede verificar el estado de las tareas de copia de seguridad en la ficha tareas.

Siga estos pasos: para verificar los planes.

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga uno de estos métodos para verificar las tareas de copia de seguridad

Método 1

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Método 2

1. En la Consola de Arcserve UDP, vaya a la ficha **tareas** > **Tareas finalizadas correctamente**.

   La lista de tareas de copia de seguridad completadas aparecerá en el panel central.
2. Haga clic en la tarea de replicación inversa finalizada. Se actualiza el panel derecho.
3. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
4. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Se verifica la tarea de copia de seguridad.

Solución de problemas

El estado de la tarea, el historial de tareas y el registro de actividades no son visibles

El estado de la tarea, el historial de tareas y el registro de actividades no son visibles

Síntoma

No puedo ver el estado de tarea, el historial de tareas y el registro de actividades para los nodos de Linux en la Consola de Arcserve UDP.

Solución

El servidor de copia de seguridad de Linux no se puede conectar a Arcserve UDP mediante el nombre de host.

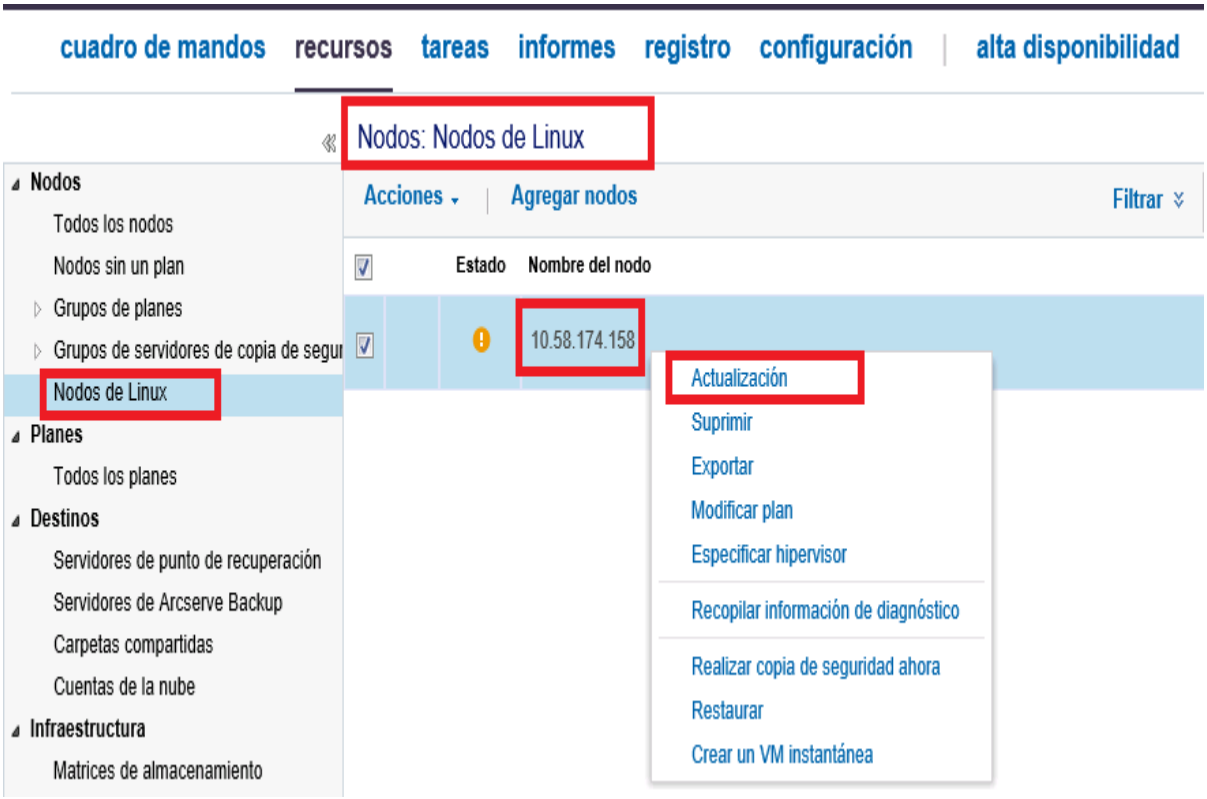
Siga estos pasos:

1. Cree el archivo server_ip.ini en la ubicación siguiente de Arcserve UDP:

   "Ruta de instalación de UDP"\Management\Configuration\server_ip.ini

2. Introduzca la dirección IP de Arcserve UDP en este archivo.
3. Inicie sesión en la Consola de Arcserve UDP y actualice el servidor de copia de seguridad de Linux y los nodos de Linux.

   Nota: El servidor de copia de seguridad de Linux solo se puede actualizar en Grupos del servidor de copia de seguridad de Linux, donde todos los servidores de copia de seguridad de Linux se clasifican.



El estado de la tarea, el historial de tareas y el registro de actividades son visibles

Cómo crear un plan de copia de seguridad de máquina virtual basada en el host

Para proteger los nodos de máquina virtual basados en el host, es necesario crear un plan de copia de seguridad basado en el host. Un plan de copia de seguridad para los nodos de máquina virtual basados en el host está formado por una tarea de copia de seguridad. La tarea de copia de seguridad le permite especificar los nodos que se desean proteger, el destino de la copia de seguridad y la programación de la copia de seguridad. El destino de la copia de seguridad puede ser un destino local, una carpeta de recurso compartido remota o el servidor de punto de recuperación donde se desean almacenar los datos de la copia de seguridad.

Se puede realizar también una copia de seguridad de las bases de datos de Oracle, SQL y los servidores de Exchange. Para realizar una copia de seguridad de las bases de datos de Oracle, asegúrese de que se cumplan los requisitos previos específicos. No hay requisitos previos para realizar la copia de seguridad de SQL Server y Exchange Server. Revise los requisitos previos siguientes para realizar una copia de seguridad coherente de la aplicación de una base de datos de Oracle:

- Requisito previo para crear una copia de seguridad coherente de la aplicación de una base de datos Oracle

El diagrama siguiente ilustra el proceso para proteger los nodos de máquina virtual basados en el host.



¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Creación de un plan de copia de seguridad basado en el host
3. (Opcional) Realización de una copia de seguridad manual
4. Verificación del plan
5. Solución de problemas

Revisión de las consideraciones y requisitos previos

Verifique si se han completado los requisitos previos siguientes:

- Inicie sesión en la Consola.
- Prepare un servidor proxy de copia de seguridad basado en host donde esté instalado el Agente de Arcserve Unified Data Protection para Windows.
- Para ejecutar funciones como la comprobación previa, los comandos previos y posteriores o las acciones de borrado definitivo del registro de aplicaciones, actualice la máquina virtual en la vista de la lista de nodos de la Consola de Arcserve UDP con una de las credenciales siguientes para la máquina virtual invitada:
  - Credenciales de usuario administrador integradas.
  - Credenciales de usuario administrador de dominio integradas.
  - Para el resto de credenciales de administrador, desactive el control de la cuenta de usuario (UAC) en la máquina virtual invitada.
- Para poder realizar una restauración de nivel de base de datos (en el caso de Exchange y SQL Server) o de nivel granular (Exchange) tras una copia de seguridad, se deben cumplir los siguientes requisitos previos:
  - La máquina virtual debe admitir la copia de seguridad coherente con la aplicación. Para obtener más información sobre la copia de seguridad coherente con la aplicación, consulte Cómo crear instantáneas coherentes con la aplicación para VMware o Cómo crear instantáneas coherentes con la aplicación para Hyper-V.
  - En el caso de las máquinas virtuales de VMware, se debe utilizar el método de desactivación de instantáneas **VMware Tools** en el plan de la copia de seguridad.
  - En lo que respecta a las máquinas virtuales de Hyper-V, Arcserve UDP debe implementar automáticamente una utilidad en el sistema operativo invitado de la máquina virtual para recopilar los metadatos de las aplicaciones durante la copia de seguridad. Se debe acceder al sistema operativo invitado de la máquina virtual desde el servidor proxy de copia de seguridad o el host de Hyper-V mediante una red. Al mismo tiempo, se debe actualizar el nodo de la máquina virtual con las credenciales administrativas adecuadas en la vista de la lista de nodos de la Consola de Arcserve UDP. Por algunos motivos, si no se puede acceder al sistema operativo invitado de la máquina virtual desde el servidor proxy de copia

de seguridad ni desde el host de Hyper-V, siga estos pasos para instalar manualmente la utilidad en el sistema operativo invitado de la máquina virtual:

a. Inicie sesión en el servidor de proxy de copia de seguridad y vaya a la siguiente carpeta:

   <Ruta de la instalación de Arcserve UDP>\Engine\BIN (por ejemplo, C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN).

b. Busque el archivo ejecutable **VMICService_32.exe** o **VMICService_64.exe**.

c. Copie el archivo ejecutable en cualquier carpeta situada dentro del sistema operativo invitado de la máquina virtual. (Para un sistema operativo de 32 bits, copie **VMICService_32.exe**, de lo contrario, copie **VMICService_64.exe**).

   Por ejemplo, puede crear una imagen ISO con este archivo ejecutable y montarla en la unidad DVD de la máquina virtual.

d. Inicie sesión en el sistema operativo invitado de la máquina virtual y ejecute **VMICService_32.exe -install** o **VMICService_64.exe -install**.

- Instale el componente del servidor y cree almacenes de datos si se desea almacenar los datos de la copia de seguridad en el servidor de punto de recuperación.
- Revise los requisitos previos para realizar una copia de seguridad de una base de datos de Oracle.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Los requisitos previos siguientes son para las instantáneas de hardware:

Para Hyper-V

- Instale un proveedor de hardware VSS en los servidores de Hyper-V y, para respaldar la instantánea transportable, instale el proveedor de hardware VSS en el servidor proxy de copia de seguridad. Una configuración habitual de un proveedor de hardware VSS incluye:
  - Especificación de un servidor que controle el LUN.
  - Especificación de las credenciales de la matriz de discos para acceder a la matriz de discos.

Para obtener más información sobre cómo configurar el proveedor de hardware VSS, póngase en contacto con el distribuidor del hardware.

- El servidor Hyper-V y el servidor proxy deben tener una versión del sistema operativo similar.
- Si el servidor Hyper-V pertenece a un clúster, el servidor proxy no debe formar parte del clúster de Hyper-V.
- Desinstale UDP CBT en Programas y características en el Panel de control del host de Hyper-V.

Para VMware

- Arcserve UDP es compatible con los LUN de NetApp iSCSI y NetApp NFS.
- Para crear una instantánea de hardware para VMware, agregue la matriz de almacenamiento a la Consola. Para obtener más información sobre cómo agregar una matriz de almacenamiento, consulte Agregar una matriz de almacenamiento.
- Para utilizar la instantánea de hardware, se requiere una licencia de FlexClone para las matrices de almacenamiento de NetApp que se ejecutan con Data ONTAP en 7-Mode y modo de clúster.

Consideraciones sobre la copia de seguridad de la máquina virtual:

- **Cómo puede afectar una desfragmentación del volumen a las copias de seguridad continuadas**

  La desfragmentación del volumen mediante la herramienta nativa de Windows afecta al tamaño de las copias de seguridad a nivel de bloque porque Arcserve UDP continúa realizando copias de seguridad incrementales de todos los bloques modificados. Esto significa que los bloques que se cambian durante la desfragmentación se incluyen en la copia de seguridad aunque no se haya cambiado ningún dato en los archivos. Como resultado, el tamaño de la copia de seguridad se incrementa. Este comportamiento es normal.

- **Cómo proteger las máquinas virtuales en Hyper-V 2016 utilizando el Seguimiento de cambios resistentes de Windows**

  Para proteger la máquina virtual de Hyper-V 2016, se recomienda aprovechar el Seguimiento de cambios resistentes (RCT) de Windows para la copia de seguridad incremental. Arcserve UDP utilizará automáticamente el Seguimiento de cambios resistentes (RCT) de Windows al realizar copias de seguridad de la máquina virtual con la versión 8.0 o posterior de la configuración que se ejecuta en el host o clúster de Hyper-V 2016. Si su instancia de Hyper-V se actualiza desde una versión anterior, actualice la configuración de la máquina virtual utilizando también la documentación de Microsoft. Cuando la actualización se

haya finalizado para todas las máquinas virtuales protegidas por Arcserve UDP, se recomienda desinstalar el servicio CBT de Arcserve UDP del host de Hyper-V.

Consideraciones para la copia de seguridad de red específica:

- El hipervisor, el servidor proxy de Windows y el servidor de puntos de recuperación deben estar en la misma red.
- Si ESXi se agrega con **Nombre de host** a vCenter, la selección de red de la copia de seguridad debe ser la red predeterminada de ESXi.

  Nota: La red predeterminada es la red resuelta por DNS.
- Si ESXi se agrega con la dirección IP a vCenter, la selección de red de la copia de seguridad debe ser la misma red que ESXi utiliza para conectarse a vCenter.

Escenario núm.	Tiene vCenter	Qué se utiliza para agregar a vCenter	¿Se puede usar la red de la copia de seguridad?	¿Funciona la solución alternativa del archivo DNS/Hosts?
1	No	N/D	Sí	N/D
2	Sí	Nombre de host de ESXi: se resuelve la dirección IP de producción del nombre de host	No	Sí. Actualice el archivo DNS o hosts en el servidor proxy.
3	Sí	Nombre de host de ESXi: se resuelve la dirección IP de red de la copia de seguridad del nombre de host	Sí	N/D
4	Sí	Dirección IP de producción de ESXi	No	No
5	Sí	Dirección IP de red de la copia de seguridad de ESXi	Sí	N/D

Revisión de los requisitos previos para realizar una copia de seguridad coherente de la aplicación para la base de datos de Oracle

Para realizar la copia de seguridad de una base de datos de Oracle con datos coherentes, se debe verificar que el modo ARCHIVELOG esté activado para permitir el archivado de los registros de rehacer.

Nota: El volumen de datos debe incluir archivos de datos de Oracle, archivos de control, archivos de parámetros del servidor y registros de rehacer en línea. Los registros de rehacer archivados deben estar ubicados físicamente en un volumen independiente.

Siga estos pasos para verificar si el modo ARCHIVELOG está activado:

a. Inicie sesión en el servidor de Oracle como usuario de Oracle con privilegios de SYSDBA.

b. En el símbolo del sistema SQL*Plus introduzca el siguiente comando:

   ARCHIVE LOG LIST;

   Aparecen los valores de configuración del registro de archivado para la instancia actual.

c. Defina la configuración siguiente:

   Modo de registro de la base de datos: modo de archivado

   Archivado automático: activado

d. Inicie el modo ARCHIVELOG.

   Nota: Si el modo ARCHIVELOG no está activado, inicie el modo ARCHIVELOG para hacer copias de seguridad de la base de datos.

Siga estos pasos para reiniciar el modo ARCHIVELOG:

a. Cierre Oracle Server.

b. Ejecute las siguientes instrucciones en Oracle:

   CONNECT SYS/SYS_PASSWORD AS SYSDBA

   STARTUP MOUNT;

   ALTER DATABASE ARCHIVELOG;

   ALTER DATABASE OPEN;

   De forma predeterminada, los registros de archivado se escriben en el área de recuperación de flash. Si no desea escribir registros de archivado en el área de

recuperación de flash, establezca el parámetro LOG_ARCHIVE_DEST_n en la ubicación donde se desea escribir los registros de archivado.

```
SQL>ALTER SYSTEM SET LOG_ARCHIVE_DEST_
1='LOCATION=e:\app\administrator\oradata\<nombre_base_datos_oracle>\arch'
SCOPE= BOTH;

System altered.

SQL> ARCHIVE LOG LIST;
```

Aparecen los valores de configuración del registro de archivado para la instancia actual.

c. Defina la configuración siguiente:

Modo de registro de la base de datos: modo de archivado

Archivado automático: activado

Destino del archivo de archivado: E:\app\oracle\oradata\<nombre_basededatos_oracle>\arch

Secuencia de registro en línea más antigua: 21

Secuencia de registro actual: 23

El servicio del editor de Oracle VSS se ha iniciado y funciona correctamente.

Creación de un plan de copia de seguridad basado en el host

Un plan de copia de seguridad incluye una tarea de copia de seguridad que realiza una copia de seguridad de la máquina virtual y almacena los datos en el destino especificado. Cada tarea está formada por parámetros que definen el origen, destino, programación y otros detalles de la copia de seguridad.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

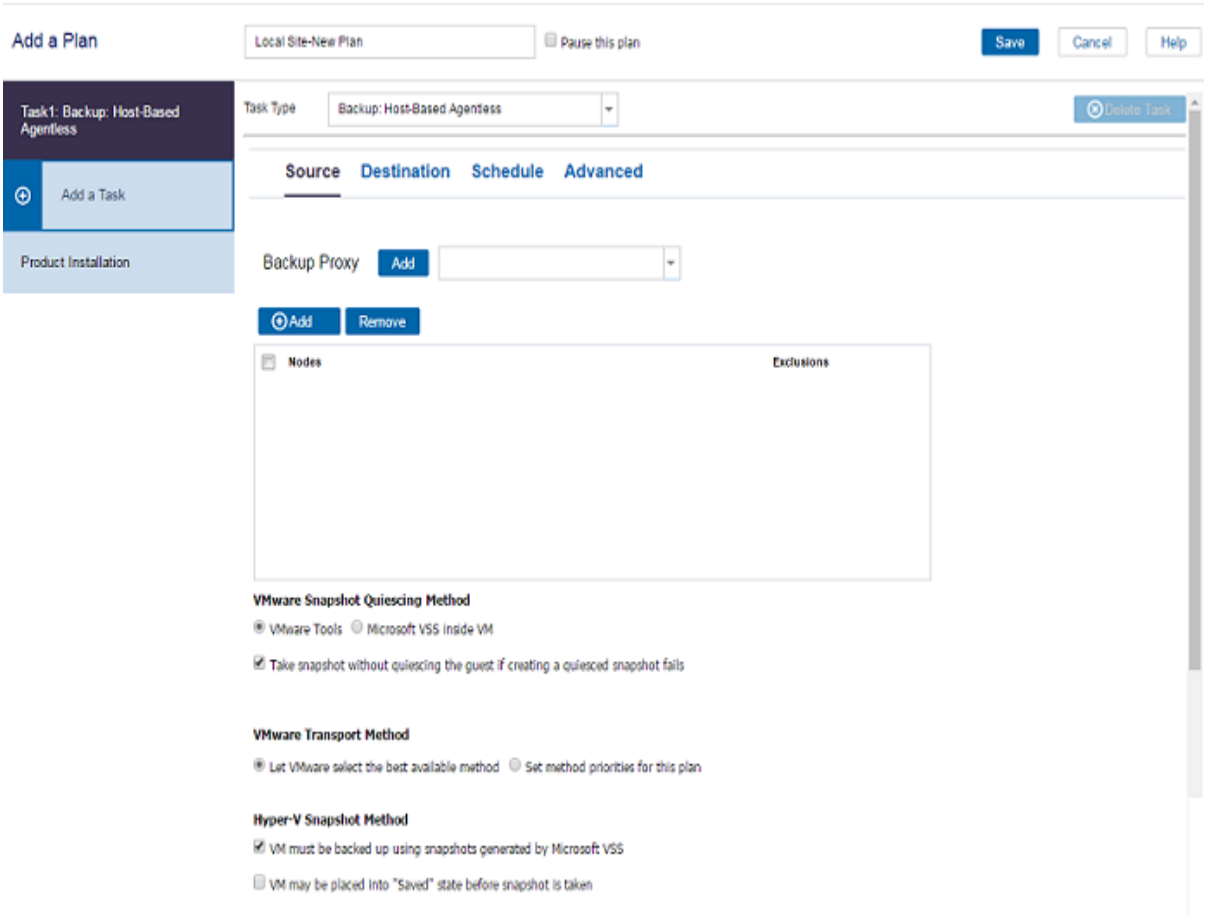
   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable **Tipo de tarea** seleccione **Copia de seguridad, sin agente y**

basada en el host.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

La página Origen le permite especificar los nodos de origen que se desean proteger. Se pueden seleccionar más de un nodo del plan. Si no se ha agregado ningún nodo a la consola, se podrán agregar nodos al crear o modificar un plan en la página Origen. Se puede guardar un plan sin agregar nodos de origen. El plan se implementa solamente después de agregar nodos de origen.

Siga estos pasos:

1. Haga clic en la ficha **Origen** y agregue un servidor proxy de copia de seguridad.

   El servidor proxy es un nodo donde se instala el Agente de Arcserve Unified Data Protection para Windows. Si el agente no está instalado en este servidor proxy, cuando se guarda el plan, el agente se implementa en el servidor proxy. La configuración de la implementación del agente está en la tarea Instalación del agente en el plan.

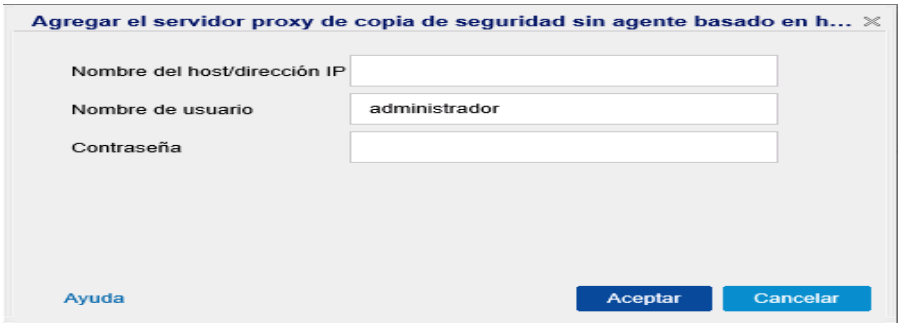
   - Si ha se ha agregado el proxy de copia de seguridad, selecciónelo en la lista desplegable.

   - Si no se ha agregado el proxy de copia de seguridad, haga clic en **Agregar**.

     Se abre el cuadro de diálogo **Agregar el servidor proxy de copia de seguridad sin agente basado en host**.

     Especifique los detalles del servidor proxy y haga clic en **Aceptar**.

   No se tiene que agregar el número de puerto ni el protocolo. Se configuran el número de puerto y el protocolo en la ficha **configuración** de la Consola.

   Nota: Cuando se modifica un plan cambiando el proxy de copia de seguridad, pero los nodos incluidos en dicho plan tienen tareas en ejecución, se produce un error en la implementación del plan. Siga estos pasos para cambiar el servidor proxy de un plan:

a. Pause el plan.

b. Espere hasta que todos los nodos del plan finalicen las tareas de copia de seguridad en ejecución. (O bien es posible cancelar las tareas en ejecución).

c. Cambie el proxy del plan y guárdelo.

d. Reanude el plan.

2. Haga clic en **Agregar nodos** para seleccionar una de las siguientes opciones para agregar los nodos a los que se desea realizar la copia de seguridad:

Selección de nodos para proteger

Aparece el cuadro de diálogo **Selección de nodos para proteger** y se pueden seleccionar los nodos en la lista que aparece. Seleccione esta opción si ya se han agregado los nodos a la consola.

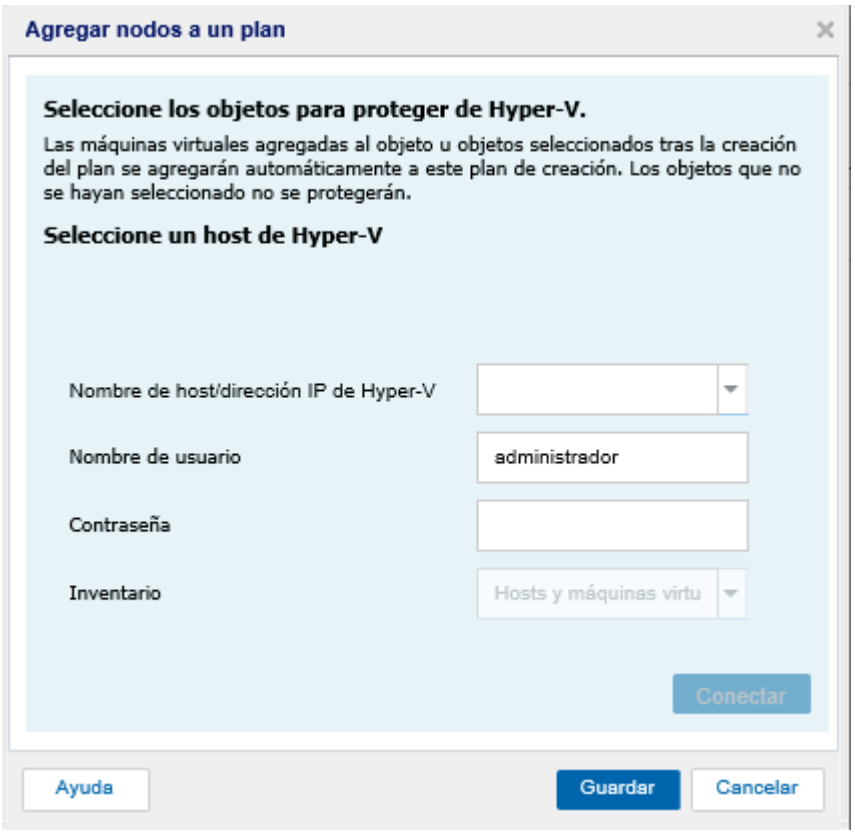
Adición de nodos desde Hyper-V

Se abre el cuadro de diálogo **Agregar nodos a la Consola de Arcserve UDP.** Se pueden agregar nodos de la máquina virtual individuales u objetos contenedores de la máquina virtual (incluido el clúster de Hyper-V, el host de Hyper-V y la ubicación de almacenamiento) a un plan. Una vez se haya agregado un objeto contenedor de la máquina virtual al plan, el plan protegerá automáticamente todas las máquinas virtuales asignadas. Cuando se crea una nueva máquina virtual en el objeto contenedor de la máquina virtual o cuando se mueve al objeto contenedor de la máquina virtual desde otro lugar, Arcserve UDP protege la máquina virtual sin intervención manual. Si la máquina virtual se suprime del objeto contenedor de la máquina virtual (o se saca del objeto contenedor de la máquina virtual) Arcserve UDP deja de proteger la máquina virtual.

Para agregar un objeto contenedor de la máquina virtual a un plan, siga estos pasos:

a. Especifique los detalles del servidor Hyper-V, seleccione cómo desea examinar las máquinas virtuales en el cuadro de la lista desplegable Inventario (Hosts y máquinas virtuales, Almacenamientos y máquinas virtuales) y haga clic en Conectar.

Se muestra un árbol de jerarquías de Hyper-V.

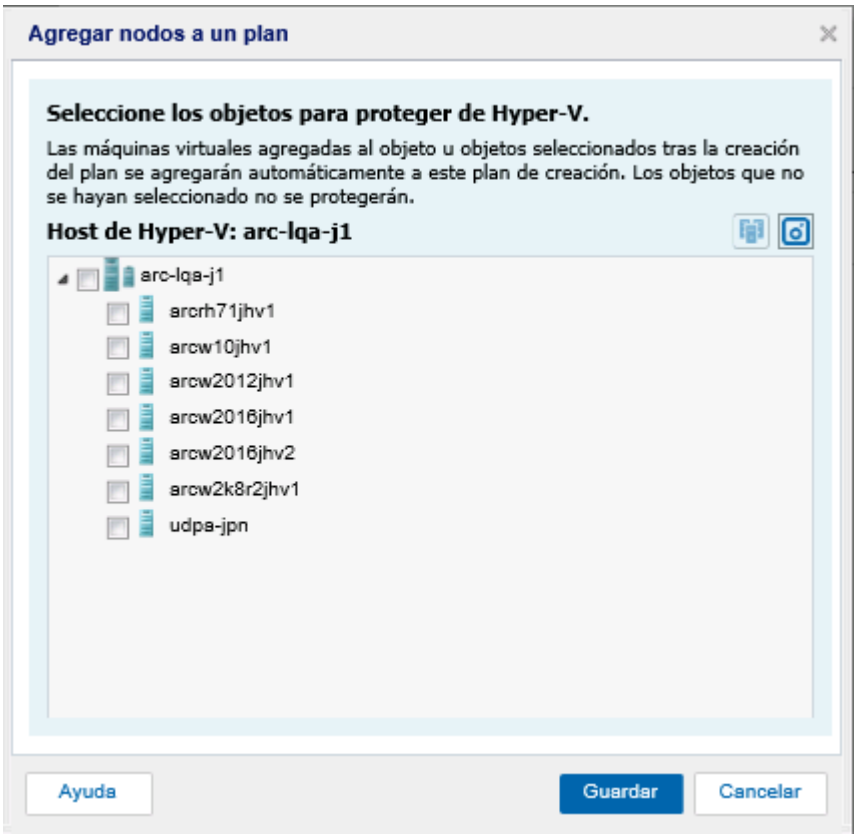


b. Expanda el árbol de jerarquías de Hyper-V para realizar las siguientes opciones:

Nota: Dependiendo de lo que está seleccionado en la lista desplegable Inventario, se mostrarán diferentes vistas del árbol de jerarquías: Hosts y máquinas virtuales o Almacenamientos y máquinas virtuales. Para cambiar entre las diferentes vistas del árbol, haga clic en los botones situados de la parte superior derecha del árbol.

i. **Adición de una máquina virtual Individual**

Seleccione en la lista la casilla de verificación de la máquina virtual que se desea agregar y haga clic en **Guardar**.



ii. **Adición de un objeto contenedor de la máquina virtual**

Seleccione en la lista la casilla de verificación del objeto contenedor de la máquina virtual que se desea agregar y haga clic en Guardar. Mientras se selecciona el objeto contenedor de la máquina virtual que se debe proteger, también se puede anular la selección de una máquina virtual secundaria o de un objeto contenedor secundario de la máquina virtual disponible debajo del objeto. Como resultado, la máquina virtual secundaria o el objeto contenedor secundario de la máquina virtual se excluirá de la protección.

Nota: Arcserve UDP utiliza el nombre de host o clúster de Hyper-V, el nombre de volumen o el nombre del recurso compartido de SMB para identificar de forma exclusiva el objeto contenedor en la lista de Hyper-V. Como resultado, se puede agregar más de una vez el mismo objeto contenedor de la máquina virtual a los planes.

Por ejemplo, agregue un host de Hyper-V mediante el nombre de host y, a continuación, agregue el mismo host de Hyper-V de nuevo utilizando la dirección IP. Otro ejemplo es agregar un recurso compartido de SMB, que utiliza el nombre de host del equipo host, y volver a agregar el mismo recurso compartido de SMB, que se utiliza la dirección IP del equipo host.

Importante: Arcserve UDP no admite la adición del mismo objeto contenedor a un plan dos veces para evitar comportamientos impredecibles.

Adición de nodos desde vCenter/ESX

Se abre el cuadro de diálogo **Agregar nodos a la Consola de Arcserve UDP.** Se pueden agregar nodos de máquinas virtuales individuales, plantillas de máquina virtual u objetos contenedor de la máquina virtual a un plan. Una vez se haya agregado un objeto contenedor de la máquina virtual al plan, el plan protegerá automáticamente todas las máquinas virtuales asignadas. Cuando se crea una nueva máquina virtual en el objeto contenedor de la máquina virtual o cuando se mueve al objeto contenedor de la máquina virtual desde otra ubicación, Arcserve UDP protege la máquina virtual sin intervención manual. Si la máquina virtual se suprime del objeto contenedor de la máquina virtual (o se saca del objeto contenedor de la máquina virtual) Arcserve UDP deja de proteger la máquina virtual.

Nota: Aparte de los objetos contenedores de la máquina virtual que existen en vSphere, Arcserve UDP también considera la etiqueta y la categoría de la etiqueta como objeto contenedor de la máquina virtual, por lo que se agregarán en el plan de copia de seguridad sin agente. En este caso, todas las máquinas virtuales y plantillas asignadas con esa etiqueta se protegen automáticamente. Además, si se asigna a un objeto contenedor de la máquina virtual de nivel superior una etiqueta, se considerará que todas las máquinas virtuales bajo ese objeto contenedor de la máquina virtual tienen prácticamente la misma etiqueta. Por ejemplo, la asignación automática de una etiqueta a una agrupación de recursos proporciona la misma etiqueta a las máquinas virtuales de esa agrupación cuando realmente no tienen ninguna etiqueta asignada en vCenter. Además, la protección automática por etiqueta solo se admite para vCenter 6.0 y 6.5.

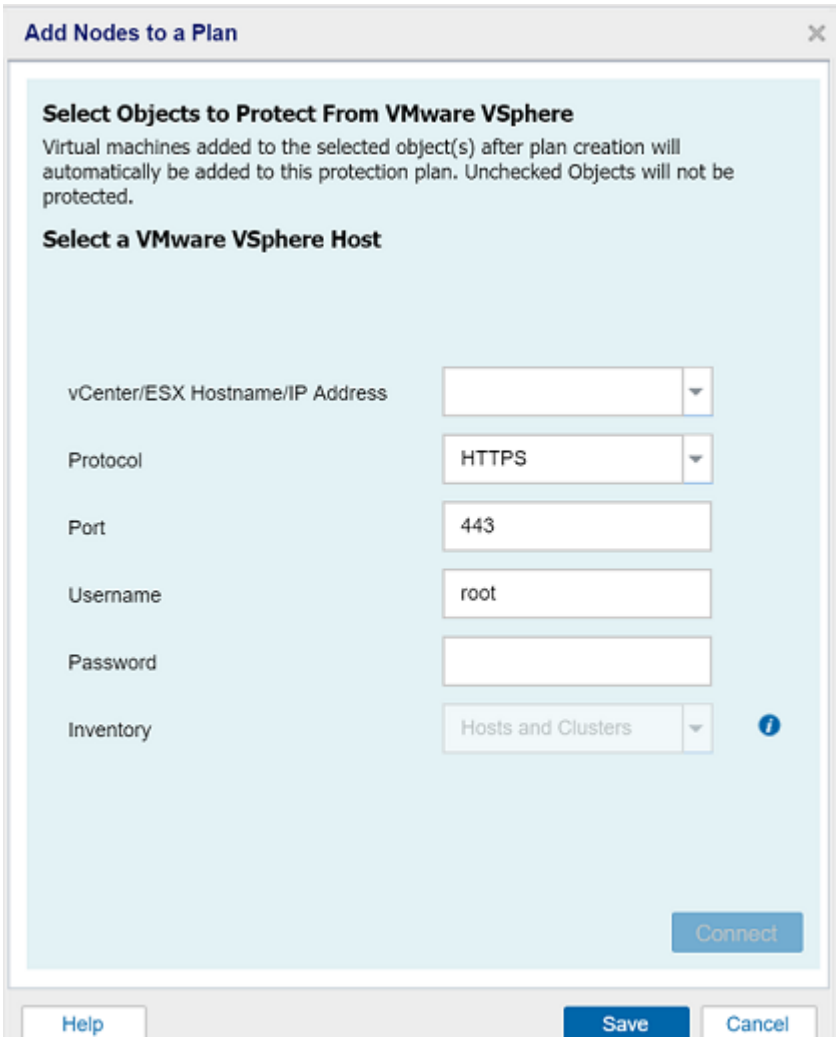
Para agregar un objeto contenedor de la máquina virtual a un plan, siga estos pasos:

a. Especifique los detalles del servidor de vCenter/ESX, seleccione cómo desea examinar las máquinas virtuales en el cuadro de diálogo de la lista desplegable Inventario (Hosts y clústeres, Máquinas virtuales y plantillas, Máquinas virtuales y etiquetas) y haga clic en **Conectar**.

   Se muestra un árbol de jerarquías de vSphere.

   Nota: Considere lo siguiente:

- VMware Virtual Disk Development Kit (VDDK) 6.x.x está incluido en el paquete de Arcserve UDP versión 7.0, pero VDDK 6.x.x no es compatible con HTTP. Además, vCenter y ESX son compatibles con la conexión HTTPS solo de forma predeterminada.
- Si desea reemplazar manualmente la versión integrada de VDDK 6.x.x por otra versión de VDDK y si desea configurar manualmente vCenter/ESX para que permita la conexión a HTTP, seleccione el **protocolo HTTPS**.

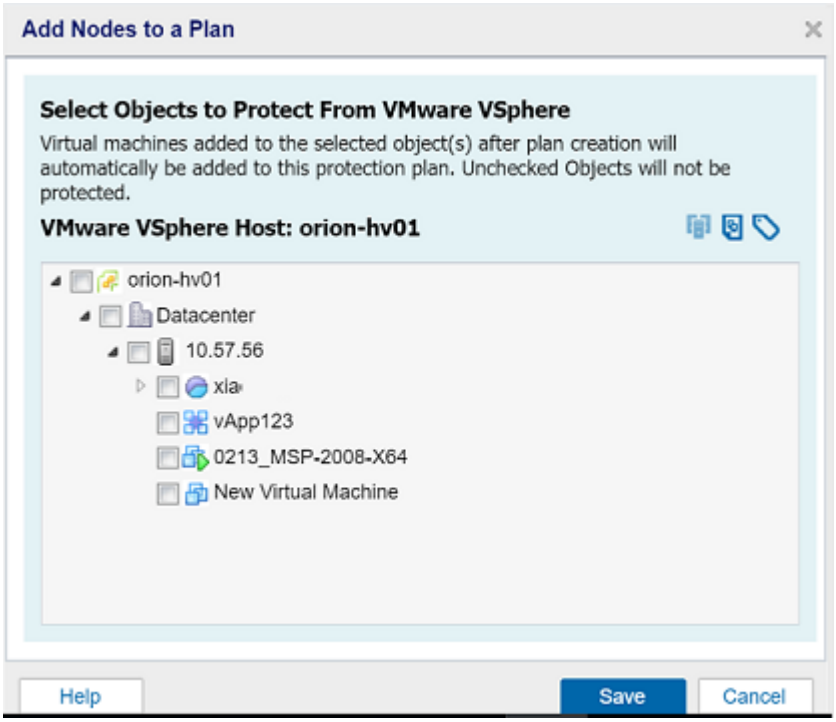


b. Expanda la lista de vSphere para agregar la siguiente:

Nota: Dependiendo de lo que está seleccionado en la lista desplegable Inventario, se mostrarán diferentes vistas del árbol de jerarquía: Hosts y clústeres, Máquinas virtuales y plantillas, y Máquinas virtuales y etiquetas. Se puede cambiar entre las diferentes vistas del árbol haciendo clic en los botones situados de la parte superior derecha del árbol.

i. **Adición de una máquina virtual individual**

Seleccione en la lista la casilla de verificación de la máquina virtual que se desea agregar y haga clic en **Guardar**.



ii. **Adición de un objeto contenedor de la máquina virtual**

Seleccione en la lista la casilla de verificación del contenedor que se desea agregar y haga clic en **Guardar**. Mientras se selecciona el contenedor que se debe proteger, también se puede anular la selección de una máquina virtual secundaria o de un objeto contenedor secundario de la máquina virtual que se encuentre debajo del mismo. Como resultado, la máquina virtual secundaria o el objeto contenedor secundario de la máquina virtual se excluirá de la protección.

Nota: Arcserve UDP utiliza vSphere MoRef ID (ID de referencia de objeto gestionado) y el nombre de vCenter/ESX para identificar de manera exclusiva el objeto contenedor de la máquina virtual en la lista **vSphere**. Esto permite agregar más de una vez el mismo objeto contenedor de la máquina virtual a los planes.

Por ejemplo:

a. Agregue un objeto contenedor de la máquina virtual a vCenter conectándose a vCenter mediante el nombre de host y, a continuación, agregue otra vez el mismo objeto

contenedor de la máquina virtual conectándose utilizando la dirección IP de vCenter.

b. Agregue un objeto contenedor de la máquina virtual a vCenter y, a continuación, vuelva a agregarlo desde el host de ESX directamente.

Importante: Arcserve UDP no admite la adición del mismo objeto contenedor de la máquina virtual a un plan dos veces, ya que se pueden producir comportamientos impredecibles.

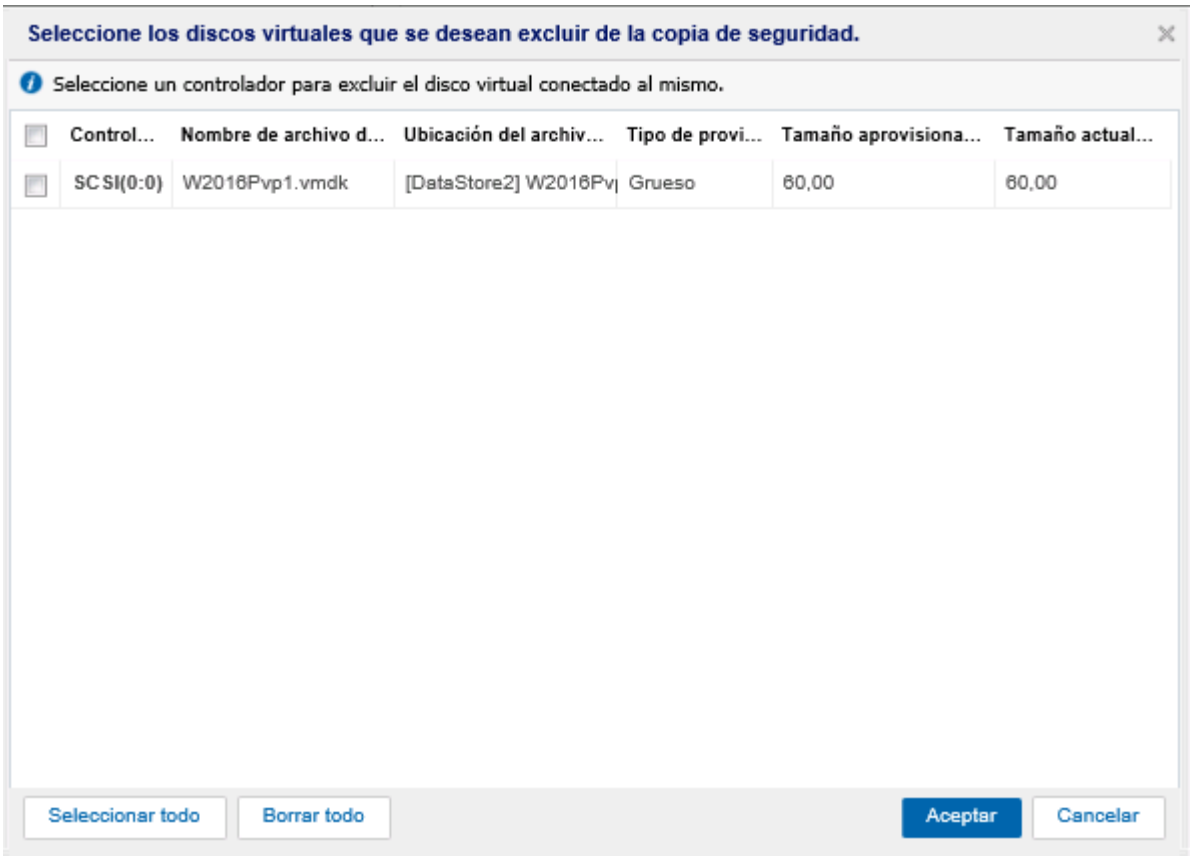
3. (Opcional) Seleccione el disco virtual que se puede excluir de la tarea de copia de seguridad.

   De forma predeterminada la tarea de copia de seguridad sin agente realiza copias de seguridad de toda la máquina virtual incluyendo todos los discos virtuales. Sin embargo, se puede especificar que uno o más discos virtuales se omitan durante la copia de seguridad.

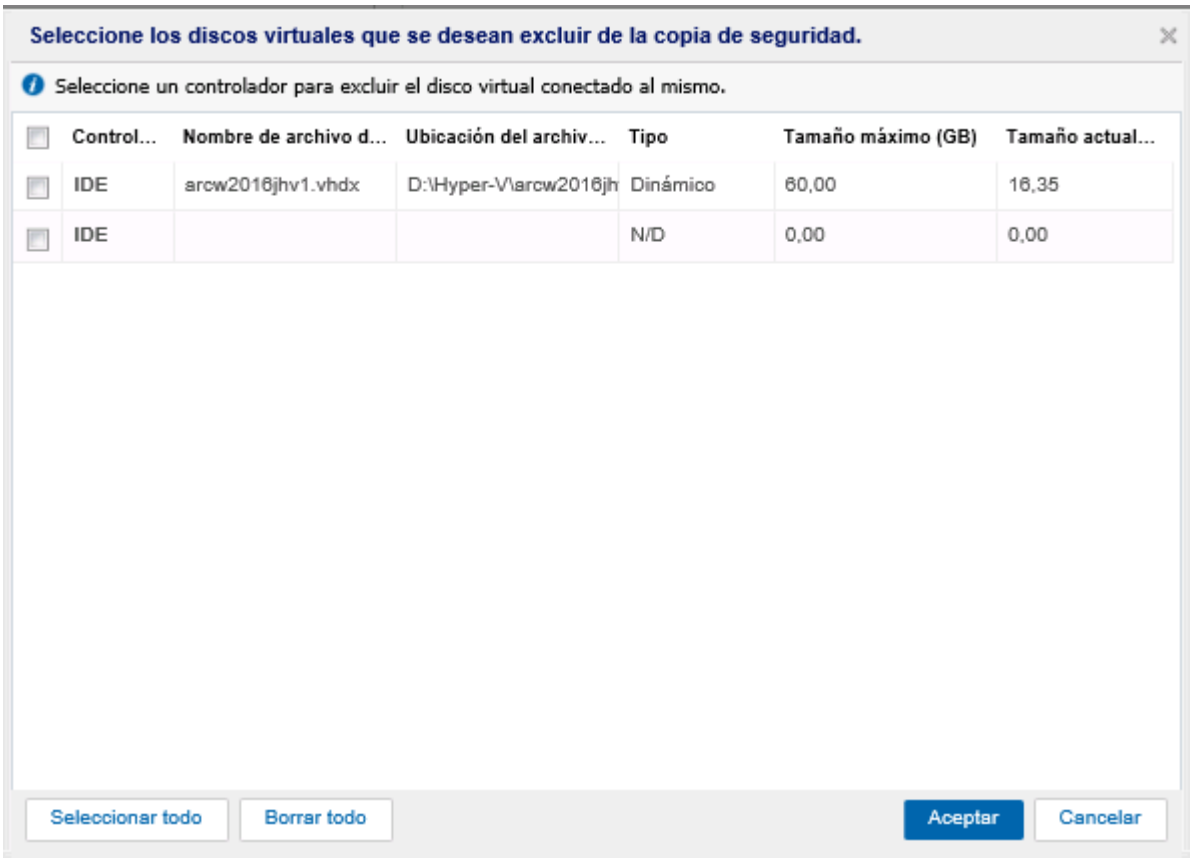
   a. Después de agregar un nodo de la máquina virtual al plan, haga clic en el botón Configurar que se encuentra disponible en el lado derecho del nodo.

      Aparece un cuadro de diálogo.

      Cuadro de diálogo para la máquina virtual de VMware



Cuadro de diálogo para la máquina virtual de Hyper-V



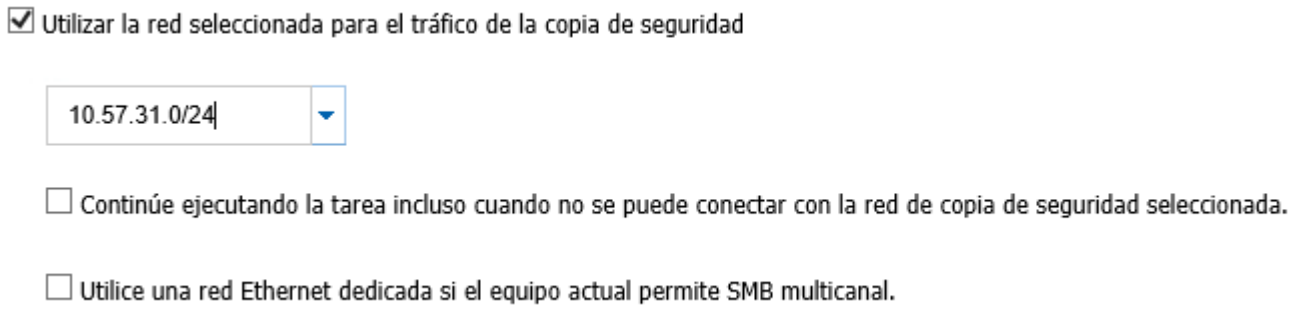
b. Seleccione la casilla de verificación del disco virtual que desea excluir de la copia de seguridad y haga clic en **Aceptar** para guardar.

Notas:

- El disco virtual se excluye por el controlador, en lugar de por el nombre del archivo del disco virtual.
- Si la copia de seguridad excluye el disco virtual que contiene el volumen del sistema del sistema operativo huésped, la máquina virtual restaurada no podrá iniciarse.
- Si la máquina virtual tiene una aplicación (SQL Server o Exchange) instalada y se excluye cualquier disco virtual mediante la copia de seguridad, no se permitirá realizar la restauración a nivel de la base de datos.

4. (Opcional) Seleccione la casilla de verificación **Usar red seleccionada para el tráfico de copia de seguridad** y siga estos pasos:

a. Para activar la comunicación entre el servidor proxy de Windows y el servidor del hipervisor, seleccione la red CIDR en el menú desplegable.



b. Si desea que la tarea de copia de seguridad continúe incluso si la red seleccionada no está disponible entre el servidor proxy y el hipervisor, active la casilla de verificación **Continuar ejecutando la tarea incluso cuando no se puede conectar con la red de copia de seguridad seleccionada**.

c. Para definir la restricción en la función SMB multicanal para que los datos se transfieran solo a través de la red seleccionada, seleccione la casilla de verificación **Utilizar una red Ethernet dedicada si el equipo actual permite SMB multicanal.**

Notas:

- Esta opción no se encuentra disponible de forma determinada. Para activar esta opción, vaya a la siguiente ubicación de la carpeta: C:\Archivos de programa\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. A continuación, modifique el valor de useDedicatedEthernet como True.

```
- <SpecifyNetwork>
    <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

- La función SMB multicanal está activada en Windows de forma predeterminada.

5. Especifique la configuración de red para la copia de seguridad de la máquina virtual de Hyper-V basada en el host:

Configuración del registro: SMBSpecifiedIONetwork

Ubicación: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll o HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\VMInstUUID

Tipo: Valor de cadena múltiple

Nombre del valor: SMBSpecifiedIONetwork

Datos del valor: Cadena con el formato CIDR (ip/maskBitCount)

Ejemplo: 192.168.10.0/24

Si los discos de la máquina virtual del clúster de Hyper-V/Hyper-V residen en el recurso compartido SMB, el usuario también puede definir otra red que se usará para la transferencia de datos entre el servidor SMB y la máquina proxy.

Nota: La asignación entre la dirección IP especificada y el nombre de host del servidor SMB debe registrarse en el dominio.

6. (Opcional) Seleccione uno de los métodos de desactivación para VMware. Estas opciones solo son aplicables para VMware.

   Herramientas de VMware

   Indica que Arcserve UDP utiliza las herramientas de VMware para desactivar la máquina virtual. Si se ha utilizado la opción **Microsoft VSS dentro de la máquina virtual** en la tarea de copia de seguridad anterior, la primera tarea de copia de seguridad posterior con esta opción requiere las credenciales para acceder a la máquina virtual. Esto es porque Arcserve UDP elimina las herramientas necesarias de la máquina virtual. Además, las herramientas de VMware se deben instalar y actualizar hasta la fecha en la máquina virtual.

   Microsoft VSS dentro de la máquina virtual

   Indica que Arcserve UDP utiliza Microsoft VSS en el sistema operativo invitado para desactivar la máquina virtual Solo es aplicable a las máquinas virtuales con sistemas operativos invitados de Windows. Las herramientas de VMware deben estar instaladas en el sistema operativo invitado y se deben actualizar. Cuando se utiliza esta opción, se debe encender la máquina virtual y se debe actualizar con las credenciales de administrador integradas. Para obtener más información sobre cómo actualizar un nodo, consulte Actualización de nodos.

   Nota: Puede que la instantánea que proporciona VMware mediante esta opción no sea coherente con la aplicación. Dicho de otro modo, la copia de seguridad generada con esta opción podría no ser una coherente con la aplicación. La solución alternativa consiste en utilizar el método de desactivación de instantánea VMware Tools, y desactivar los editores de VSS, como el *editor del servicio de Microsoft Search* y el *editor de optimización de instantáneas VSS* en el sistema operativo invitado de la máquina virtual para corregir el problema.

   Tomar la instantánea sin inactividad de invitado si se produce un error en la instantánea de inactividad

Indica que, cuando una tarea de copia de seguridad no realiza la instantánea con la opción de desactivación, Arcserve UDP continúa con la copia de seguridad tomando una instantánea sin desactivar la máquina virtual.

Notas:

- La opción **Microsoft VSS dentro de la máquina virtual** no es compatible con el nivel de la base de datos de la aplicación ni con el nivel granular de la restauración.
- Ambos métodos de desactivación no son aplicables cuando se apaga la máquina virtual. Si se inicia una tarea de copia de seguridad cuando la máquina virtual está apagada, la tarea de copia de seguridad ignorará ambos métodos de desactivación.
- En el caso de ambos métodos de desactivación, si la tarea de copia de seguridad no puede continuar por cualquier motivo (por ejemplo, las credenciales no son correctas), Arcserve UDP hace que se produzca un error en la tarea de copia de seguridad. Para obtener más información sobre el error de la tarea de copia de seguridad, consulte el tema Solución de problemas.

7. (Opcional) Seleccione uno de los métodos de transporte para VMware. Estas opciones son aplicables para VMware.

Permitir que VMware seleccione el mejor método disponible

Indica que VMware selecciona la opción de transferencia de datos. No debe establecer manualmente ninguna opción de transferencia de datos.

Establecer prioridades de método para este plan

Indica que puede seleccionar la opción de transferencia de datos y establecer una prioridad para cada opción. Use el botón de flecha para dar prioridad al modo de transporte.

- modo de transporte HOTADD
- modo de transporte NBD
- modo de transporte NBDSSL
- modo de transporte SAN

Nota: Si se ha especificado el modo de transporte tanto en la consola como en la clave de registro, la prioridad establecida en la Consola anula la prioridad establecida en la clave de registro. Para obtener más información sobre la configuración de la prioridad mediante la clave de registro, consulte Definición de un modo de transporte para la copia de seguridad sin agentes basada en host y para la restauración.

8. (Opcional) Seleccione el método de instantánea de Hyper-V. Estas opciones solo son aplicables para Hyper-V.

   Se debe realizar una copia de seguridad de la máquina virtual utilizando copias instantáneas generadas por el método de Microsoft VSS.

   Indica que Arcserve UDP utiliza los métodos de instantánea nativos de Microsoft, en línea y sin conexión, para la tarea de copia de seguridad. Se trata de la opción predeterminada. Cuando esta casilla de verificación no está seleccionada y, además, tanto el método en línea como el método sin conexión de Microsoft no están disponibles, la tarea de copia de seguridad utiliza el método de Arcserve UDP para realizar la copia de seguridad de la máquina virtual.

   Si se utiliza el método sin conexión de Microsoft para la copia de seguridad y la máquina virtual es necesaria para estar en el estado Guardado, seleccione también la casilla de verificación **Se puede colocar la máquina virtual en el estado Guardado antes de tomar la instantánea.** Si no se selecciona esta casilla de verificación, se producirá un error en la tarea de copia de seguridad.

   La copia de seguridad en línea es el método recomendado para la copia de seguridad porque es compatible con la copia de seguridad coherente con la aplicación sin el tiempo de inactividad de la máquina virtual. La máquina virtual es accesible durante la copia de seguridad. El método de copia de seguridad en línea debe satisfacer algunos requisitos previos como que los servicios de integración deban estar instalados y funcionando. Si alguno de los requisitos previos no se cumplen, solo se utilizará el método de copia de seguridad sin conexión.

   El método de copia de seguridad sin conexión de Microsoft tiene dos enfoques: el enfoque de guardar el estado y el enfoque del punto de control. Si el host de Hyper-V tiene el sistema operativo Windows 2012 R2 con KB 2919355 o posterior, se utiliza el enfoque del punto de control. En caso contrario, se utiliza el enfoque de guardar el estado.

   La principal diferencia entre estos dos enfoques es que el enfoque de guardar el estado requiere que no se pueda acceder a la máquina virtual durante un breve período. La máquina virtual debe colocarse en el estado Guardado durante unos minutos mientras se esté tomando la instantánea.

   Aparte de los métodos de instantánea nativos de Microsoft, Arcserve UDP tiene su propio método de instantánea, que se puede utilizar cuando los métodos de instantánea nativos de Microsoft no están disponibles.

Nota: Tanto el método sin conexión de Microsoft como el método de Arcserve UDP son métodos de copia de seguridad coherentes con los bloqueos. Ambos métodos no pueden garantizar la integridad de los datos. La principal diferencia entre los métodos es que el método sin conexión de Microsoft se puede comparar con el estado de cuando la máquina virtual se apaga abruptamente mientras que el método de Arcserve UDP se puede comparar con el estado de cuando el host de Hyper-V se apaga abruptamente.

La máquina virtual se puede colocar en el estado Guardado antes de tomar la instantánea.

Indica que la máquina virtual está colocada en el estado Guardado, si es necesario, antes de tomar la instantánea VSS. Seleccione esta opción cuando la máquina virtual no es compatible con la copia de seguridad en línea. Si la máquina virtual es compatible con la copia de seguridad en línea, entonces incluso en la activación de esta opción la máquina virtual no estará en el estado Guardado.

Se especifica el origen.

Definición de un modo de transporte en el registro para la restauración y copia de seguridad sin agente y basada en el host

Se puede definir un modo de transporte (transferir datos) para utilizar el Agente de UDP como un proxy que ejecuta la tarea de copia de seguridad o restauración sin agente basada en host para las máquinas virtuales que residen en el servidor ESX de VMware. De forma predeterminada, la copia de seguridad y la restauración sin agentes basada en el host utiliza un modo que permite a la copia de seguridad y la restauración sin agentes basada en el host optimizar el rendimiento (aumentar la velocidad) de la transferencia de datos. Sin embargo, si desea especificar un modo de transporte particular para la copia de seguridad o la restauración, se debe configurar la clave de registro que se describe en este tema.

Nota: Para la copia de seguridad, el modo de transporte definido en un plan prevalece sobre lo definido en el registro.

Host-Based VM Backup puede ejecutar copias de seguridad mediante los modos de transporte siguientes:

- modo de transporte HOTADD
- modo de transporte NBD
- modo de transporte NBDSSL
- modo de transporte SAN

Tenga en cuenta las consideraciones siguientes:

- Esta tarea se puede configurar opcionalmente. De forma predeterminada, Host-Based VM Backup ejecuta copias de seguridad mediante un modo de transporte que optimiza el rendimiento de la operación de copia de seguridad.
- Cuando se configura esta clave de registro para utilizar un modo de transporte específico y el modo no está disponible, la copia de seguridad de la máquina virtual basada en el host utiliza un modo de transporte predeterminado disponible para la operación de copia de seguridad.
- Se puede definir el modo de transporte para todas las máquinas virtuales que se utilizan para la copia de seguridad mediante el servidor proxy (a nivel de proxy) o definir una máquina virtual específica (a nivel de máquina virtual). Si se configura tanto el servidor proxy como la máquina virtual, el registro a nivel de máquina virtual toma precedencia sobre el registro a nivel de proxy.

Siga estos pasos para definir el modo de transporte a nivel del servidor proxy (aplicable tanto para la copia de seguridad como para la restauración):

1. Inicie sesión en el servidor proxy de la copia de seguridad del Agente de Arcserve Unified Data Protection para Windows.
2. Abra el editor del registro de Windows y desplácese hasta la siguiente clave:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine]
3. Haga clic con el botón secundario del ratón en VDDKEnforceTransport y haga clic en Modificar en el menú emergente para abrir el cuadro de diálogo de edición de la cadena.
4. En el campo de datos Valor, especifique el modo de transporte que se desea utilizar durante la tarea de copia de seguridad. Especifique uno o más de los valores siguientes separados por ":". (Por ejemplo, nbd o san:nbd:nbdssl:)

   hotadd

   modo de transporte HOTADD

   nbd

   modo de transporte NBD

   nbdssl

   modo de transporte NBDSSL

   san

   modo de transporte SAN
5. Haga clic en Aceptar para aplicar el valor y cerrar el cuadro de diálogo de edición de la cadena.

   El modo de transporte se define y se utiliza la próxima vez que se ejecuta una tarea.

   Nota: Para restaurar discos VMDK delgados, se utiliza de forma predeterminada el modo de transferencia no avanzada (modo de transporte de LAN). Para activar el modo de transporte avanzado para los discos de VMDK delgados, actualice la clave de registro tal y como se muestra en el ejemplo siguiente:

   a. Abra el editor del registro de Windows y desplácese hasta la siguiente clave:

      ```
      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine]
      ```

   b. Cree una clave llamada AFRestoreDll.

   c. Cree un valor de cadena llamado EnforceTransportForRecovery dentro de la clave AFRestoreDll.

   d. Especifique el modo de transporte que se desea utilizar durante la tarea de recuperación. (Por ejemplo: "san:nbd:nbdssl")

      Ejemplo

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFRestoreDll]

"EnforceTransportForRecovery"="san:hotadd:nbd:nbdssl"

Siga estos pasos para definir el modo de transporte a nivel de la máquina virtual (solo aplicable a la copia de seguridad):

1. Inicie sesión en el servidor proxy de la copia de seguridad del Agente de Arcserve Unified Data Protection para Windows para las máquinas virtuales.
2. Abra el editor del registro de Windows y desplácese hasta la siguiente clave:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\{VM-InstanceUUID}
3. Haga clic con el botón secundario del ratón en VM-InstanceUUID.sys y seleccione Nuevo.
4. Haga clic en Valor de cadena en el menú emergente.
5. Nombre el nuevo valor de cadena de la manera siguiente.

   EnforceTransport
6. Haga clic con el botón secundario del ratón en EnforceTransport y haga clic en Modificar en el menú emergente para abrir el cuadro de diálogo de edición de la cadena.
7. En el campo de datos Valor, especifique el modo de transporte que se desea utilizar durante la tarea de copia de seguridad. Indique uno de los siguientes valores

   hotadd

   modo de transporte HOTADD

   nbd

   modo de transporte NBD

   nbdssl

   modo de transporte NBDSSL

   san

   modo de transporte SAN
8. Haga clic en Aceptar para aplicar el valor y cerrar el cuadro de diálogo de edición de la cadena.

   El modo de transporte se define y se utiliza la próxima vez que se ejecuta una tarea.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Seleccione uno de los siguientes **Tipos de destino**:

   Disco local o carpeta compartida

   Especifica que el destino de la copia de seguridad es un destino local o una carpeta compartida. Si se selecciona esta opción, se pueden guardar datos como puntos de recuperación o como conjuntos de recuperación. Las opciones Puntos de recuperación y Conjuntos de recuperación están disponibles en la ficha **Programación**.

   Servidor de puntos de recuperación de Arcserve UDP

   Especifica que el destino de la copia de seguridad es un servidor de puntos de recuperación. Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.

2. Si se ha seleccionado **Servidor de puntos de recuperación de Arcserve UDP**, se deben proporcionar los detalles siguientes:

   a. Seleccione un servidor de puntos de recuperación.

   b. Seleccione un almacén de datos. La lista muestra todos los almacenes de datos que se han creado en el servidor de punto de recuperación especificado.

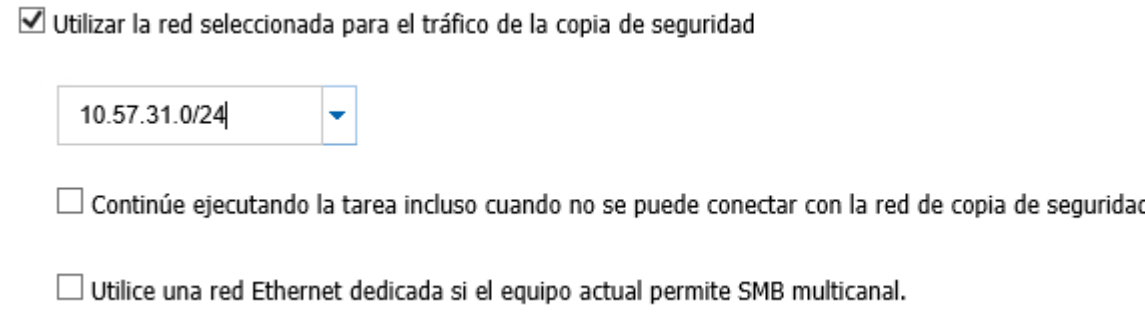
   c. Proporcione una contraseña de la sesión.

      Nota: La contraseña de la sesión es opcional cuando el destino de copia de seguridad es un almacén de datos del servidor de puntos de recuperación no cifrado.

   d. Confirme la contraseña de la sesión.

   e. (Opcional) Seleccione la casilla de verificación **Usar red seleccionada para el tráfico de copia de seguridad** y siga estos pasos:

      1. Para activar la comunicación entre el servidor proxy de Windows y el servidor de puntos de recuperación, seleccione la red CIDR en el menú desplegable.



2. Si desea que la tarea de copia de seguridad continúe incluso si la red seleccionada no está disponible entre el servidor proxy y el Servidor de puntos de recuperación, active la casilla de verificación **Continuar ejecutando la tarea incluso cuando no se puede conectar con la red de copia de seguridad seleccionada**.
3. Para desactivar la función SMB multicanal para que los datos se transfieran solo a través de la red seleccionada, seleccione la casilla de verificación **Utilizar una red Ethernet dedicada si el equipo actual permite SMB multicanal.**

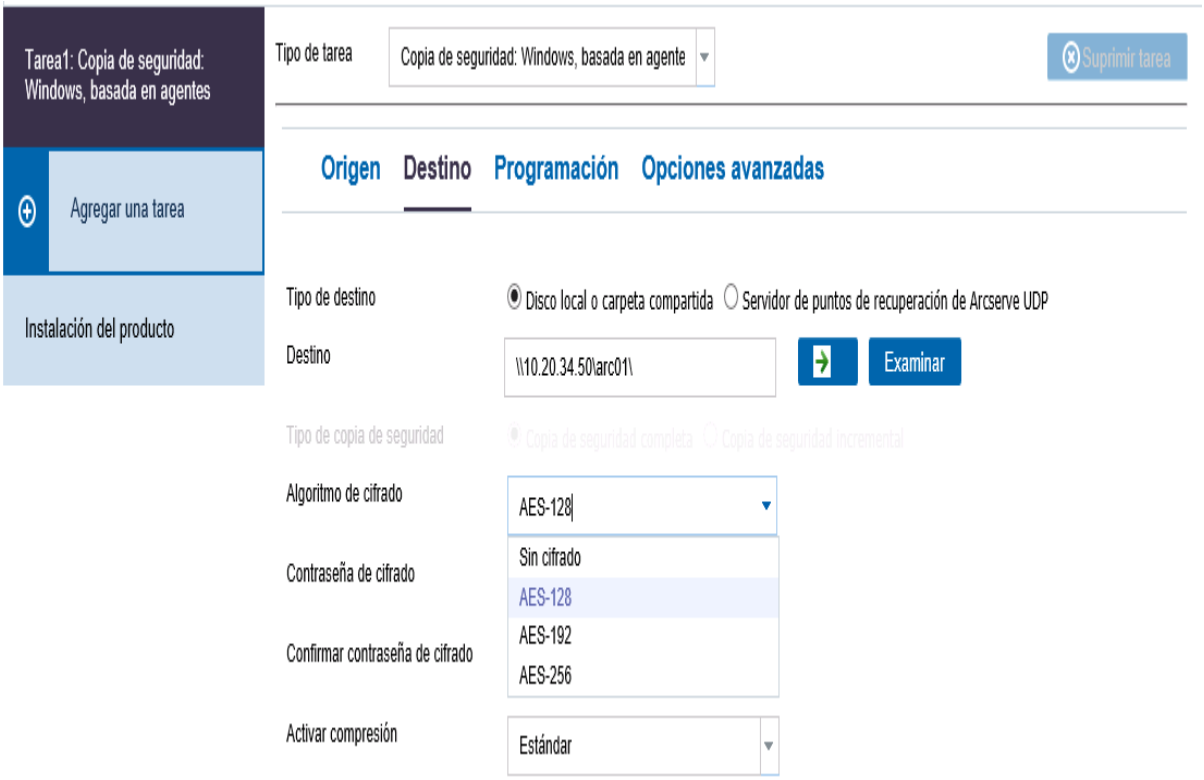
Notas:

- Esta opción no se encuentra disponible de forma determinada. Para activar esta opción, vaya a la siguiente ubicación de la carpeta: C:\Archivos de programa\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. A continuación, modifique el valor de *useDedicatedEthernet* como True.

```
- <SpecifyNetwork>
    <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

  La función Especificar red se desactiva en caso de almacén de datos remoto, que utilizaba la carpeta compartida de la red como destino.
- La función SMB multicanal está activada en Windows de forma predeterminada.

3. Si ha seleccionado **Disco local o carpeta compartida**, a continuación proporcione los detalles siguientes:



a. Proporcione la ruta completa del destino local o de red. Para el destino de la red, especifique las credenciales con acceso de escritura. Se puede hacer clic en Examinar para buscar el destino o haga clic en el icono de flecha hacia adelante para probar la conexión y proporcione las credenciales de la carpeta de destino proporcionada.

b. En la lista de opciones de la lista desplegable, seleccione el algoritmo de cifrado. Para obtener más información, consulte Configuración de cifrado.

c. Opcionalmente, proporcione una contraseña de cifrado.

d. Especifique la nueva contraseña de cifrado para confirmarla.

e. Seleccione un tipo de compresión. Para obtener más información, consulte Tipo de compresión.

Nota: Si se almacenan los datos a un disco local o a una carpeta compartida, no se pueden replicar los datos a otro servidor de puntos de recuperación. Solo se admite la replicación si se almacenan los datos en un servidor de puntos de recuperación.

Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces diariamente basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

Siga estos pasos:

1. (Opcional) Seleccione la opción para gestionar puntos de recuperación. Esta opción solo está visible si se ha seleccionado la carpeta local o compartida como destino de la copia de seguridad.

   Retener por puntos de recuperación

   Los datos de la copia de seguridad se almacenan como puntos de recuperación.

   Retener por conjuntos de recuperación

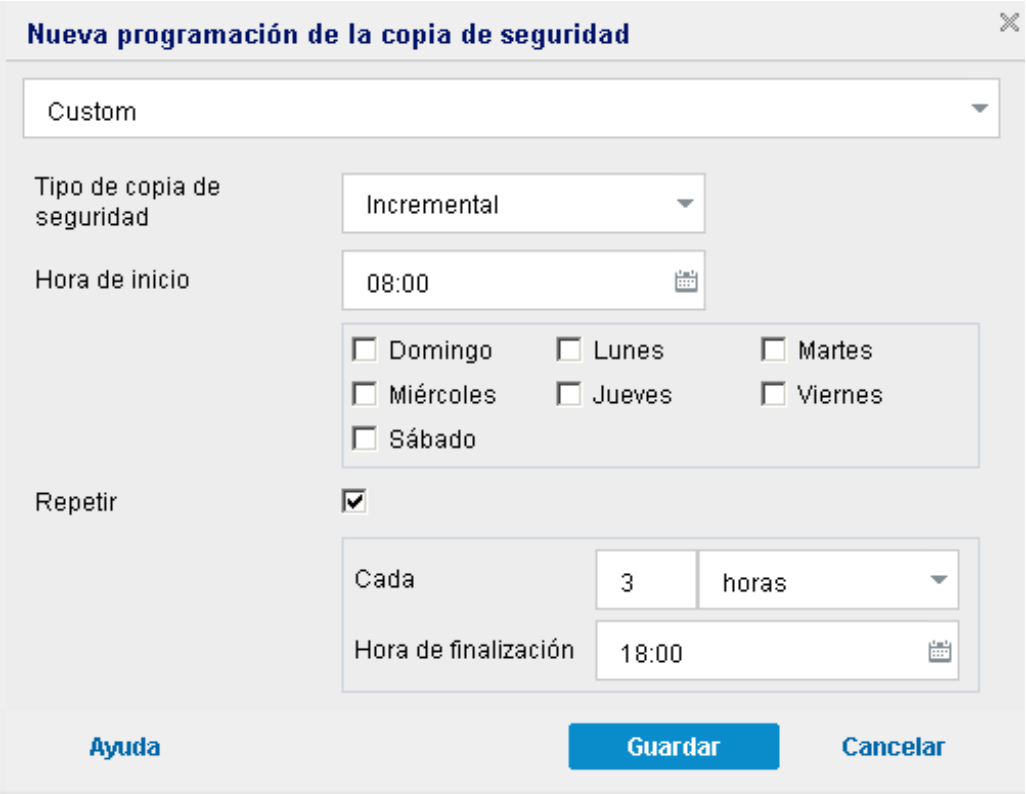
   Los datos de la copia de seguridad se almacenan como conjuntos de recuperación.

2. Agregue las programaciones de la copia de seguridad, de la combinación y del regulador.

   Agregar programación de la copia de seguridad

   a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

      Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Verificar

Especifica la programación de la copia de seguridad para las copias de seguridad de verificación.

Tal y como se ha programado, Arcserve UDP verifica que los datos protegidos sean válidos y estén completos mediante una comprobación de confianza de la imagen de copia de seguridad almacenada en el origen de la copia de seguridad original. Si es necesario, volverá a sincronizar la imagen. Una copia de seguridad de verificación se fijará en la copia de seguridad más reciente de cada bloque individual y comparará el contenido y la información con la de origen. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad de un bloque no coincide con la del origen (posiblemente por cambios en el sistema desde la última copia de seguridad), Arcserve UDP actualiza (resincroniza) la copia de seguridad del bloque que no coincide. Se puede utilizar también una copia de seguridad de verificación (aunque poco frecuentemente) para obtener la garantía de copia de seguridad completa sin utilizar el espacio necesario para una copia de seguridad completa.

Ventajas: produce una pequeña imagen de copia de seguridad si se compara con la copia de seguridad completa porque solamente se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventajas: el tiempo durante el cual se realiza la copia de seguridad es considerable puesto que todos los bloques de origen se comparan con los bloques de la última copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Es la manera más

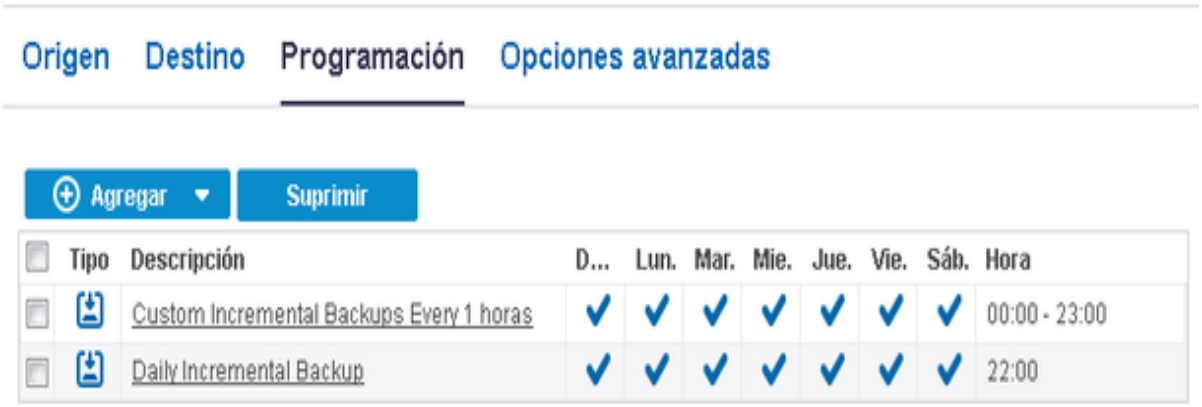
óptima de realizar copias de seguridad y es la que se debería utilizar de manera predeterminada.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en **Agregar** y seleccione **Agregar programación de la combinación**.

b. Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

c. Especifique la hora de inicio para iniciar la tarea de combinación.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

e. Haga clic en **Guardar**.

La Programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

b. Se abre el cuadro de diálogo Agregar nueva programación del limitador.

c. Especifique el límite de rendimiento en MB por minuto.

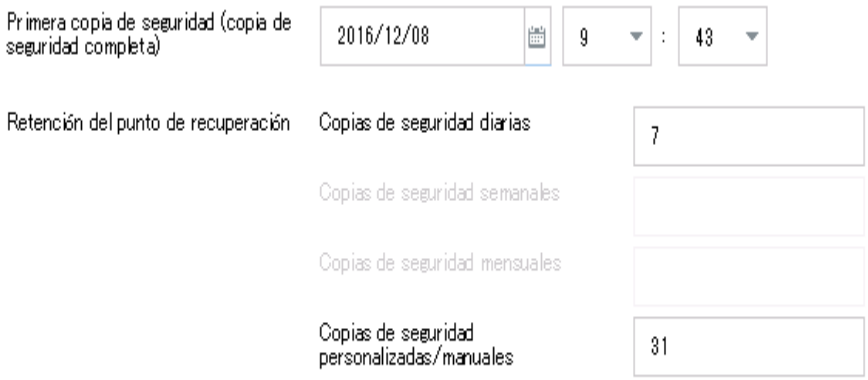
d. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

e. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

f. Haga clic en **Guardar**.

La Programación del rendimiento se especifica y se muestra en la página **Programación.**

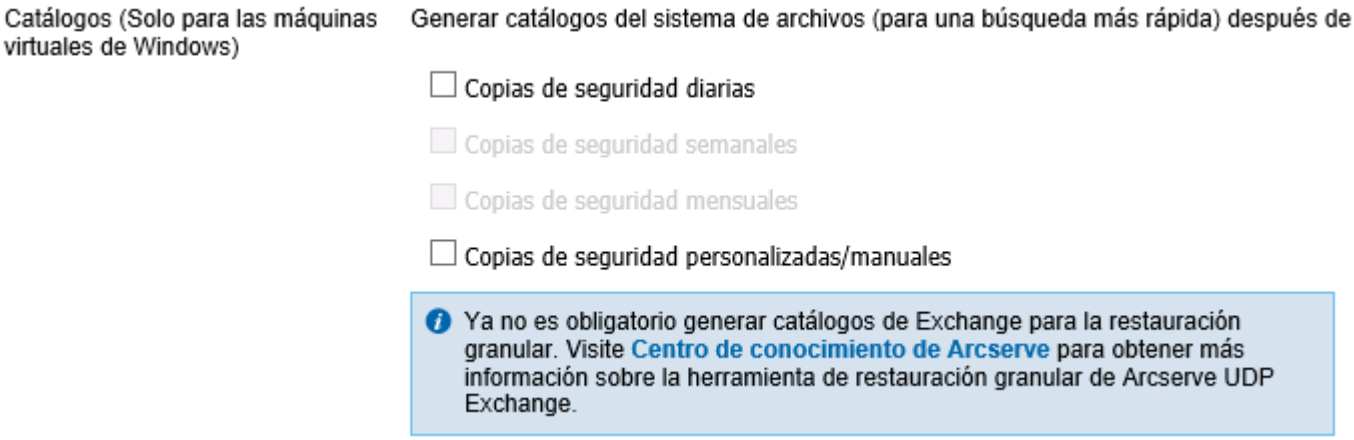
3. Especifique la hora de inicio para la copia de seguridad programada.



4. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

   Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo Programación de la copia de seguridad.

5. Especifique los detalles del catálogo.



Los catálogos permiten generar el catálogo del sistema de archivos. El catálogo del sistema de archivos se requiere para realizar la búsqueda más rápida y más fácil. Los catálogos se activan en función del tipo de copia de seguridad especificada.

Se especifica la programación.

Funcionamiento de la programación avanzada y de la retención

La opción de programación le permite especificar una programación personalizada, una programación diaria/semanal/mensual o ambas. En la programación personalizada, se puede configurar la programación de la copia de seguridad durante cada día de la semana y se pueden agregar hasta cuatro programaciones de copia de seguridad cada día. Se puede seleccionar un día específico de una semana y crear un período de tiempo para definir cuando se desea ejecutar la copia de seguridad y con qué frecuencia.

Programación	Tarea compatible	Comentarios
Copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para ejecutar las tareas de copia de seguridad.
Regulación de la copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para controlar la velocidad de la copia de seguridad.
Combinar	Tarea de combinación	Defina cuando se deben ejecutar las tareas de combinación.
Programación diaria	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad diarias.
Programación semanal	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad semanales.
Programación mensual	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad mensuales.

Se pueden especificar también los valores de configuración de retención para los puntos de recuperación.

Nota: Establezca la configuración de la retención en cada plan para controlar cómo se retienen los datos para los nodos asignados a ese plan en el almacén de datos de destino.

Las programaciones para las copias de seguridad diarias/semanales/mensuales son independientes de la programación personalizada y de las unas a las otras. Se puede configurar solamente ejecutar una copia de seguridad diaria, una copia de seguridad semanal o una copia de seguridad mensual sin configurar la programación personalizada.

Programación de la tarea de copia de seguridad

Se pueden agregar cuatro períodos de tiempo por día en la programación de la copia de seguridad. Un período de tiempo válido es desde las 12:00 horas hasta las 23:59 horas. No se puede especificar un período de tiempo como, por

ejemplo, de las 18:00 horas a las 06:00 horas. En tales casos, se debe especificar manualmente dos períodos de tiempo diferentes.

Para cada período de tiempo, la hora de inicio está incluida y, en cambio, no se incluye la hora de finalización. Por ejemplo, se ha configurado ejecutar una copia de seguridad incremental ejecutada todas las horas entre las 06:00 horas y las 09:00 horas y la copia de seguridad se iniciará a las 06:00 horas. Esto significa que la copia de seguridad se ejecuta a las 06:00 horas, a las 07:00 horas y a las 08:00 horas, pero NO a las 09:00 horas.

Nota: Si desea ejecutar la tarea de copia de seguridad reiteradamente hasta el final del día, configure la programación hasta las 12:00 horas. Por ejemplo, para ejecutar la tarea de copia de seguridad cada 15 minutos durante todo el día, configure la programación de las 12:00 a las 12:00, cada 15 minutos.

Programación del regulador de la copia de seguridad

La programación del regulador de la copia de seguridad le permite controlar la velocidad del rendimiento de la copia de seguridad, que a su vez controla el uso de recursos (E/S del disco, CPU, ancho de banda de la red) del servidor del que se está realizando la copia de seguridad. Esto es útil si no se desea afectar al rendimiento del servidor durante el horario comercial. Se pueden agregar cuatro períodos de tiempo por día en la programación del regulador de la copia de seguridad. Para cada período de tiempo, se puede especificar un valor en MB por minuto. Este valor se utiliza para controlar el rendimiento de la copia de seguridad. Los valores válidos van desde 1 MB/minuto a 99999 MB/minuto.

Si una tarea de copia de seguridad excede el tiempo especificado, el límite del regulador se ajusta según el período de tiempo especificado. Por ejemplo, se ha definido el límite del regulador de la copia de seguridad en 500 MB/minuto desde las 08:00 horas a las 20:00 horas y en 2500 MB/minuto de las 20:00 horas a las 22:00 horas. Si una tarea de copia de seguridad se inicia a las 19:00 horas y se ejecuta durante tres horas, el límite del regulador es de 500 MB/minuto de las 19:00 horas a las 20:00 horas y de 2500 MB/minuto de las 20:00 horas a las 22:00 horas.

Si no se define ninguna programación de la copia de seguridad ni ninguna programación del rendimiento de la copia de seguridad, la copia de seguridad se ejecuta tan deprisa como pueda.

Programación de la combinación

Le permite combinar puntos de recuperación basándose en la programación proporcionada.

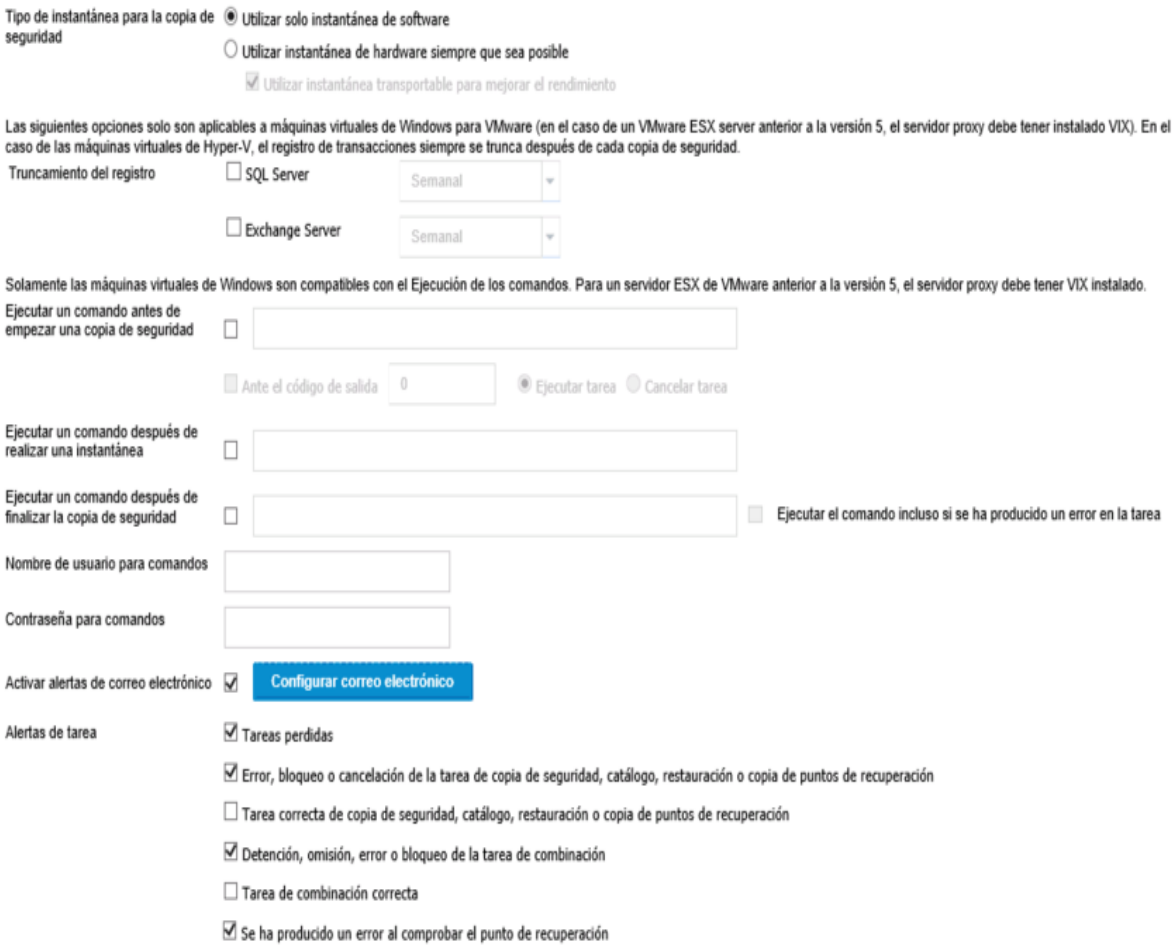
Tenga en cuenta los puntos siguientes para la tarea de combinación:

- Solamente una tarea de combinación puede ejecutarse para un nodo en cualquier momento proporcionado.
- Si se inicia una tarea de combinación, se tiene que completar antes de que la siguiente tarea de combinación se pueda iniciar. Esto no significa que, si uno o más conjuntos de puntos de recuperación se combinan, no se pueda agregar un punto de recuperación nuevo a este proceso de combinación hasta que el proceso de combinación del conjunto actual de puntos de recuperación se complete.
- Si una tarea de combinación está procesando más de un conjunto de puntos de recuperación (por ejemplo, el conjunto [1~4], el conjunto [5~11] y el conjunto [12~14] son tres conjuntos), el servidor de puntos de recuperación procesará estos conjuntos uno a uno.
- Si una tarea de combinación se reanuda después de una pausa, la tarea detecta en qué punto se ha pausado y reanuda la combinación a partir del punto de pausa.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye proporcionar el tipo de instantánea para la copia de seguridad, configurar el truncamiento de los registros, proporcionar la ubicación de los scripts y configurar el correo electrónico. Revise los requisitos previos antes de seleccionar el tipo de instantánea de hardware.

La imagen siguiente se muestra en la ficha Avanzada:



Siga estos pasos:

1. Especifique los siguientes detalles:

   Tipo de instantánea para la copia de seguridad

   Seleccione una de las opciones siguientes para la instantánea de copia de seguridad:

Utilizar solo instantánea de software

Especifica que el tipo de copia de seguridad utiliza solo la instantánea de software. Arcserve UDP no buscará la instantánea de hardware. La instantánea de software utiliza menos recursos en las máquinas virtuales. Se puede utilizar esta opción si el servidor tiene una velocidad de configuración y procesamiento menor.

Utilice la instantánea de hardware siempre que sea posible

Especifica que el tipo de copia de seguridad primero busca una instantánea de hardware. Si se cumplen todos los criterios, el tipo de copia de seguridad utiliza la instantánea de hardware.

Nota: Para obtener más información sobre los criterios de instantánea de hardware, consulte los requisitos previos.

En el caso de Hyper-V, Arcserve UDP utiliza el proveedor de hardware para tomar una instantánea VSS de los volúmenes del host de Hyper-V e importar la instantánea de hardware en el servidor proxy. El servidor proxy debe tener un proveedor de hardware apropiado instalado. En el caso de VMware, Arcserve UDP crea una instantánea de software vSphere durante un período de tiempo breve y, a continuación, crea una instantánea de hardware. Esta instantánea de hardware se monta en el servidor ESX de VMware y se suprime la instantánea de software. A continuación, Arcserve UDP utiliza el contenido de la instantánea de hardware para realizar una copia de seguridad de los archivos relacionados con la máquina virtual.

Utilizar instantáneas transportables para mejorar el rendimiento

Especifica que la instantánea de hardware utiliza una instantánea transportable. Una instantánea transportable aumenta el rendimiento de la copia de seguridad. Esta opción solo es aplicable para servidores de Hyper-V.

Cómo truncar un registro

Permite especificar la programación para truncar los registros de SQL Server y Exchange Server. Se puede especificar la programación como **Diaria**, **Semanal** o **Mensual**. Esto es aplicable solamente para VMware.

Ejecutar un comando antes de empezar una copia de seguridad

Permite ejecutar un script antes de que se inicie la tarea de copia de seguridad. Especifique la ruta donde está almacenado el script en el sistema operativo invitado de la máquina virtual. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de seguridad continuará cuando el script devuelva el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se

detendrá cuando el script devuelva el código de salida. Esto es aplicable solamente para la máquina virtual de Windows.

Notas: (aplicable también para los comandos Después de realizar la instantánea y After backup is completed [Después de que se haya completado la copia de seguridad])

- Se recomienda especificar la ruta completa del comando/script. Por ejemplo, se debe utilizar C:\Windows\System32\Ping.exe, en lugar de simplemente Ping.exe.
- Para evitar que la tarea de copia de seguridad se bloquee debido a la detención del script o del comando, el script o comando terminan de manera predeterminada si no pueden completar la tarea transcurridos 3 minutos desde su inicio. Si desea cambiar el valor de configuración del tiempo de espera predeterminado, siga estos pasos en el servidor proxy o en el nivel de la máquina virtual:

  En el nivel de servidor proxy (aplicable a todas las tareas de copia de seguridad que se ejecutan en este servidor proxy)

  a. Abra la clave de registro desde la siguiente ubicación:

     [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

  b. Agregue un valor DWORD con el nombre PrePostCMDTimeoutInMinute y especifique el valor del tiempo de espera en minutos.

  En el nivel de máquina virtual

  a. Abra la clave de registro desde la siguiente ubicación:

     [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

  b. Agregue un valor DWORD con el nombre PrePostCMDTimeoutInMinute y especifique el valor del tiempo de espera en minutos.

     Nota: Si se agrega el valor de registro en el registro tanto en el nivel de la máquina virtual como en el nivel del proxy, la configuración del registro en el nivel de la máquina virtual tiene prioridad sobre la configuración del registro en el nivel del servidor proxy.

Ejecutar un comando después de realizar una instantánea

Le permite ejecutar un script después de realizar la instantánea de la copia de seguridad. Especifique la ruta donde está almacenado el script en el sistema operativo invitado de la máquina virtual. Esto es aplicable solamente para la máquina virtual de Windows.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta donde está almacenado el script en el sistema operativo invitado de la máquina virtual. Esto es aplicable solamente para la máquina virtual de Windows.

Ejecutar el comando incluso si se ha producido un error en la tarea

Si se selecciona esta casilla de verificación, el script especificado en Ejecutar un comando después de finalizar una copia de seguridad se ejecuta incluso cuando se produce un error en la tarea de copia de seguridad. De lo contrario, este script se ejecuta solamente cuando la tarea de copia de seguridad finaliza correctamente.

Nombre de usuario para comandos

Permite especificar el nombre de usuario para ejecutar los comandos.

Contraseña para comandos

Permite especificar la contraseña para ejecutar los comandos.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de alerta de las tareas que se desean recibir.

2. Haga clic en **Guardar**.

Las actualizaciones se guardan y se muestra una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota:

- Si se debe agregar otra tarea, se debe seleccionar el plan en la ficha Recursos y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar.
- Cuando se selecciona un nodo que no tiene instalado el Agente de Arcserve UDP, como el proxy de la copia de seguridad, la Consola de UDP implementa automáticamente a un agente en ese nodo después de guardar el plan.

Se crea el plan de copia de seguridad sin agente basada en el host para la máquina virtual. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

Ejecución del comando de script y truncamiento del registro con la cuenta del administrador adicional

La cuenta del administrador adicional hace referencia a esas cuentas que no son administradores predeterminados. Las dos cuentas siguientes están implicadas cuando se ejecutan los comandos o scripts:

1. Cuenta establecida por la Actualización de nodos
2. Cuenta establecida en la ficha Avanzada de un plan

Las máquinas virtuales de VMware e Hyper-V tienen condiciones diferentes para utilizar las cuentas de administradores adicionales.

Máquinas virtuales de VMware

Si se establecen las dos cuentas, utilice la primera cuenta para iniciar sesión en la máquina virtual (se utiliza el SDK de vSphere para comunicarse con la máquina virtual, por lo que el acceso de la red no será necesario entre el servidor proxy y la máquina virtual). A continuación, utilice la segunda cuenta para ejecutar el comando o script en la máquina virtual.

Si no se ha establecido una de las dos cuentas, utilice la cuenta disponible para iniciar sesión en la máquina virtual y ejecutar el comando o script.

Se recomienda utilizar la cuenta del administrador integrada o la cuenta del administrador del dominio integrada para ambas cuentas.

Si se utiliza cualquier cuenta de administrador adicional (cuenta de administrador no integrada), el procedimiento es diferente.

Siga estos pasos:

1. Para iniciar sesión en la máquina virtual mediante la cuenta del administrador agregada, siga el paso que se muestra en el tema Actualización de nodos para garantizar que la cuenta tenga los permisos obligatorios.
2. Para ejecutar el comando o script mediante la cuenta del administrador adicional, garantice que esta cuenta tiene el permiso obligatorio. Inicie sesión en la máquina virtual invitada mediante la cuenta del administrador adicional, ejecute el comando o script y confirme que el comando o script se pueden completar correctamente.

Máquinas virtuales de Hyper-V

Solo se necesita una cuenta para las máquinas virtuales de Hyper-V. Si se establecen las dos cuentas, utilice la segunda cuenta (que se ha establecido en la ficha Avanzada de un plan) para conectarse a la máquina virtual e iniciar el comando o script. Se utiliza Windows Management Instrumentation (WMI) para comunicarse

con la máquina virtual, por lo que el acceso de la red sea necesario entre el servidor proxy y la máquina virtual.

Si no se ha establecido una de las dos cuentas, utilice la cuenta del administrador disponible para conectarse a la máquina virtual e iniciar el comando o script.

Siga estos pasos:

1. Acceda a la máquina virtual con el servicio WMI remoto. Garantice que se tienen los permisos obligatorios con la cuenta del administrador adicional. Consulte el tema Actualización de nodos para obtener los requisitos de la cuenta.
2. Para ejecutar el comando o script mediante la cuenta del administrador adicional, garantice que esta cuenta tiene el permiso obligatorio. Inicie sesión en la máquina virtual invitada mediante la cuenta del administrador adicional, ejecute el comando o script y confirme que el comando o script se pueden completar correctamente.

   Además, compruebe si el cortafuegos permite WMI en la máquina virtual invitada. Si no está activado, siga estos pasos:

1. Inicie sesión en la máquina virtual invitada.
2. Abra el Panel de control.
3. Abra Firewall de Windows.
4. Haga clic en Permitir una aplicación o una característica a través de Firewall de Windows.
5. Active Windows Management Instrumentation (WMI).
6. Haga clic en Aceptar.

Definición de un límite para la cantidad de copias de seguridad simultáneas

La aplicación permite definir un límite para la cantidad de tareas de copia de seguridad que se ejecutan simultáneamente. Esta capacidad permite optimizar el rendimiento del servidor proxy de Host-Based VM Backup en el entorno de copia de seguridad. De forma predeterminada, Host-Based VM Backup puede ejecutar hasta cuatro tareas de copia de seguridad de máquina virtual de VMware, diez tareas de copia de seguridad de máquina virtual de Hyper-V y cuatro tareas de copia de seguridad de máquina virtual de Nutanix AHV simultáneamente. En entornos que contienen muchas máquinas virtuales asociadas con un servidor proxy, una cantidad elevada de copias de seguridad simultáneas puede tener un efecto adverso en el rendimiento de red y de copia de seguridad.

Nota: cuando la cantidad de tareas simultáneas sobrepasa el límite definido, las tareas que sobrepasan el límite se introducen en una cola de tareas.

Nota: Si el número máximo de tareas de copia de seguridad de VMware simultáneas excede el límite de conexión del servidor ESX, se puede producir un error de comunicación entre el servidor ESX y el proxy de la copia de seguridad, por lo que el sistema de archivos del almacén de datos de servidor ESX puede permanecer bloqueado. En tales casos, reinicie el servidor ESX o migre la máquina virtual bloqueada a otro almacén de datos para desbloquear la máquina virtual. Para obtener más detalles, consulte el documento de VMware (base de conocimiento de VMware: 1022543).

Siga estos pasos:

1. Inicie sesión en el sistema de proxy de la máquina virtual de Arcserve UDP.
2. Abra el editor del registro de Windows y desplácese hasta la siguiente clave:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
   ```

3. Busque las siguientes claves:

   ```
   VMwareMaxJobNum
   ```

   ```
   HyperVMaxJobNum
   ```

   ```
   AHVMaxJobNum
   ```

   Nota: Ambas claves están ya creadas y su valor predeterminado es 4 y 10, respectivamente.

4. Haga clic con el botón secundario del ratón en HyperVMaxJobNum o AHVMaxJobNum y, a continuación, haga clic en Modificar en el menú emergente.

Se abre el cuadro de diálogo Editar cadena.

5. En el campo Dato de valores, especifique la cantidad de tareas de copia de seguridad que se desea permitir ejecutar simultáneamente.
   - **Límite mínimo:** 1
   - **Límite máximo:** ninguno
   - **Valor predeterminado**: 10 para Hyper-V y 4 para VMware y Nutanix AHV.
6. Haga clic en Aceptar.

   Se definirá el límite.

   El límite de tareas de copia de seguridad simultáneas se ha definido.

(Opcional) Realización de una copia de seguridad manual

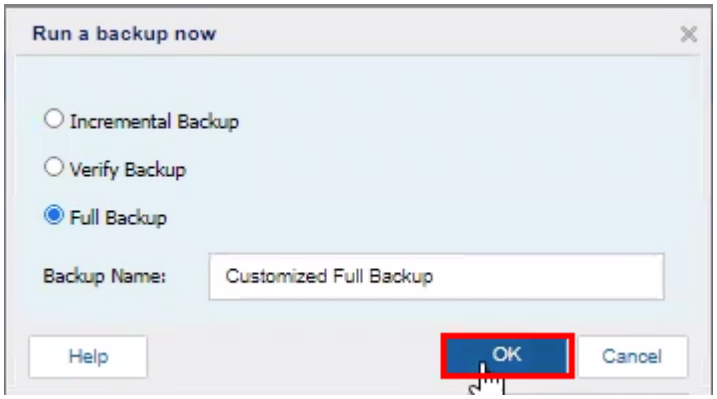
Normalmente se realizan copias de seguridad automáticamente y las controlan los valores de configuración de programación. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario. Por ejemplo, si tiene una programación de repetición para las copias de seguridad completas, incrementales y de resincronización y desea hacer cambios importantes en el equipo, se deberá realizar una copia de seguridad manual inmediata sin necesidad de esperar a la siguiente copia de seguridad programada.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Vaya a **recursos** > **Plan** > **Todos los planes**.

   La lista de todos los planes se muestra en el panel central.
3. Haga clic con el botón secundario del ratón en el plan y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
4. En el cuadro de diálogo Ejecutar una copia de seguridad ahora, seleccione el tipo de copia de seguridad que desea realizar y, a continuación, especifique el nombre de la copia de seguridad si es necesario.



A continuación se especifican las opciones disponibles:

Copia de seguridad incremental

Inicia una copia de seguridad incremental del equipo. Una copia de seguridad incremental sólo hará una copia de seguridad de los bloques que han cambiado desde la copia de seguridad anterior.

Nota: Si está realizando una copia de seguridad por primera vez, la copia de seguridad completa se iniciará automáticamente aunque haya seleccionado la opción Copia de seguridad incremental.

Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Ésta es la manera más óptima de realizar copias de seguridad.

Copia de seguridad de verificación

Inicia una copia de seguridad de verificación de su equipo examinando la copia de seguridad más reciente de cada bloque individual y comparando el contenido y la información con la original. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad para un bloque no coincide con la de origen, el Agente de Arcserve UDP (Windows) actualizará (resincronizará) la copia de seguridad del bloque que no coincida.

Ventaja: Una imagen de copia de seguridad muy pequeña se produce cuando se compara con una copia de seguridad completa porque solo se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventaja: El tiempo de copia de seguridad es lento porque todos los bloques del disco de origen se comparan con los bloques de la última copia de seguridad.

Copia de seguridad completa

Inicia una copia de seguridad completa del equipo o los volúmenes seleccionados.

Notas:

- Si se agrega un nuevo volumen al origen de la copia de seguridad, se realizará una copia de seguridad completa del nuevo volumen agregado, independientemente del método de copia de seguridad general seleccionado.
- Si no se especifica ningún nombre de copia de seguridad, de forma predeterminada se denominará Copia de seguridad completa/incremental/de verificación personalizada.

5. Haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.

6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.

7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   Nota: Solamente se puede restaurar una tarea cada vez. Si intenta iniciar una tarea de copia de seguridad manualmente cuando se está ejecutando otra tarea al mismo tiempo, aparecerá un mensaje de alerta para informar de que otra tarea está en ejecución y solicitará intentarlo de nuevo más tarde.

   La copia de seguridad manual se realiza correctamente.

   Nota: También se puede activar la copia de seguridad de manera manual. Haga clic con el botón secundario del ratón y seleccione **Copia de seguridad ahora** de la lista de opciones. En este caso, si el plan protege objetos contenedor de vSphere, UDP activa la copia de seguridad para todas las máquinas virtuales disponibles en ese contenedor.

Verificación del plan

Para verificar la copia de seguridad, confirme que se ha creado correctamente el plan de copia de seguridad. Después de verificar que el plan se ha creado correctamente, confirme si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Se puede verificar el estado de las tareas de copia de seguridad en la ficha tareas.

Siga estos pasos: para verificar los planes.

1. Haga clic en la ficha Recursos.
2. En el panel izquierdo, vaya a Nodos y haga clic en Todos los nodos.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga estos pasos: para verificar las tareas de copia de seguridad.

1. Haga clic en la ficha tareas.
2. En el panel izquierdo, haga clic en Todas las tareas.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Cómo crear un plan de Virtual Standby a AWS EC2

Virtual Standby convierte los puntos de recuperación en formatos de máquina virtual en la nube especificada y prepara una instantánea para poder recuperar fácilmente los datos cuando sea necesario. Esta función también proporciona la capacidad de alta disponibilidad y garantiza que la máquina virtual puede tomar el control inmediatamente cuando se produce un error en el equipo de origen. La máquina de Virtual Standby se crea convirtiendo los puntos de recuperación en un formato de máquina virtual de Amazon AWS EC2.

Nota: La tarea de Virtual Standby se ejecuta solamente si la tarea de copia de seguridad crea una instantánea del punto de recuperación válida. Si se produce un error en la tarea de copia de seguridad, se omite la tarea de Virtual Standby.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Creación de un plan con una tarea de copia de seguridad
3. Adición al plan de una tarea de Virtual Standby a EC2
4. (Opcional) Ejecución manual de la tarea de Virtual Standby a EC2
5. Pausa y reanudación de la tarea de Virtual Standby
6. Verificación del plan
7. Finalización de recursos de EC2

Revisión de las consideraciones y requisitos previos

Verifique si se han completado los requisitos previos siguientes:

- Inicie sesión en la Consola.
- Se ha instalado el componente del servidor y se han creado almacenes de datos si se desea almacenar los datos de la copia de seguridad en servidores de punto de recuperación.
- Se tiene un punto de recuperación válido para crear un equipo de Virtual Standby. Los puntos de recuperación pueden ser de una de las tareas siguientes:
  - Copia de seguridad de Windows basada en el agente
  - Copia de seguridad sin agente basada en el host
  - Replicación
  - Replicación desde un servidor de punto de recuperación remoto
- Realice una copia de seguridad de todo el equipo para activar la tarea de Virtual Standby. Si la copia de seguridad no es completa, no se puede crear una tarea de Virtual Standby.
- Instale el volumen del sistema en el primer disco. Verifique que el volumen del sistema y el volumen de arranque del equipo de origen se encuentran en el mismo disco.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.
- Configure la configuración del grupo de seguridad en EC2 para abrir los puertos relacionados para el acceso entrante, incluyendo TCP 8014 y TCP 4091.
- Compruebe si la cuenta Amazon AWS puede acceder a AWS S3 y a AWS EC2. Arcserve UDP no proporciona la cuenta.
- Instale el volumen del sistema en el primer disco. Verifique que el volumen del sistema y el volumen de arranque del equipo de origen se encuentran en el mismo disco.
- Se requieren permisos de la API de AWS específicos para los usuarios de Amazon IAM para lograr el control y la interacción con las API de AWS para Virtual Standby para EC2. Para obtener más detalles, consulte Configuración de los permisos granulares de IAM para los usuarios de IAM con Virtual Standby para EC2.

Consideraciones:

- La tarea de Virtual Standby a EC2 NO admite el arranque del equipo de origen desde el firmware de UEFI debido a la limitación de Amazon AWS EC2.
- .NET framework 4.5 es necesario en el equipo de origen para instalar el controlador de Amazon PV para la tarea de Virtual Standby a EC2.
- El volumen de arranque y del sistema que se encuentran en el nodo de origen en el plan Virtual Standby para EC2 deben estar en el primer disco debido a una limitación de AWS.
- La personalización de la configuración de TCP/IP no se puede aplicar a la primera interfaz de red en la instancia de EC2 debido a una limitación de AWS.
- La asignación de direcciones IP elástica solo está disponible para la primera interfaz de red de la instancia de EC2.
- La personalización de la configuración de TCP/IP solo es aplicable en el escenario cuando se configura el acceso directo o VPN entre el sitio principal y la red de AWS. De lo contrario, la personalización hace que la instancia de EC2 sea inaccesible.
- No se puede modificar la propiedad de activar/desactivar la asignación automática de la IP pública para los nodos existentes en el plan y la actualización solo afecta a los nuevos nodos agregados en el plan.
- Se debe instalar PowerShell versión 3.0 o posterior en el equipo de origen antes de configurar VSB a EC2 para los siguientes tipos de instancia:

  C5, C5d, C5n, F1, G3, G4, H1, I3, I3en, Inf1, m4.16xlarge, M5, M5a, M5ad, M5d, M5dn, M5n, P2, P3, R4, R5, R5a, R5ad, R5d, R5dn, R5n, T3, T3a, X1, X1e y z1d

Configuración de los permisos granulares de IAM para los usuarios de IAM con Virtual Standby para EC2

Esta sección explica los pasos y la política de permisos de la API requeridos para el Agente de Arcserve UDP instalado en el proxy de la nube de Virtual Standby en los servicios web de Amazon EC2. Los permisos permiten realizar las acciones requeridas para la transferencia de datos y Virtual Standby para la nube de AWS EC2.

Mediante el procedimiento, se puede ayudar a un usuario de Amazon IAM a obtener el control y la interacción con la API de AWS. La política de permisos no solo se aplica directamente al usuario, sino que también se aplica a un rol y grupo en la interfaz de seguridad de IAM de los servicios web de Amazon.

Siga estos pasos:

1. Inicie sesión en los servicios web de Amazon como administrador.
2. Seleccione My Security Credentials, haga clic en **Users** en el lado izquierdo y, a continuación, haga clic en el botón **Create New Users**.
3. Escriba el nombre de usuario que desee.

   Nota: Verifique si la opción para **generar una clave de acceso para cada usuario** está seleccionada.
4. Haga clic en el botón **Create**.
5. Haga clic en **Download Credentials**.

   Las credenciales contienen la clave de acceso y el secreto, que se necesitará más tarde en la Consola de UDP.
6. Desde la vista Users, seleccione el usuario de la lista de usuarios y, a continuación, haga clic en la ficha Permissions disponible en la parte inferior.
7. Desde la opción Custom Policy, cree una política personalizada en línea para el usuario.
8. Introduzca un nombre para la política y pegue el siguiente contenido en el documento de la política.

   ```
   {
   "Version": "2012-10-17",
   "Statement": [
   {
       "Sid": "Stmt1477881304097",
       "Action": [
   ```

"ec2:AssignPrivateIpAddresses",

"ec2:AssociateAddress",

"ec2:AttachNetworkInterface",

"ec2:AttachVolume",

"ec2:AuthorizeSecurityGroupEgress",

"ec2:AuthorizeSecurityGroupIngress",

"ec2:CreateNetworkInterface",

"ec2:CreateSnapshot",

"ec2:CreateTags",

"ec2:CreateVolume",

"ec2:DeleteNetworkInterface",

"ec2:DeleteSnapshot",

"ec2:DeleteTags",

"ec2:DeleteVolume",

"ec2:DescribeAccountAttributes",

"ec2:DescribeAddresses",

"ec2:DescribeAvailabilityZones",

"ec2:DescribeBundleTasks",

"ec2:DescribeClassicLinkInstances",

"ec2:DescribeConversionTasks",

"ec2:DescribeCustomerGateways",

"ec2:DescribeDhcpOptions",

"ec2:DescribeExportTasks",

"ec2:DescribeFlowLogs",

"ec2:DescribeHosts",

"ec2:DescribeHostReservations",

"ec2:DescribeHostReservationOfferings",

"ec2:DescribeIdentityIdFormat",

"ec2:DescribeIdFormat",

"ec2:DescribeImageAttribute",

"ec2:DescribeImages",

"ec2:DescribeImportImageTasks",

"ec2:DescribeImportSnapshotTasks",

"ec2:DescribeInstanceAttribute",

"ec2:DescribeInstanceStatus",

"ec2:DescribeInstances",

"ec2:DescribeInternetGateways",

"ec2:DescribeKeyPairs",

"ec2:DescribeMovingAddresses",

"ec2:DescribeNatGateways",

"ec2:DescribeNetworkAcls",

"ec2:DescribeNetworkInterfaceAttribute",

"ec2:DescribeNetworkInterfaces",

"ec2:DescribePlacementGroups",

"ec2:DescribePrefixLists",

"ec2:DescribeRegions",

"ec2:DescribeReservedInstances",

"ec2:DescribeReservedInstancesListings",

"ec2:DescribeReservedInstancesModifications",

"ec2:DescribeReservedInstancesOfferings",

"ec2:DescribeRouteTables",

"ec2:DescribeSecurityGroups",

"ec2:DescribeSnapshotAttribute",

"ec2:DescribeSnapshots",

"ec2:DescribeSpotDatafeedSubscription",

"ec2:DescribeSpotFleetInstances",

"ec2:DescribeSpotFleetRequestHistory",

"ec2:DescribeSpotFleetRequests",

"ec2:DescribeSpotInstanceRequests",

"ec2:DescribeSpotPriceHistory",

"ec2:DescribeStaleSecurityGroups",

"ec2:DescribeSubnets",

"ec2:DescribeTags",

"ec2:DescribeVolumeAttribute",

"ec2:DescribeVolumeStatus",

"ec2:DescribeVolumes",

"ec2:DescribeVpcAttribute",

"ec2:DescribeVpcClassicLink",

"ec2:DescribeVpcEndpointServices",

"ec2:DescribeVpcEndpoints",

"ec2:DescribeVpcPeeringConnections",

"ec2:DescribeVpcs",

"ec2:DescribeVpnConnections",

"ec2:DescribeVpnGateways",

"ec2:DetachClassicLinkVpc",

"ec2:DetachInternetGateway",

"ec2:DetachNetworkInterface",

"ec2:DetachVolume",

"ec2:DetachVpnGateway",

"ec2:DisableVgwRoutePropagation",

"ec2:DisableVpcClassicLink",

"ec2:DisableVpcClassicLinkDnsSupport",

"ec2:DescribeVpcClassicLinkDnsSupport",

"ec2:DetachNetworkInterface",

"ec2:DetachVolume",

"ec2:DisassociateAddress",

"ec2:ModifyInstanceAttribute",

"ec2:ModifyNetworkInterfaceAttribute",

"ec2:ModifySnapshotAttribute",

"ec2:ModifySubnetAttribute",

"ec2:ModifyVolumeAttribute",

"ec2:RevokeSecurityGroupEgress",

"ec2:RevokeSecurityGroupIngress",

```
            "ec2:RunInstances",
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Effect": "Allow",
        "Resource": [
        "*"
        ]
    },
    {
        "Sid": "Stmt1477880716900",
        "Action": [
            "s3:CreateBucket",
            "s3:DeleteBucket",
            "s3:DeleteObject",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:PutObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "Stmt1477883239716",
        "Action": [
            "iam:GetUser"
        ],
        "Effect": "Allow",
```

```
        "Resource": [
            "*"
        ]
    }
    ]
    }
```

9. Haga clic en **Apply Policy**.
10. En la Consola de UDP, utilice la clave de acceso de seguridad y la clave de acceso del usuario de IAM para crear Virtual Standby para EC2.

Creación de un plan con una tarea de copia de seguridad

Un plan incluye tipos diferentes de tareas que se desea realizar. Para crear una máquina de Virtual Standby, se crea un plan que incluye una tarea de copia de seguridad y una tarea de Virtual Standby. Una tarea de copia de seguridad realiza una copia de seguridad de los nodos de origen y almacena los datos en el destino especificado. La función de Virtual Standby utiliza a continuación estos datos de la copia de seguridad y los convierte a un formato de máquina virtual.

Se puede crear una máquina de Virtual Standby a partir de una copia de seguridad de Windows basada en el agente o a partir de una copia de seguridad sin agente basada en el host. Se puede crear también una máquina de Virtual Standby a partir de datos que se replican mediante la tarea **Replicar.** El procedimiento siguiente es un ejemplo para crear una copia de seguridad de Windows basada en el agente.

Notas:

- Para obtener más información sobre la copia de seguridad sin agente basada en el host, consulte Cómo crear un plan de copia de seguridad de máquina virtual basada en el host.
- Para obtener más información sobre cómo replicar los datos de una copia de seguridad, consulte Cómo replicar datos entre almacenes de datos gestionados desde una Consola de UDP y gestionados desde Consolas de UDP diferentes.
- La tarea Virtual Standby a EC2 no es compatible con el inicio del equipo de origen desde el firmware de UEFI debido a las limitaciones de Amazon AWS EC2.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

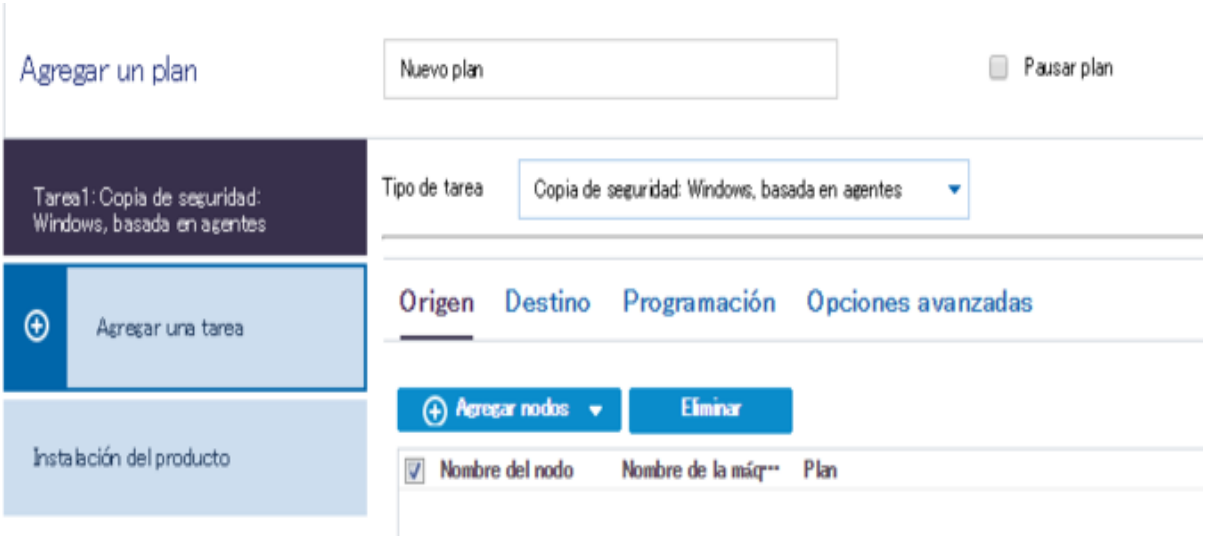
   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.

6. En la lista desplegable **Tipo de tarea** seleccione **Copia de Seguridad, Windows basado en el agente**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

La página Origen le permite especificar los nodos de origen que se desean proteger. Se pueden seleccionar más de un nodo del plan. Si no se ha agregado ningún nodo a la consola, se podrán agregar nodos al crear o modificar un plan en la página Origen. Se puede guardar un plan sin agregar ningún nodo de origen. El plan se implementa solamente después de agregar nodos de origen.

Siga estos pasos:

1. En la ficha Origen, haga clic en **Agregar**.
2. Seleccione una de las opciones siguientes:

   Seleccionar los nodos para proteger en Arcserve UDP

   Abre el cuadro de diálogo Seleccionar los nodos para proteger en Arcserve UDP. Seleccione los nodos de la lista que se muestra. Seleccione esta opción si ya se han agregado los nodos a la consola.

   Agregar nodo de Windows

   Se abre el cuadro de diálogo Agregar nodos a un plan. Seleccione esta opción si no se han agregado los nodos y desea agregarlos manualmente para la protección.

   Detectar nodos desde Active Directory

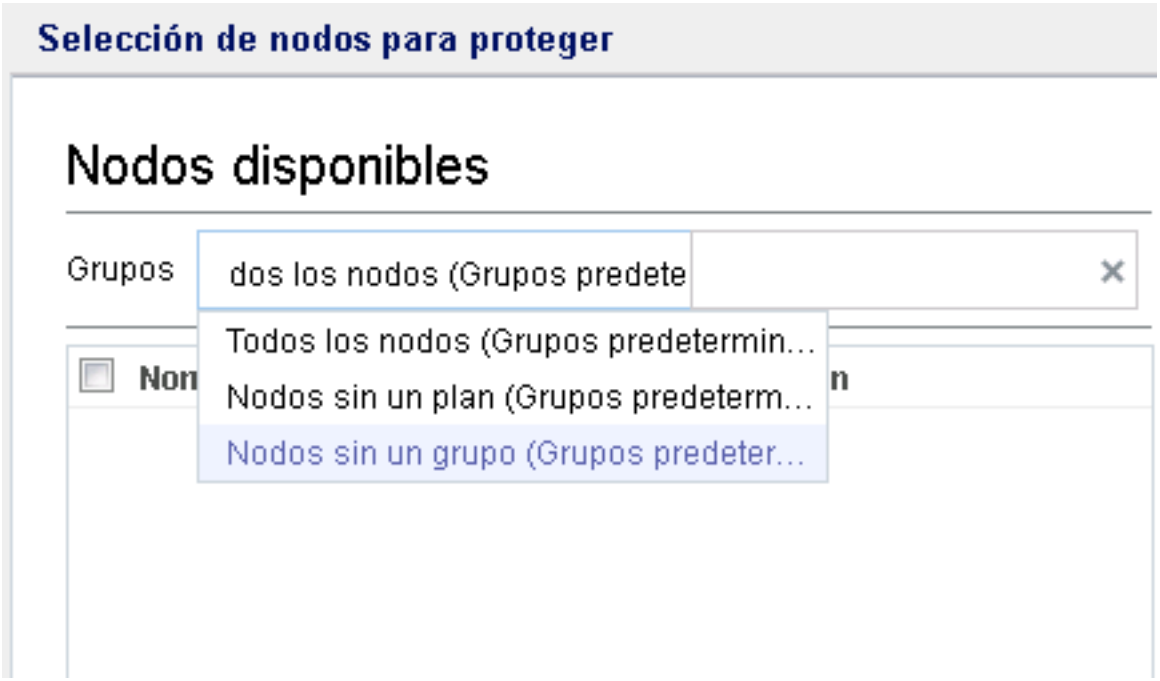
   Se abre el cuadro de diálogo Agregar nodos a la Consola de Arcserve UDP. Seleccione esta opción si desea detectar y agregar nodos en Active Directory.
3. Si ha seleccionado la opción **Seleccionar nodos para proteger en Arcserve UDP**, haga lo siguiente en el cuadro de diálogo Seleccionar nodos para proteger:
   a. (Opcional) Seleccione un filtro en la lista desplegable Grupos para filtrar nodos. Se pueden especificar palabras clave para filtrar más detalladamente los nodos.

      Los nodos se muestran en la columna Nodos disponibles.

   b. Seleccione los nodos en la columna Nodos disponibles y, a continuación, haga clic en la flecha simple hacia la derecha (>) o en la flecha doble hacia la derecha (>>) para mover los nodos seleccionados o todos los nodos respectivamente a la columna Nodos seleccionados.

      Los nodos se muestran en la columna Nodos seleccionados.

   c. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.



4. Para elegir el Tipo de El Protección, seleccione una de las opciones siguientes:

   Realizar copia de seguridad de todos los volúmenes

   Prepara una instantánea de copia de seguridad de todos los volúmenes.

   Realizar copia de seguridad de los volúmenes seleccionados

   Prepara una instantánea de copia de seguridad del volumen seleccionado.

   Se especifica el origen.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Seleccione uno de los siguientes **Tipos de destino**:

   Disco local o carpeta compartida

   Especifica que el destino de la copia de seguridad es un destino local o una carpeta compartida. Si se selecciona esta opción, se pueden guardar datos como puntos de recuperación o como conjuntos de recuperación. Las opciones Puntos de recuperación y Conjuntos de recuperación están disponibles en la ficha **Programación**.

   Servidor de puntos de recuperación de Arcserve UDP

   Especifica que el destino de la copia de seguridad es un servidor de punto de recuperación. Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.

2. Si se ha seleccionado **Servidor de punto de recuperación de Arcserve UDP**, se deben proporcionar los detalles siguientes:
   a. Seleccione un servidor de punto de recuperación.
   b. Seleccione un almacén de datos. La lista muestra todos los almacenes de datos que se han creado en el servidor de punto de recuperación especificado.
   c. Proporcione una contraseña de la sesión.
   d. Confirme la contraseña de la sesión.

3. Si ha seleccionado **Disco local o carpeta compartida**, a continuación proporcione los detalles siguientes:
   a. Proporcione la ruta completa del destino local o de red. Para el destino de la red, especifique las credenciales con acceso de escritura.
   b. Seleccione el algoritmo de cifrado. Para obtener más información, consulte Configuración de cifrado.
   c. Opcionalmente, proporcione una contraseña de cifrado.
   d. Confirme la contraseña de cifrado.

e. Seleccione un tipo de compresión. Para obtener más información, consulte Tipo de compresión.

Nota: Si se almacenan los datos a un disco local o a una carpeta compartida, no se pueden replicar los datos a otro servidor de punto de recuperación. Se es compatible con la replicación solamente si se almacenan los datos en un servidor de punto de recuperación.

Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y se pueden proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

Siga estos pasos:

1. (Opcional) Seleccione la opción para gestionar puntos de recuperación. Esta opción solo está visible si se ha seleccionado la carpeta local o compartida como destino de la copia de seguridad.

   Retener por puntos de recuperación

   Los datos de la copia de seguridad se almacenan como puntos de recuperación.

   Retener por conjuntos de recuperación

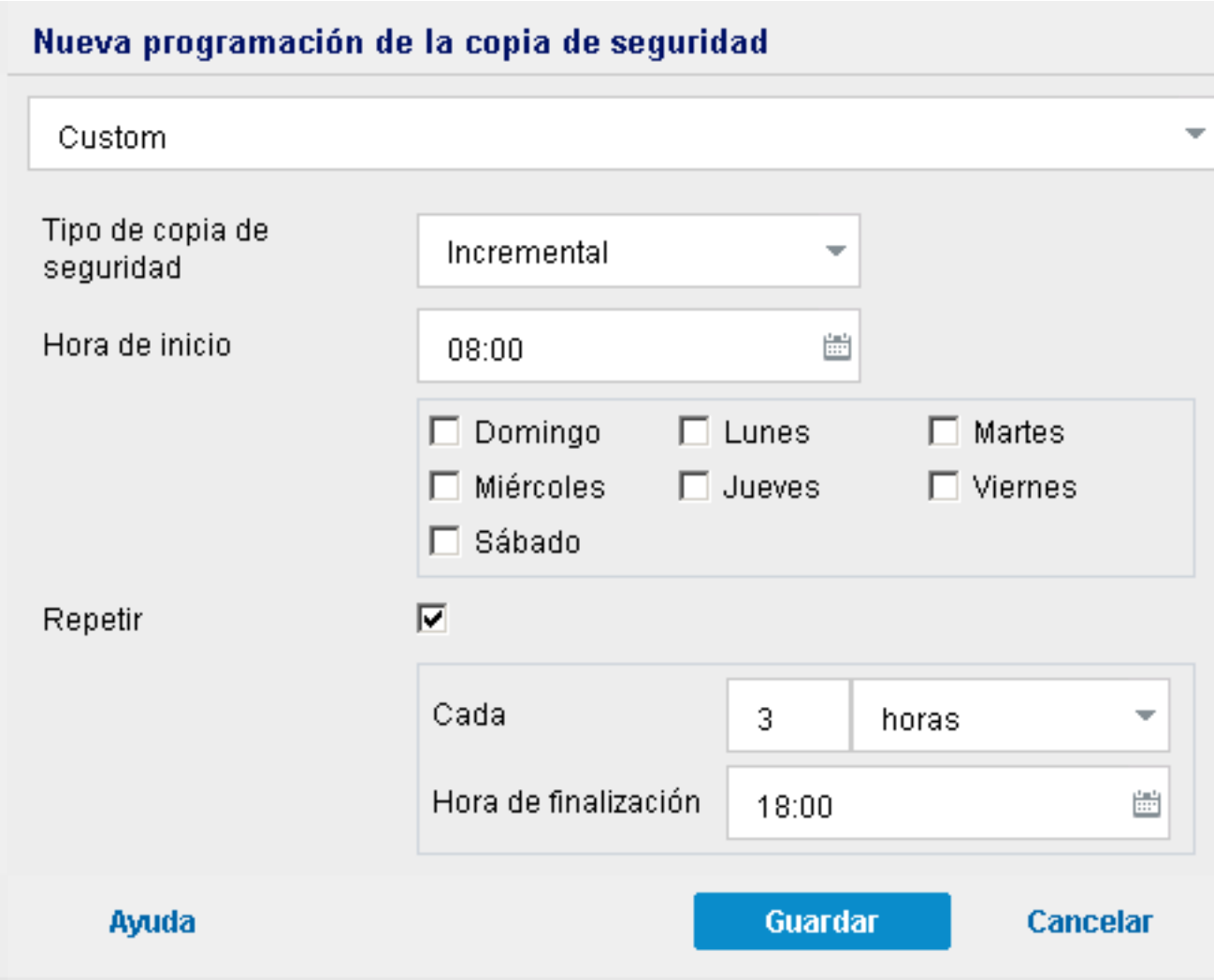
   Los datos de la copia de seguridad se almacenan como conjuntos de recuperación.

2. Agregue las programaciones de la copia de seguridad, de la combinación y del regulador.

   Agregar programación de la copia de seguridad

   a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

      Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Verificar

Especifica la programación de la copia de seguridad para las copias de seguridad de verificación.

Arcserve UDP verifica que los datos protegidos sean válidos y estén completos mediante una comprobación de confianza de la imagen de copia de seguridad almacenada en el origen de la copia de seguridad. Si es necesario, volverá a sincronizar la imagen. Una copia de seguridad de verificación se fijará en la copia de seguridad más reciente de cada bloque individual y comparará el contenido y la información con la de origen. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad de un bloque no coincide con la del origen (posiblemente por cambios en el sistema desde la última copia de seguridad), Arcserve UDP actualiza (resincroniza) la copia de seguridad del bloque que no coincide. Se puede utilizar también una copia de seguridad de verificación (aunque poco frecuentemente) para obtener la garantía de copia de seguridad completa sin utilizar el espacio necesario para una copia de seguridad completa.

Ventajas: produce una pequeña imagen de copia de seguridad si se compara con la copia de seguridad completa porque solamente se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventajas: el tiempo durante el cual se realiza la copia de seguridad es considerable puesto que todos los bloques de origen se comparan con los bloques de la última copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

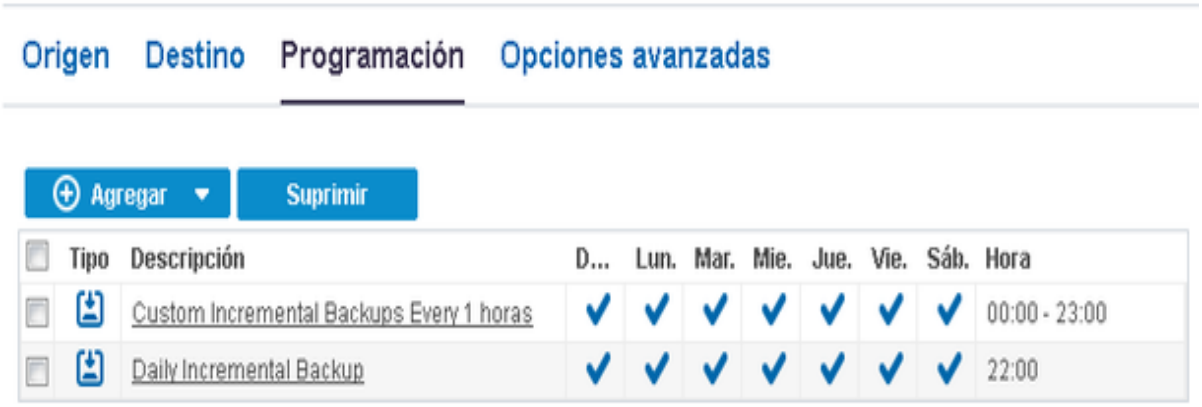
Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en Agregar y seleccione Agregar programación de la combinación.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

b. Especifique la hora de inicio para iniciar la tarea de combinación.

c. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

d. Haga clic en **Guardar**.

La Programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

   Se abre el cuadro de diálogo Agregar nueva programación del limitador.

b. Especifique el límite de rendimiento en MB por minuto.

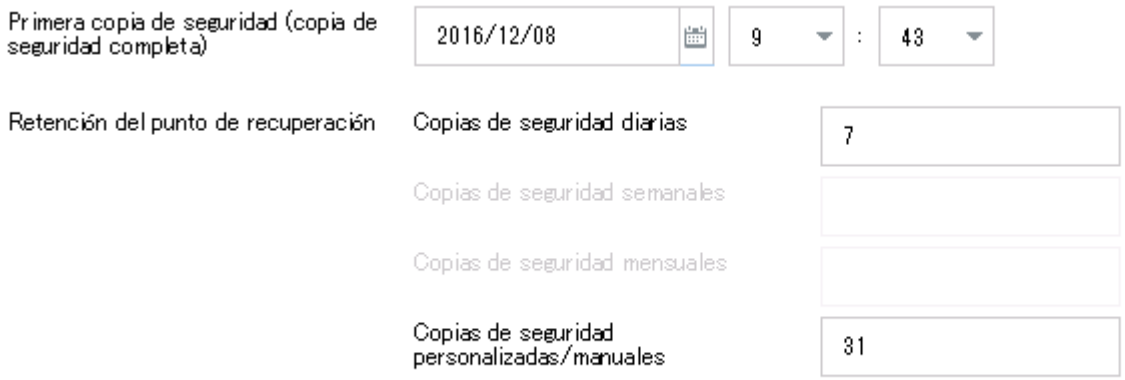
c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

   La programación del limitador se especifica y se muestra en la página **Programación**.

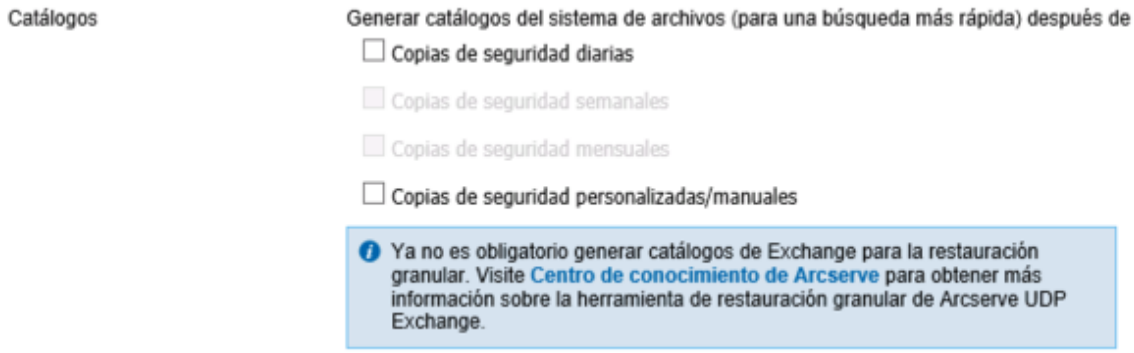
3. Especifique la hora de inicio para la copia de seguridad programada.



4. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

   Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo Programación de la copia de seguridad.

5. Especifique los detalles del catálogo.



Los catálogos permiten generar el catálogo del sistema de archivos. El catálogo del sistema de archivos se requiere para realizar la mejor búsqueda de la forma más rápida. Si se seleccionan las casillas de verificación del catálogo, los catálogos se activan en función del tipo de copia de seguridad especificada. Desactive la casilla de verificación para desactivar la generación del catálogo.

Se especifica la programación.

Funcionamiento de la programación avanzada y de la retención

La opción de programación le permite especificar una programación personalizada, una programación diaria/semanal/mensual o ambas. En la programación personalizada, se puede configurar la programación de la copia de seguridad durante cada día de la semana y se pueden agregar hasta cuatro programaciones de copia de seguridad cada día. Se puede seleccionar un día específico de una semana y crear un período de tiempo para definir cuando se desea ejecutar la copia de seguridad y con qué frecuencia.

Programación	Tarea compatible	Comentarios
Copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para ejecutar las tareas de copia de seguridad.
Regulación de la copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para controlar la velocidad de la copia de seguridad.
Combinar	Tarea de combinación	Defina cuando se deben ejecutar las tareas de combinación.
Programación diaria	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad diarias.
Programación semanal	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad semanales.
Programación mensual	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad mensuales.

Se pueden especificar también los valores de configuración de retención para los puntos de recuperación.

Nota: Establezca la configuración de la retención en cada plan para controlar cómo se retienen los datos para los nodos asignados a ese plan en el almacén de datos de destino.

Las programaciones para las copias de seguridad diarias/semanales/mensuales son independientes de la programación personalizada y de las unas a las otras. Se puede configurar solamente ejecutar una copia de seguridad diaria, una copia de seguridad semanal o una copia de seguridad mensual sin configurar la programación personalizada.

Programación de la tarea de copia de seguridad

Se pueden agregar cuatro períodos de tiempo por día en la programación de la copia de seguridad. Un período de tiempo válido es desde las 12:00 horas hasta las 23:59 horas. No se puede especificar un período de tiempo como, por

ejemplo, de las 18:00 horas a las 06:00 horas. En tales casos, se debe especificar manualmente dos períodos de tiempo diferentes.

Para cada período de tiempo, la hora de inicio está incluida y, en cambio, no se incluye la hora de finalización. Por ejemplo, se ha configurado ejecutar una copia de seguridad incremental ejecutada todas las horas entre las 06:00 horas y las 09:00 horas y la copia de seguridad se iniciará a las 06:00 horas. Esto significa que la copia de seguridad se ejecuta a las 06:00 horas, a las 07:00 horas y a las 08:00 horas, pero NO a las 09:00 horas.

Nota: Si desea ejecutar la tarea de copia de seguridad reiteradamente hasta el final del día, configure la programación hasta las 12:00 horas. Por ejemplo, para ejecutar la tarea de copia de seguridad cada 15 minutos durante todo el día, configure la programación de las 12:00 a las 12:00, cada 15 minutos.

Programación del regulador de la copia de seguridad

La programación del regulador de la copia de seguridad le permite controlar la velocidad del rendimiento de la copia de seguridad, que a su vez controla el uso de recursos (E/S del disco, CPU, ancho de banda de la red) del servidor del que se está realizando la copia de seguridad. Esto es útil si no se desea afectar al rendimiento del servidor durante el horario comercial. Se pueden agregar cuatro períodos de tiempo por día en la programación del regulador de la copia de seguridad. Para cada período de tiempo, se puede especificar un valor en MB por minuto. Este valor se utiliza para controlar el rendimiento de la copia de seguridad. Los valores válidos van desde 1 MB/minuto a 99999 MB/minuto.

Si una tarea de copia de seguridad excede el tiempo especificado, el límite del regulador se ajusta según el período de tiempo especificado. Por ejemplo, se ha definido el límite del regulador de la copia de seguridad en 500 MB/minuto desde las 08:00 horas a las 20:00 horas y en 2500 MB/minuto de las 20:00 horas a las 22:00 horas. Si una tarea de copia de seguridad se inicia a las 19:00 horas y se ejecuta durante tres horas, el límite del regulador es de 500 MB/minuto de las 19:00 horas a las 20:00 horas y de 2500 MB/minuto de las 20:00 horas a las 22:00 horas.

Si no se define ninguna programación de la copia de seguridad ni ninguna programación del rendimiento de la copia de seguridad, la copia de seguridad se ejecuta tan deprisa como pueda.

Programación de la combinación

Le permite combinar puntos de recuperación basándose en la programación proporcionada.

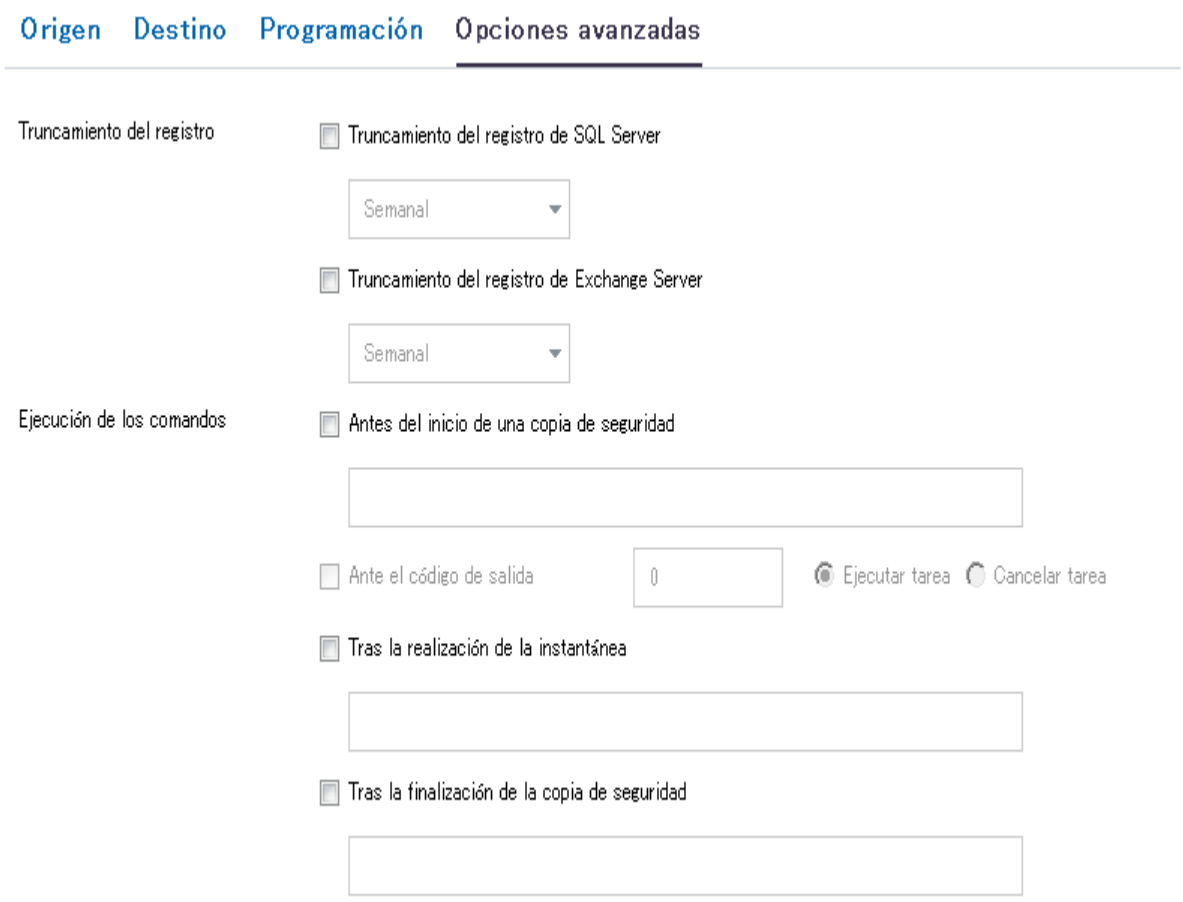
Tenga en cuenta los puntos siguientes para la tarea de combinación:

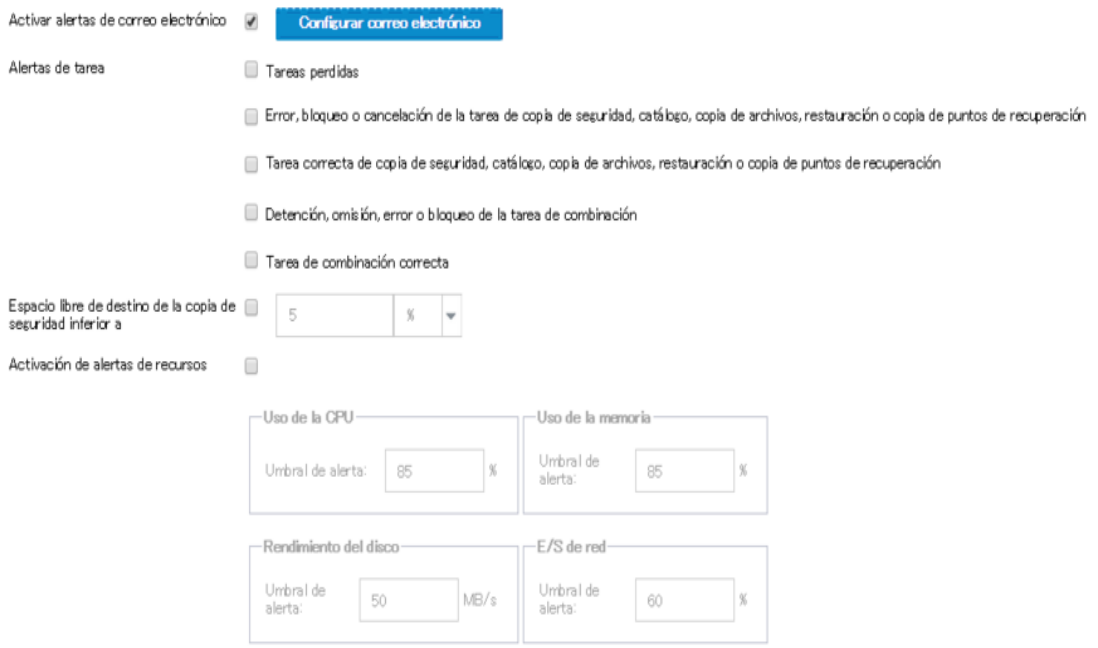
- Solamente una tarea de combinación puede ejecutarse para un nodo en cualquier momento proporcionado.
- Si se inicia una tarea de combinación, se tiene que completar antes de que la siguiente tarea de combinación se pueda iniciar. Esto no significa que, si uno o más conjuntos de puntos de recuperación se combinan, no se pueda agregar un punto de recuperación nuevo a este proceso de combinación hasta que el proceso de combinación del conjunto actual de puntos de recuperación se complete.
- Si una tarea de combinación está procesando más de un conjunto de puntos de recuperación (por ejemplo, el conjunto [1~4], el conjunto [5~11] y el conjunto [12~14] son tres conjuntos), el servidor de puntos de recuperación procesará estos conjuntos uno a uno.
- Si una tarea de combinación se reanuda después de una pausa, la tarea detecta en qué punto se ha pausado y reanuda la combinación a partir del punto de pausa.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye la configuración de registros de truncamiento, proporcionar la ubicación de los scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha Avanzada:





Siga estos pasos:

1. Especifique los siguientes detalles:

Cómo truncar un registro

Le permite especificar la programación para truncar los registros de SQL Server y Exchange Server. Se puede especificar la programación como **Diaria**, **Semanal** o **Mensual**.

Nombre de usuario

Le permite especificar el usuario que se autoriza para ejecutar un script.

Contraseña

Le permite especificar la contraseña del usuario autorizado para ejecutar el script.

Ejecutar un comando antes de empezar una copia de seguridad

Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde el script está almacenado. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de seguridad continuará cuando el script devuelva el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detendrá cuando el script devuelva el código de salida.

Ejecutar un comando después de realizar una instantánea

Le permite ejecutar un script después de realizar la instantánea de la copia de seguridad. Especifique la ruta donde el script está almacenado.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta donde el script está almacenado.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y se pueden especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de tareas que se desea recibir.

Cómo activar las alertas de recurso

Le permite especificar un umbral para el Uso de CPU, Uso de memoria, Rendimiento del disco y E/S de la red. Se puede proporcionar el valor en porcentaje. Se recibirá un correo electrónico cuando se exceda el valor de Umbral de alerta.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en Guardar.

Los cambios se guardan y se muestra una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **Recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar.

El plan de copia de seguridad se crea y se implementa automáticamente en el nodo de origen. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

Adición al plan de una tarea de Virtual Standby a EC2

Cree una tarea de Virtual Standby a EC2 para que los datos de la copia de seguridad se conviertan a un formato de máquina virtual y se cree una máquina virtual.

Notas:

- Virtual Standby a EC2 no es compatible con el inicio automático de la máquina virtual.
- Si se pausa el plan, la tarea de Virtual Standby no se iniciará. Cuando se vuelva a reanudar el plan, la tarea de Virtual Standby no se reanuda automáticamente. Se tiene que ejecutar manualmente otra tarea de copia de seguridad para iniciar la tarea de Virtual Standby. También, si el plan se pausa la opción Pausar/reanudar Virtual Standby no estará disponible. Si no se desea que la máquina virtual se inicie automáticamente después de que se haya pausado el plan, se deberá pausar manualmente el latido para los nodos.

Siga estos pasos:

1. Haga clic en **Agregar una tarea** en el panel izquierdo.

   Una tarea nueva se agrega al panel izquierdo.

2. En el menú desplegable **Tipo de tarea** seleccione **Virtual Standby**.

   La tarea de Virtual Standby se agrega.

3. En la ficha **Origen** seleccione un origen para la tarea de Virtual Standby.
4. Haga clic en la pestaña **Servidor de virtualización**.
5. Seleccione EC2 como el tipo de virtualización e introduzca los detalles.

   Tipo de virtualización: EC2

   Nombre de la cuenta

   Seleccione la cuenta de Amazon AWS existente para acceder a AWS EC2. También se puede agregar una nueva cuenta haciendo clic en **Agregar**. Para obtener más información, consulte Adición de una cuenta de la nube para Amazon EC2.

   Región de EC2

   Seleccione la región de EC2 donde se encuentra el servidor proxy de la nube. Arcserve UDP es compatible con todas las regiones globales de EC2 y con la región China EC2.

Nota: la cuenta especificada debe ser una cuenta administrativa o una cuenta con privilegios administrativos en EC2.

Servidor proxy de la nube de VSB

Especifique una instancia de EC2 en la región seleccionada como el servidor proxy de la nube.

Nota: La instancia de EC2 debe tener instalado el Agente de Arcserve UDP.

Nombre de usuario y Contraseña

Especifique las credenciales de inicio de sesión en el servidor proxy de la nube de VSB.

Protocolo

Especifique HTTP o HTTPS como el protocolo que desea utilizar para la comunicación entre el Agente de Arcserve Unified Data Protection de origen y el servidor proxy en la nube de Virtual Standby.

Puerto

Especifique el puerto que se desea utilizar para la transferencia de datos entre el servidor de origen y el servidor proxy de la nube de VSB.

Nota: Como el servidor proxy de la nube se utiliza para la transferencia de datos, los puertos relacionados deben estar activados para acceder como entrante en el grupo de seguridad de AWS EC2, incluyendo TCP 8014 y 4091.

6. Haga clic en la ficha **Máquina virtual** e introduzca los detalles de la configuración básica, de la configuración del almacenamiento en la nube y de la configuración de las redes.

   Amazon AWS EC2

   Aplique las siguientes opciones de la máquina virtual a Amazon AWS:

   Prefijo del nombre de la máquina virtual

   Especifique el prefijo que se desea agregar al nombre de visualización para la máquina virtual en AWS EC2.

   Valor predeterminado: UDPVM_

   Instantáneas del punto de recuperación

   Especifique el número de instantáneas del punto de recuperación (puntos de recuperación) para la máquina Virtual Standby. El número máximo de instantáneas del punto de recuperación es de 29 para AWS EC2.

   Combinar todas las sesiones sin convertir en una instantánea de punto de recuperación única

Especifique si desea combinar todas las sesiones sin convertir en una instantánea única de punto de recuperación cuando tenga lugar la siguiente tarea de Virtual Standby programada.

Valor predeterminado: Seleccionado

Tipo de instancia

Amazon EC2 proporciona una amplia selección de tipos de instancia optimizados para adaptarse a distintos casos de uso. Las instancias son servidores virtuales que pueden ejecutar aplicaciones. Tienen diversas combinaciones de CPU, memoria, almacenamiento y capacidad de la red, y proporcionan la flexibilidad necesaria para elegir la combinación apropiada de recursos para las aplicaciones. Para obtener más información sobre los tipos de instancia y cómo cumplen con las necesidades informáticas del usuario, consulte este vínculo.

Tipos de volumen EBS

Los volúmenes de uso general (SSD) pueden llegar a 3000 IOPS y entregar una línea de referencia coherente de 3 IOPS/GiB. Los volúmenes de IOPS aprovisionadas pueden llegar a 20000 IOPS y son los mejores para las instancias de EBS optimizadas. Los volúmenes magnéticos, conocidos anteriormente como volúmenes estándares, llegan a 100 IOPS de media y pueden llegar a cientos de IOPS. Para obtener más información sobre los tipos de volumen de EBS, consulte el vínculo.

Red

Permite definir el VPC, las subredes, las NIC y el grupo de seguridad de la máquina virtual de Virtual Standby en AWS EC2.

Nota: Cuando se activa la dirección IP pública de asignación automática, debido a la limitación de AWS EC2, solo se asigna una tarjeta NIC a AWS EC2 y el resto se descarta.

Mismo número de adaptadores de red que el origen en última copia de seguridad

Seleccione esta opción para definir cómo asignar la NIC virtual a la red en EC2. Especifique esta opción cuando la máquina virtual contiene NIC virtuales y una red virtual.

Nota: Estos valores de configuración solo están disponibles para la configuración cuando la dirección IP pública de asignación automática está desactivada.

7. Haga clic en **Guardar**.

Los cambios se guardan y la tarea de Virtual Standby se implementa automáticamente en el servidor de Virtual Standby.

Se ha creado e implementado correctamente el plan de Virtual Standby.

Agregación de una programación de limitación para la transferencia de datos a la nube

La programación de una limitación permite controlar la velocidad de rendimiento de la transferencia de datos a la nube (ancho de banda de la red) del servidor que se está transfiriendo a la nube. Esto es útil si no se desea afectar al rendimiento del servidor durante el horario comercial. Se pueden agregar hasta cuatro ventanas de tiempo por día en la programación de la limitación de la transferencia de datos a la nube. Para cada ventana de tiempo, se puede especificar un valor en MB o kB por segundo. Este valor se utiliza para controlar el rendimiento de la transferencia a la nube. Los valores válidos van desde 1 a 99999 MB o kB por segundo.

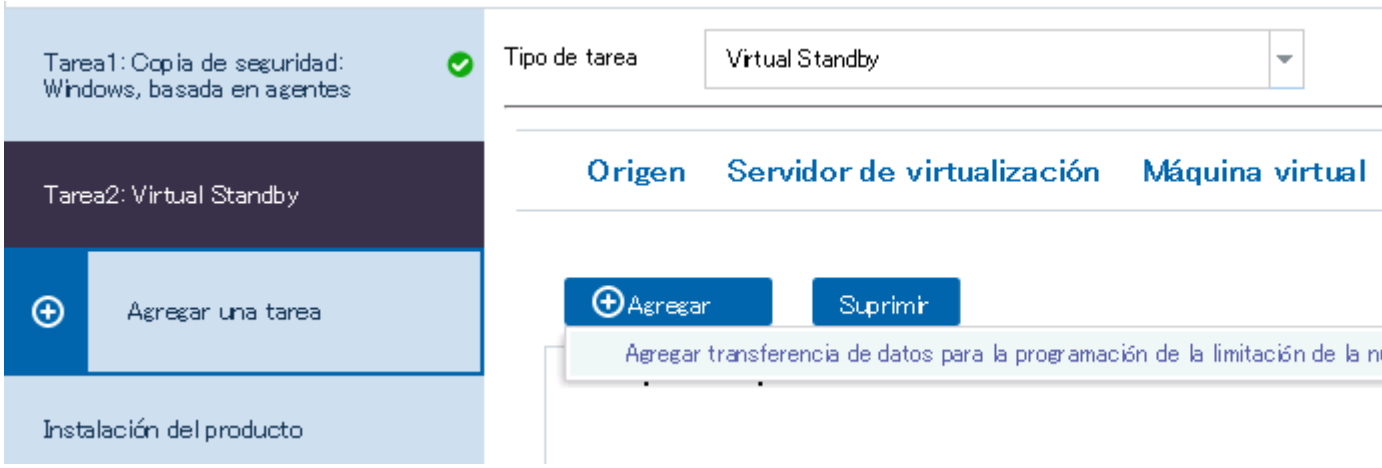
Si una tarea de transferencia de datos excede el tiempo especificado, el límite de la limitación se ajusta según la ventana de tiempo especificada. Por ejemplo, se ha definido el límite de la limitación de la transferencia de datos en 500 MB/s desde las 08:00 horas hasta las 20:00 horas y en 2500 MB/s de las 20:00 horas a las 22:00 horas. Si una tarea de transferencia de datos se inicia a las 19:00 horas y se ejecuta durante tres horas, el límite de la limitación es de 500 MB/s de las 19:00 horas a las 20:00 horas y de 2500 MB/s de las 20:00 horas a las 22:00 horas.

Si hay más de un nodo de origen en la tarea de copia de seguridad con espera virtual para la nube, se divide el límite de la limitación de manera equitativa. Por ejemplo, si se ha definido el límite de la limitación de la transferencia de datos en 500 MB/s y hay dos nodos de origen en el plan, cuando se transfieren sus datos a la nube al mismo tiempo, el límite de la limitación es de 250 MB/s para ambos nodos. Una vez que ha finalizado la tarea de transferencia de uno de los nodos, el límite de la limitación del otro nodo en ejecución se cambia a 500 MB/s.

Si no se define ninguna programación de limitación, la tarea de transferencia de datos a la nube se ejecuta tan rápido como sea posible.

Siga estos pasos:

1. Haga clic en Agregar y seleccione Agregar programación de limitación para a la transferencia de datos a la nube.



Aparece el cuadro de diálogo Agregar nueva programación del limitador.

2. Especifique el límite del rendimiento en MB o kB por segundo.

   Se abre la página Configuración de red de la máquina virtual en espera - <nombre de nodo>.

3. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

4. Especifique Hasta para especificar una hora de finalización para la tarea de rendimiento.

5. Haga clic en Guardar.

   Se ha especificado la programación de la limitación, la cual se muestra en la página Programación.

Configuración de la red de máquinas virtuales en espera

Se puede encender la máquina virtual en espera en AWS EC2 con valores de configuración de red personalizados. Se pueden configurar los siguientes valores de configuración de red en la máquina virtual en espera:

- Especifique la red virtual y la NIC (Tarjeta de interfaz de red) y los valores de configuración de TCP/IP para cada adaptador desde la ficha **Configuración del adaptador de red**.
- Actualice los servidores DNS para volver a dirigir a los clientes del equipo de origen a las máquinas virtuales de Virtual Standby en función de los valores de configuración de TCP/IP desde la ficha **Valores de configuración de actualización de DNS**.

Siga estos pasos:

1. En la ficha **Recursos**, vaya al grupo de nodos de **Virtual Standby**.

   Los nodos de Virtual Standby se muestran en el panel central.

2. En el panel central, seleccione el nodo y haga clic en **Configuración de red de la máquina virtual en espera**.

   Se abre la página Configuración de red de la máquina virtual en espera - <nombre de nodo>.

3. En la ficha **Configuración del adaptador de red**, seleccione la red virtual en la lista **Máquina virtual en espera - red virtual**.
4. Seleccione la subred en la lista de subredes.
5. Seleccione la dirección IP elástica en la lista **Direcciones IP elásticas**.
6. Seleccione **Personalizar los valores de configuración de TCP/IP**.
7. Haga clic en el botón **Agregar dirección** y agregue **Direcciones IP**, **Direcciones de puerta de enlace**, **Direcciones de DNS** y **Direcciones WINS**.

   Nota: Si se agregan **Direcciones de DNS**, a continuación configure los servidores DNS en la ficha **Valores de configuración de actualización de DNS**.

8. Haga clic en **Guardar**.

   Se cierra la página Configuración de red de la máquina virtual en espera - <nombre de nodo>.

   La red de máquina virtual en espera se ha configurado.

(Opcional) Ejecución manual de la tarea de Virtual Standby a EC2

Para ejecutar manualmente una tarea de Virtual Standby, se tiene que realizar primero una copia de seguridad manual. La tarea de Virtual Standby en EC2 se asocia con una tarea de copia de seguridad. Si un plan incluye una tarea de copia de seguridad y una tarea de Virtual Standby en EC2, cuando se ejecuta manualmente la tarea de copia de seguridad, la tarea de Virtual Standby se ejecuta automáticamente después de la terminación de la tarea de copia de seguridad.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Si se han agregado algunos planes, estos planes se mostrarán en el panel central.
3. Seleccione los nodos de los que desea realizar la copia de seguridad y que tienen un plan asignado.
4. En el panel central, haga clic en **Acciones**, **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo **Ejecutar ahora una copia de seguridad**.
5. Seleccione el tipo de copia de seguridad y proporcione un nombre para la tarea de copia de seguridad.
6. Haga clic en **Aceptar**.

   Se ejecuta la tarea de copia de seguridad.

   La tarea de Virtual Standby en EC2 se ejecuta inmediatamente después de que se complete la tarea de copia de seguridad.

   La tarea de Virtual Standby en EC2 se ejecuta manualmente.

Pausa y reanudación de la tarea de Virtual Standby

La conversión virtual es el proceso en el cual Virtual Standby convierte puntos de recuperación de Arcserve Unified Data Protection de los nodos de origen a formatos de máquina virtual denominados instantáneas de puntos de recuperación. En el caso de que se produzca un error en un nodo de origen, la función de Virtual Standby utiliza las instantáneas de puntos de recuperación para encender una máquina virtual para el nodo de origen.

Permitir que el proceso de conversión virtual funcione continuamente se considera una práctica recomendable. Sin embargo, si se desea pausar temporalmente el proceso de conversión virtual en servidores de Virtual Standby locales y remotos, se puede hacer desde la consola. Una vez se han corregido los problemas del nodo de origen, se puede reanudar el proceso de conversión virtual.

Cuando se ponen en pausa tareas de Virtual Standby (tareas de conversión), la operación de pausa no pondrá en pausa la tarea de conversión que está en curso actualmente. La operación de pausa se aplica solamente a la tarea que se espera que se ejecute al final de la siguiente tarea de copia de seguridad. Como resultado, la tarea de conversión siguiente no se inicia hasta que se reanuda explícitamente la tarea de conversión (en pausa).

Si se reanuda Virtual Standby para los nodos y si hay varias sesiones de copia de seguridad sin instantánea de punto de recuperación, obtendrá un cuadro de diálogo para seleccionar la opción de copia inteligente. Si se hace clic en Sí, Virtual Standby convertirá la sesión combinada en una instantánea única de punto de recuperación. Si se hace clic en No, Virtual Standby convertirá cada sesión individualmente

Nota: Opcionalmente, se pueden pausar las tareas de Virtual Standby y reanudarlas directamente desde los nodos. Para obtener más información, consulte Pausa y reanudación de tareas de pausa virtual desde los nodos.

Siga estos pasos:

1. Inicie sesión en el Arcserve Unified Data Protection.
2. Haga clic en la ficha **recursos**.
3. En el panel izquierdo, vaya a **Virtual Standby** y haga clic en **Todos los nodos**.

   Si se han agregado algunos nodos, los nodos se mostrarán en el panel central.
4. Seleccione el nodo que se desea pausar o reanudar.

5. En el panel central, haga clic en **Acciones**, **Virtual Standby**, **Pausa** o **Reanudación**.

   La función de Virtual Standby del nodo seleccionado se pausa o se reanuda.

Verificación del plan

Para verificar la función de Virtual Standby, confirme que se ha creado correctamente el plan de Virtual Standby. Después de verificar que el plan se ha creado correctamente, compruebe si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Después de que la tarea de copia de seguridad se complete correctamente, se ejecutará la tarea de Virtual Standby. Se puede comprobar el estado de la tarea de copia de seguridad y de la tarea de Virtual Standby en la ficha **tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga estos pasos para verificar las tareas de Virtual Standby:

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad y la tarea de Virtual Standby se han realizado correctamente.

   El plan de Virtual Standby se ha verificado correctamente.

   Se crea la máquina de Virtual Standby.

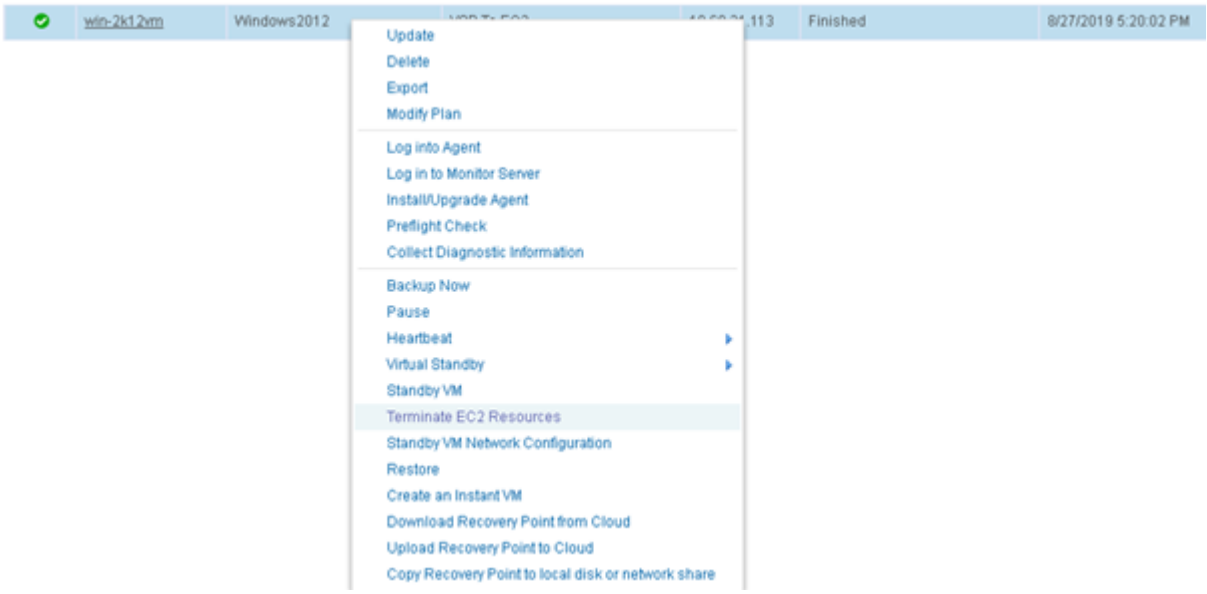
Finalización de recursos de EC2

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

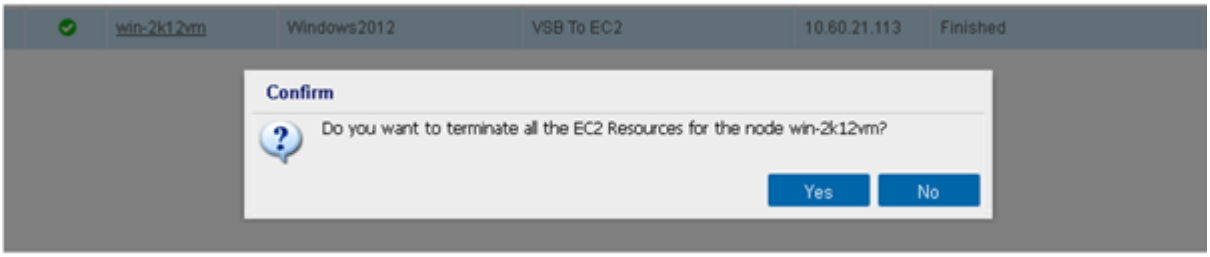
   Se muestran todos los nodos en el panel central.
3. Haga clic con el botón secundario del ratón en un nodo y seleccione Finalizar recursos de EC2.

   Se abre el cuadro de diálogo Confirmar.



4. Haga clic en **Sí** para limpiar los recursos de la nube de AWS que se generan desde la tarea de Virtual Standby a EC2. Haga clic en **No** para detener el proceso de finalización.

   Nota: Si un nodo no tiene ninguna tarea de VSB a EC2, dicho nodo no tendrá la opción Finalizar recursos de EC2.



Cómo crear un plan de Virtual Standby a Microsoft Azure

Virtual Standby convierte los puntos de recuperación a formatos de máquina virtual y prepara una instantánea para poder recuperar fácilmente los datos cuando sea necesario. Esta función también proporciona la capacidad de alta disponibilidad y garantiza que la máquina virtual puede tomar el control inmediatamente cuando se produce un error en el equipo de origen. La máquina de Virtual Standby se crea convirtiendo los puntos de recuperación en un formato de máquina virtual de Microsoft.

Nota: La tarea de Virtual Standby se ejecuta solamente si la tarea de copia de seguridad crea una instantánea del punto de recuperación válida. Si se produce un error en la tarea de copia de seguridad, se omite la tarea de Virtual Standby.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Creación de un plan con una tarea de copia de seguridad
3. Adición de una tarea de Virtual Standby a Azure
4. (Opcional) Ejecución de la tarea de Virtual Standby manualmente
5. Pausa y reanudación de latidos
6. Pausa y reanudación de la tarea de Virtual Standby
7. Verificación del plan

Revisión de las consideraciones y requisitos previos

Verifique si se han completado los requisitos previos siguientes:

- Inicie sesión en la Consola.
- Se ha instalado el componente del servidor y se han creado almacenes de datos si se desea almacenar los datos de la copia de seguridad en servidores de punto de recuperación.
- Se tiene un punto de recuperación válido para crear un equipo de Virtual Standby. Los puntos de recuperación pueden ser de una de las tareas siguientes:
  - Copia de seguridad de Windows basada en el agente
  - Copia de seguridad sin agente basada en el host
  - Replicación
  - Replicación desde un servidor de punto de recuperación remoto
- Compruebe si se cumplen los requisitos previos para agregar una cuenta de la nube a Microsoft Azure. Para obtener más información, consulte la sección Requisitos previos para agregar una cuenta de la nube a Microsoft Azure.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Creación de un plan con una tarea de copia de seguridad

Un plan incluye tipos diferentes de tareas que se desea realizar. Para crear una máquina de Virtual Standby, se crea un plan que incluye una tarea de copia de seguridad y una tarea de Virtual Standby. Una tarea de copia de seguridad realiza una copia de seguridad de los nodos de origen y almacena los datos en el destino especificado. La función de Virtual Standby utiliza a continuación estos datos de la copia de seguridad y los convierte a un formato de máquina virtual.

Para obtener más información, consulte Creación de un plan con una tarea de copia de seguridad.

Adición de una tarea de Virtual Standby al plan

Cree una tarea de Virtual Standby a Azure para que los datos de la copia de seguridad se conviertan a un formato de máquina virtual y se cree una máquina virtual. La función de Virtual Standby también controla el latido del nodo de origen para que cuando el nodo de origen esté bloqueado, la máquina virtual tome inmediatamente el control como nodo de origen.

Notas:

- Virtual Standby no puede encender automáticamente las instantáneas de punto de recuperación tomadas de nodos de máquinas virtuales basadas en host o replicados de un servidor de puntos de recuperación remoto, y el origen de la tarea de Virtual Standby es el que se replica en un sitio distinto. Se tiene que encender manualmente las instantáneas de punto de recuperación para dichos nodos.
- Si se pausa el plan, la tarea de Virtual Standby no se iniciará. Cuando se vuelva a reanudar el plan, la tarea de Virtual Standby no se reanudará automáticamente. Se tiene que ejecutar manualmente otra tarea de copia de seguridad para iniciar la tarea de Virtual Standby. También, si el plan se pausa la opción Pausar/reanudar Virtual Standby no estará disponible. Si no se desea que la máquina virtual se inicie automáticamente después de que se haya pausado el plan, se tendrá que pausar manualmente el latido para los nodos.

Siga estos pasos:

1. Haga clic en **Agregar una tarea** en el panel izquierdo.

   Una tarea nueva se agrega al panel izquierdo.

2. En el menú desplegable **Tipo de tarea** seleccione **Virtual Standby**.

   La tarea de Virtual Standby se agrega.

3. En la ficha **Origen** seleccione un origen para la tarea de Virtual Standby.

4. Haga clic en la ficha **Servidor de virtualización** e introduzca el servidor de virtualización y los detalles del servidor de control.

   Tipo de virtualización: Azure

   Tipo de virtualización

   Especifique Azure como el tipo de virtualización.

   Nombre de la cuenta

Seleccione una cuenta existente de Azure. También se puede agregar una nueva cuenta haciendo clic en **Agregar**.

Para obtener más información, consulte Cómo agregar una cuenta de la nube.

Grupo de recursos

Especifique un grupo de recursos. Debe tener un grupo de recursos en Azure.

Para obtener instrucciones, consulte Grupo de recursos en Azure en la documentación de Microsoft.

Región

Seleccione la región de Azure donde se desea que esté la máquina virtual en espera. Para obtener más información sobre la región, consulte Regiones en Azure.

Control

Especifique el nombre de host del servidor que controla el estado del servidor de origen.

Notas:

- Puede utilizar cualquier equipo físico o máquina virtual como servidor de control.
- No puede utilizar el servidor de origen de la copia de seguridad como servidor de control.
- La configuración del servidor de control no es necesaria si los nodos se replican a partir de un servidor de puntos de recuperación remoto o si el origen de la tarea de Virtual Standby es el que se replica en un sitio distinto.
- La configuración del servidor de control no es necesaria si el origen de Virtual Standby es la tarea de replicación y el servidor de puntos de replicación de destino de la replicación se encuentra en Azure.

Nombre de usuario

Especifique el nombre de usuario para iniciar sesión en el sistema de control.

Contraseña

Especifique la contraseña del nombre de usuario para iniciar sesión en el sistema de control.

Protocolo

Especifique HTTP o HTTPS como el protocolo que desea utilizar para la comunicación entre Arcserve Unified Data Protection y el servidor de control.

Puerto

Especifique el puerto que se desea utilizar para la transferencia de datos entre Arcserve Unified Data Protection y el servidor de control.

5. Haga clic en la ficha **Máquina virtual** e introduzca los detalles de los siguientes campos: Configuración básica de la máquina virtual, Almacén de datos de la máquina virtual para VMware, Ruta de la máquina virtual para Hyper-V y Red de la máquina virtual.

Prefijo del nombre de la máquina virtual

Especifique el prefijo que se desea agregar al nombre de visualización para la máquina virtual en Azure.

Valor predeterminado: UDPVM_

Instantáneas del punto de recuperación

Especifique el número de instantáneas del punto de recuperación (puntos de recuperación) para la máquina virtual en espera. El número máximo de instantáneas del punto de recuperación es de 29 para Azure.

Valor predeterminado: 5

Combinar todas las sesiones sin convertir en una instantánea de punto de recuperación única

Especifique si desea combinar todas las sesiones sin convertir en una instantánea única de punto de recuperación cuando tenga lugar la siguiente tarea de Virtual Standby programada.

Valor predeterminado: Seleccionado

Tamaño de la máquina virtual

Microsoft Azure proporciona una amplia selección de tamaños de la máquina virtual optimizados para adaptarse a distintos casos de uso. Disponen de diversas combinaciones de CPU, memoria, almacenamiento y capacidad de red. Para obtener más información sobre el tamaño de la máquina virtual y sobre cómo satisfacen sus necesidades informáticas, consulte los tamaños de la máquina virtual de Windows en Azure.

Nombre de la cuenta de almacenamiento

Seleccione un nombre de la cuenta de almacenamiento. Debe tener un nombre de la cuenta de almacenamiento en Azure. Para el tipo de cuenta de almacenamiento, seleccione Storage (Uso general v1) o StorageV2 (Uso general v2). Para obtener más información, consulte la cuenta de almacenamiento en Azure en la documentación de Microsoft.

Red virtual

Seleccione una red virtual. Debe tener una red virtual en Azure. Para obtener más información, consulte la red virtual en Azure en la documentación de Microsoft.

Subred

Seleccione una subred según la red virtual seleccionada. Debe tener una subred en Azure. Para obtener más información, consulte la subred en Azure en la documentación de Microsoft.

Grupo de seguridad de red

Seleccione un grupo de seguridad de red. Debe tener un grupo de seguridad de red en Azure. Configure las reglas del grupo de seguridad para abrir los puertos relacionados, incluido el puerto 3389 para el escritorio remoto, el puerto 8014 y el puerto 8015 para la comunicación de Arcserve UDP. Para obtener instrucciones, consulte el grupo de seguridad de red en la documentación de Microsoft.

Activar asignación automática de IP pública

Cuando se activa la asignación automática de IP pública, la dirección IP pública se asignará automáticamente a la máquina virtual en espera cuando se inicia en Azure.

6. Haga clic en la ficha **Avanzada** y proporcione los detalles siguientes:

Iniciar automáticamente la máquina virtual

Especifique si se desea iniciar la máquina virtual automáticamente.

Nota: Esta opción no se encuentra disponible para nodos de máquinas virtuales basadas en el host ni para nodos replicados desde un servidor de puntos de recuperación remoto, y el origen de la tarea de Virtual Standby es el que se replica en un sitio distinto. El origen de Virtual Standby es la tarea de replicación y el servidor de puntos de recuperación de destino de la replicación en Azure.

Tiempo de espera

Especifique el tiempo que el servidor de control debe esperar a un latido antes de encender una instantánea de punto de recuperación.

Frecuencia

Especifique la frecuencia con la que el servidor de origen comunica latidos al servidor de control.

Ejemplo: el valor de Tiempo de espera especificado es 60. El valor de Frecuencia especificado es 10. El servidor de origen comunicará los latidos en intervalos de 10 segundos. Si el servidor de control no detecta ningún latido en 60

segundos desde el último latido detectado, el servidor de controlador enciende una máquina virtual mediante la última instantánea de punto de recuperación.

Personalizar los parámetros de la tarea

Se pueden personalizar los parámetros de la tarea para las siguientes opciones:

- *Número de subprocesos que se cargan para cada tarea*: Valor predeterminado: 4
- *Tamaño del búfer para cada subproceso*: Valor predeterminado: 4096 kB

Activar Alertas de correo electrónico

Le permite recibir alertas de correo electrónico en función de los valores de configuración que se proporcionan. Cuando se selecciona esta opción, se activan otras categorías de alertas de correo electrónico para su selección.

- **Falta el latido del equipo de origen**: Virtual Standby envía notificaciones de alerta cuando el servidor de control no detecta el latido del servidor de origen.

  Nota: Esta opción no está disponible para los nodos de Replicación desde un servidor de puntos de recuperación remoto o si el origen de la tarea de Virtual Standby es el que se va a replicar en un sitio distinto.

- **Máquina virtual encendida para el equipo de origen configurado con encendido automático**: Virtual Standby envía notificaciones de alerta cuando enciende una máquina virtual que está configurada para el encendido automático en el caso de que no se detecte el latido.

  Nota: Esta opción no está disponible para los nodos de Replicación desde un servidor de puntos de recuperación remoto o si el origen de la tarea de Virtual Standby es el que se va a replicar en un sitio distinto. Esta opción tampoco no está disponible para los nodos de máquina virtual basada en el host.

- **Máquina virtual encendida para el equipo de origen configurado con encendido manual**: Virtual Standby envía notificaciones de alerta cuando enciende manualmente una máquina virtual.
- **Errores/bloqueo de Virtual Standby**: Virtual Standby envía notificaciones de alerta cuando detecta que se ha producido un error durante el proceso de conversión.
- **Virtual Standby correcto**: Virtual Standby envía notificaciones de alerta cuando detecta que una máquina virtual se enciende correctamente.
- **Virtual Standby no se ha iniciado correctamente desde la instantánea del punto de recuperación**: Virtual Standby envía notificaciones de alerta cuando detecta que una máquina virtual no se ha encendido automáticamente y se

encuentra especificada la opción de recuperación local Iniciar automáticamente la máquina virtual.

7. Haga clic en **Guardar**.

   Los cambios se guardan y la tarea de Virtual Standby se implementa automáticamente en el servidor de Virtual Standby.

   Nota: Una vez finalizada la tarea de Virtual Standby, se crea el volumen de la máquina virtual en espera. La máquina virtual en espera solo se crea después de la máquina virtual se encienda desde Arcserve UDP.

   Se ha creado e implementado correctamente Virtual Standby al plan de Azure.

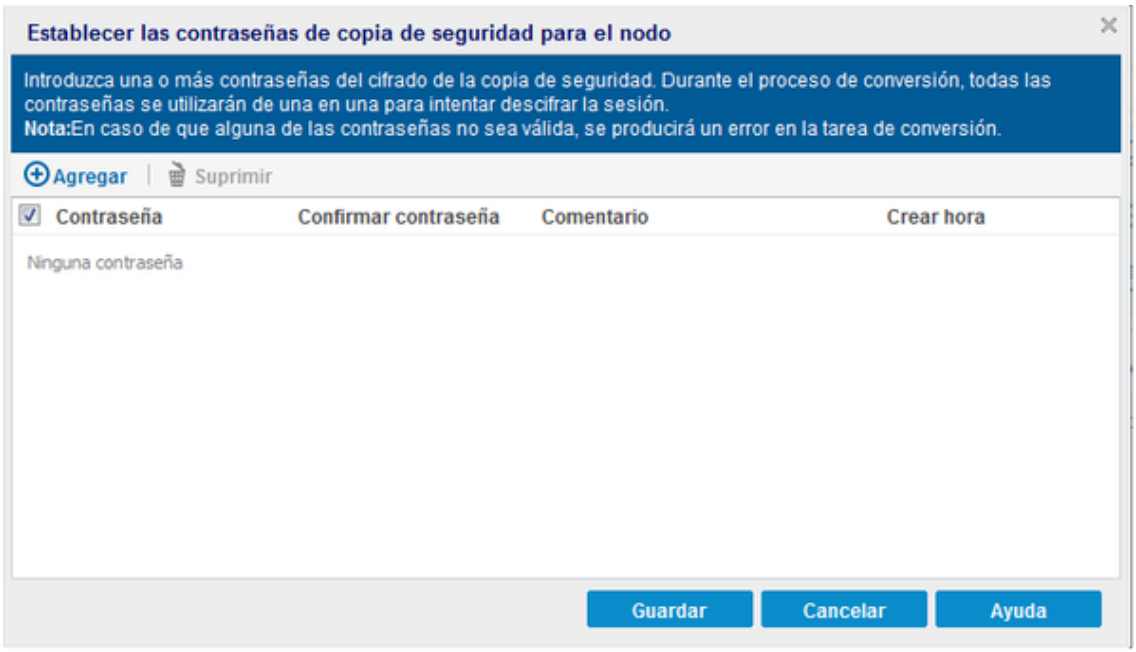
Cómo establecer las contraseñas de copia de seguridad para uno o más nodos

Para garantizar que el conversor pueda convertir los puntos de recuperación replicados, Virtual Standby permite especificar las contraseñas de la copia de seguridad de los datos que el conversor pueda utilizar para convertir los datos.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.
3. En el panel central, haga clic con el botón secundario del ratón en el nodo y haga clic en **Establecer contraseñas de la copia de seguridad**.

   Aparecerá el cuadro de diálogo **Establecer las contraseñas de copia de seguridad para el nodo**.

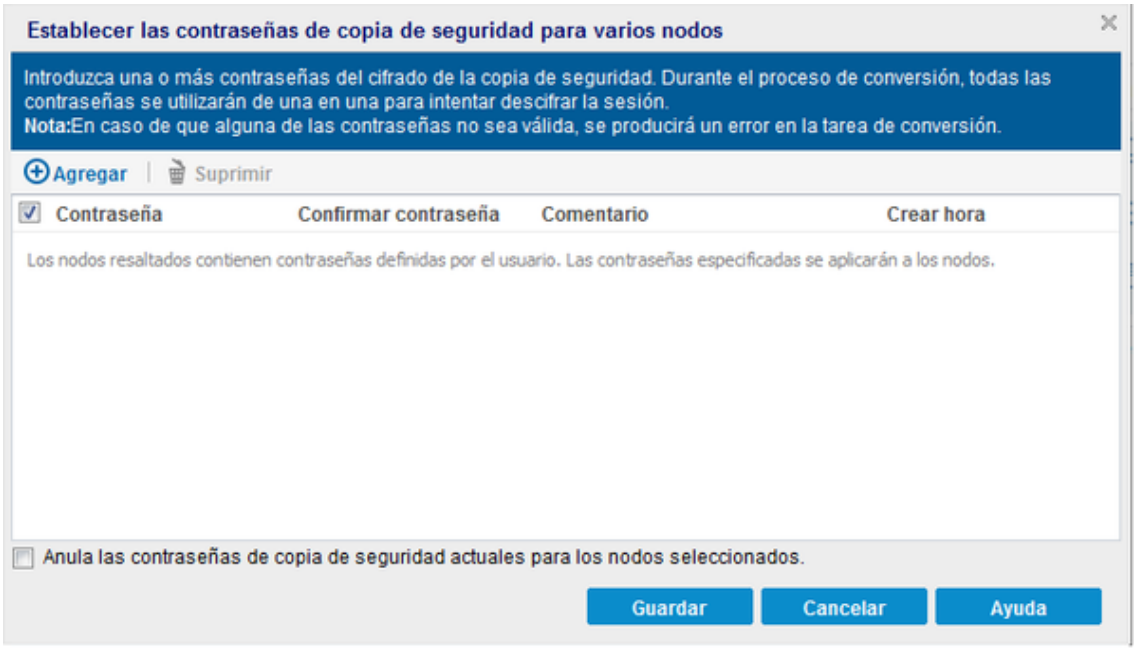


4. Realice las tareas siguientes en el cuadro de diálogo **Establecer contraseñas de la copia de seguridad** para uno o más nodos:

   Agregar: haga clic en **Agregar** para agregar una o más contraseñas de copia de seguridad a los nodos seleccionados.

   Suprimir:haga clic en **Suprimir** para suprimir una o más contraseñas de copia de seguridad de los nodos seleccionados.

Nota: Se pueden anular las contraseñas de copia de seguridad actuales para varios nodos seleccionando la casilla de verificación **Anula las contraseñas de copia de seguridad actuales para los nodos seleccionados**.



5. Haga clic en **Guardar**.

   El cuadro de diálogo desaparece y las contraseñas de copia de seguridad se establecen para los nodos remotos seleccionados.

(Opcional) Ejecución de la tarea de Virtual Standby manualmente

Para ejecutar manualmente una tarea de Virtual Standby, se tiene que realizar primero una copia de seguridad manual. La tarea de Virtual Standby se asocia con una tarea de copia de seguridad. Si un plan incluye una tarea de copia de seguridad y una tarea de Virtual Standby y se ejecuta manualmente la tarea de copia de seguridad, la tarea de Virtual Standby se ejecuta automáticamente después de la terminación de la tarea de copia de seguridad.

Siga estos pasos:

1. Haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Muestra los planes que se han agregado.
3. Seleccione los nodos que de los que desea realizar la copia de seguridad. El nodo seleccionado debe tener asignado un plan.
4. En el panel central, haga clic en **Acciones**, **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo **Ejecutar ahora una copia de seguridad**.
5. Seleccione el tipo de copia de seguridad y proporcione un nombre para la tarea de copia de seguridad.
6. Haga clic en **Aceptar**.

   Se ejecuta la tarea de copia de seguridad.

   La tarea de Virtual Standby se ejecuta inmediatamente después de que se complete la tarea de copia de seguridad.

   La tarea de Virtual Standby se ejecuta manualmente.

Pausa y reanudación de latidos

La solución Arcserve Unified Data Protection permite pausar y reanudar los latidos detectados por el servidor de control. El latido es el proceso a través del cual el servidor de origen y el servidor de control comunican el estado del servidor de origen. Si el servidor de control no detecta ningún latido tras un período de tiempo especificado, la función de Virtual Standby puede aprovisionar la máquina virtual para que funcione como el nodo de origen.

Ejemplos: cuándo pausar o reanudar los latidos

Los ejemplos siguientes describen cuándo pausar y reanudar los latidos:

- Pause el latido cuando desee dejar sin conexión un nodo (servidor de origen) por motivos de mantenimiento.
- Reanude el latido cuando hayan finalizado las tareas de mantenimiento y el nodo (servidor de origen) esté en línea.

Tenga en cuenta el siguiente comportamiento:

- Se pueden pausar y reanudar los latidos a nivel del grupo o a nivel del nodo individual.
- Se pueden pausar y reanudar los latidos para uno o varios nodos en un paso.
- La solución Arcserve Unified Data Protection
- Cuando se actualizan las instalaciones del Agente en los nodos de origen, Arcserve Unified Data Protection Para asegurarse de que los servidores de control controlen los nodos actualizados, reinicie el latido de los nodos una vez que se hayan completado las actualizaciones de los nodos.

Siga estos pasos:

1. Inicie sesión en el Arcserve Unified Data Protection.
2. Haga clic en la ficha **recursos**.
3. En el panel izquierdo, vaya a **Virtual Standby** y haga clic en **Todos los nodos**.

   Si se han agregado algunos nodos, los nodos se mostrarán en el panel central.
4. Seleccione el nodo que se desea pausar o reanudar.
5. En el panel central, haga clic en **Acciones**, **Latido**, **Pausa** o **Reanudación**.

   El latido del nodo seleccionado se pausa o se reanuda.

Pausa y reanudación de la tarea de Virtual Standby

La conversión virtual es el proceso en el cual Virtual Standby convierte puntos de recuperación de Arcserve Unified Data Protection de los nodos de origen a formatos de máquina virtual denominados instantáneas de puntos de recuperación. En el caso de que se produzca un error en un nodo de origen, la función de Virtual Standby utiliza las instantáneas de puntos de recuperación para encender una máquina virtual para el nodo de origen.

Permitir que el proceso de conversión virtual funcione continuamente se considera una práctica recomendable. Sin embargo, si se desea pausar temporalmente el proceso de conversión virtual en servidores de Virtual Standby locales y remotos, se puede hacer desde la consola. Una vez se han corregido los problemas del nodo de origen, se puede reanudar el proceso de conversión virtual.

Cuando se ponen en pausa tareas de Virtual Standby (tareas de conversión), la operación de pausa no pondrá en pausa la tarea de conversión que está en curso actualmente. La operación de pausa se aplica solamente a la tarea que se espera que se ejecute al final de la siguiente tarea de copia de seguridad. Como resultado, la tarea de conversión siguiente no se inicia hasta que se reanuda explícitamente la tarea de conversión (en pausa).

Si se reanuda Virtual Standby para los nodos y si hay varias sesiones de copia de seguridad sin instantánea de punto de recuperación, obtendrá un cuadro de diálogo para seleccionar la opción de copia inteligente. Si se hace clic en Sí, Virtual Standby convertirá la sesión combinada en una instantánea única de punto de recuperación. Si se hace clic en No, Virtual Standby convertirá cada sesión individualmente

Nota: Opcionalmente, se pueden pausar las tareas de Virtual Standby y reanudarlas directamente desde los nodos. Para obtener más información, consulte Pausa y reanudación de tareas de pausa virtual desde los nodos.

Siga estos pasos:

1. Inicie sesión en el Arcserve Unified Data Protection.
2. Haga clic en la ficha **recursos**.
3. En el panel izquierdo, vaya a **Virtual Standby** y haga clic en **Todos los nodos**.

   Si se han agregado algunos nodos, los nodos se mostrarán en el panel central.
4. Seleccione el nodo que se desea pausar o reanudar.

5. En el panel central, haga clic en **Acciones**, **Virtual Standby**, **Pausa** o **Reanudación**.

   La función de Virtual Standby del nodo seleccionado se pausa o se reanuda.

Verificación del plan

Para verificar la función de Virtual Standby, confirme que se ha creado correctamente el plan de Virtual Standby. Después de verificar que el plan se ha creado correctamente, compruebe si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Después de que la tarea de copia de seguridad se complete correctamente, se ejecutará la tarea de Virtual Standby. Se puede comprobar el estado de la tarea de copia de seguridad y de la tarea de Virtual Standby en la ficha **tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga estos pasos para verificar las tareas de Virtual Standby:

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad y la tarea de Virtual Standby se han realizado correctamente.

   El plan de Virtual Standby se ha verificado correctamente.

   Se crea la máquina de Virtual Standby.

Cómo crear un plan de Virtual Standby

Virtual Standby convierte los puntos de recuperación a formatos de máquina virtual y prepara una instantánea para poder recuperar fácilmente los datos cuando sea necesario. Esta función también proporciona la capacidad de alta disponibilidad y garantiza que la máquina virtual puede tomar el control inmediatamente cuando se produce un error en el equipo de origen. La máquina de Virtual Standby se crea convirtiendo los puntos de recuperación a un formato de máquina virtual de VMware o de Hyper-V.

Nota: La tarea de Virtual Standby se ejecuta solamente si la tarea de copia de seguridad crea una instantánea del punto de recuperación válida. Si se produce un error en la tarea de copia de seguridad, se omite la tarea de Virtual Standby.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Creación de un plan con una tarea de copia de seguridad
3. Adición de una tarea de Virtual Standby al plan
4. (Opcional) Ejecución de la tarea de Virtual Standby manualmente
5. Pausa y reanudación de latidos
6. Pausa y reanudación de la tarea de Virtual Standby
7. Verificación del plan

Revisión de las consideraciones y requisitos previos

Verifique si se han completado los requisitos previos siguientes:

- Inicie sesión en la Consola.
- Se ha instalado el componente del servidor y se han creado almacenes de datos si se desea almacenar los datos de la copia de seguridad en servidores de punto de recuperación.
- Se tiene un punto de recuperación válido para crear un equipo de Virtual Standby. Los puntos de recuperación pueden ser de una de las tareas siguientes:
  - Copia de seguridad de Windows basada en el agente
  - Copia de seguridad sin agente basada en el host
  - Replicación
  - Replicación desde un servidor de punto de recuperación remoto
- Realice una copia de seguridad de todo el equipo para activar la tarea de Virtual Standby. Si la copia de seguridad no es completa, no se puede crear una tarea de Virtual Standby.
- Compruebe si se tienen los permisos mínimos para realizar las tareas de Virtual Standbay necesarias. Para obtener más información, consulte Permisos mínimos de VMware necesarios para las tareas de VSB.
- Virtual Standby no es compatible con los orígenes de Linux. Para ver una lista de los sistemas operativos, las bases de datos y los exploradores compatibles, consulte la Matriz de compatibilidad.

Consideraciones:

- Virtual Standby utiliza discos con aprovisionamiento fino para vSphere.
- Virtual Standby utiliza los discos duros virtuales con expansión dinámica para Hyper-v.
- VMware utiliza un equipo independiente para el servidor de control con el agente instalado.
- Hyper-v actúa como servidor de control con el agente instalado.

Nota: Como práctica recomendada, se recomienda excluir archivos del análisis del antivirus para asegurarse de que Virtual Standby funciona correctamente. Para obtener más información, consulte Exclusión de archivos de la exploración de antivirus.

Permisos mínimos necesarios para las tareas de VSB

La tabla muestra la lista de permisos mínimos necesarios para realizar todas las tareas de Virtual Standby.

Nota: Los permisos globales se establecen en el nivel de vCenter.

Tareas	Permiso
Almacén de datos	Allocate space
	Explorar el almacén de datos
	Low level file operations
Global	Desactivar métodos
	Activar métodos
	Licencias
Host > Configuración	Configuración de la partición de alma-cenamiento
Red	Asignar red
Recurso	Asignar la máquina virtual a la agrupación de recursos
Máquina virtual > Configuración	Agregar disco existente
	Agregar disco nuevo
	Agregar o eliminar dispositivo
	Avanzado
	Cambiar número de CPU
	Seguimiento de cambios de disco
	Memoria
Máquina virtual > Interacción	Apagar
	Encender
	Interacción de la consola
Máquina virtual > Inventario	Crear a partir de existente
	Crear nuevo
	Eliminar
Máquina virtual > Aprovisionamiento	Permitir el acceso de disco
	Permitir el acceso de solo lectura al disco
	Permitir la descarga de la máquina virtual
Máquina virtual > Gestión de las ins-tantáneas	Crear instantáneas
	Eliminar instantáneas
	Revertir a instantánea

Creación de un plan con una tarea de copia de seguridad

Un plan incluye tipos diferentes de tareas que se desea realizar. Para crear una máquina de Virtual Standby, se crea un plan que incluye una tarea de copia de seguridad y una tarea de Virtual Standby. Una tarea de copia de seguridad realiza una copia de seguridad de los nodos de origen y almacena los datos en el destino especificado. La función de Virtual Standby utiliza los datos de la copia de seguridad y los convierte a un formato de máquina virtual.

Se puede crear una máquina de Virtual Standby a partir de una copia de seguridad de Windows basada en el agente o a partir de una copia de seguridad sin agente basada en el host. Se puede crear también una máquina de Virtual Standby a partir de datos que se replican mediante la tarea **Replicar.** El procedimiento siguiente es un ejemplo para crear una copia de seguridad de Windows basada en el agente.

Notas:

- Para obtener más información sobre la copia de seguridad sin agente basada en el host, consulte Cómo crear un plan de copia de seguridad de máquina virtual basada en el host.
- Para obtener más información sobre cómo replicar los datos de una copia de seguridad, consulte Cómo replicar datos entre almacenes de datos gestionados desde una Consola de UDP y gestionados desde Consolas de UDP diferentes.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán.

Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.

6. En la lista desplegable **Tipo de tarea** seleccione **Copia de Seguridad, Windows basado en el agente**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

La página Origen le permite especificar los nodos de origen que se desean proteger. Se pueden seleccionar más de un nodo del plan. Si no se ha agregado ningún nodo a la consola, se podrán agregar nodos al crear o modificar un plan en la página Origen. Se puede guardar un plan sin agregar ningún nodo de origen. El plan se implementa solamente después de agregar nodos de origen.

Siga estos pasos:

1. En la ficha Origen, haga clic en **Agregar**.
2. Seleccione una de las opciones siguientes:

   Seleccionar los nodos para proteger en Arcserve UDP

   Abre el cuadro de diálogo Seleccionar los nodos para proteger en Arcserve UDP. Seleccione los nodos de la lista que se muestra. Seleccione esta opción si ya se han agregado los nodos a la consola.

   Agregar nodo de Windows

   Se abre el cuadro de diálogo Agregar nodos a un plan. Seleccione esta opción si no se han agregado los nodos y desea agregarlos manualmente para la protección.

   Detectar nodos desde Active Directory

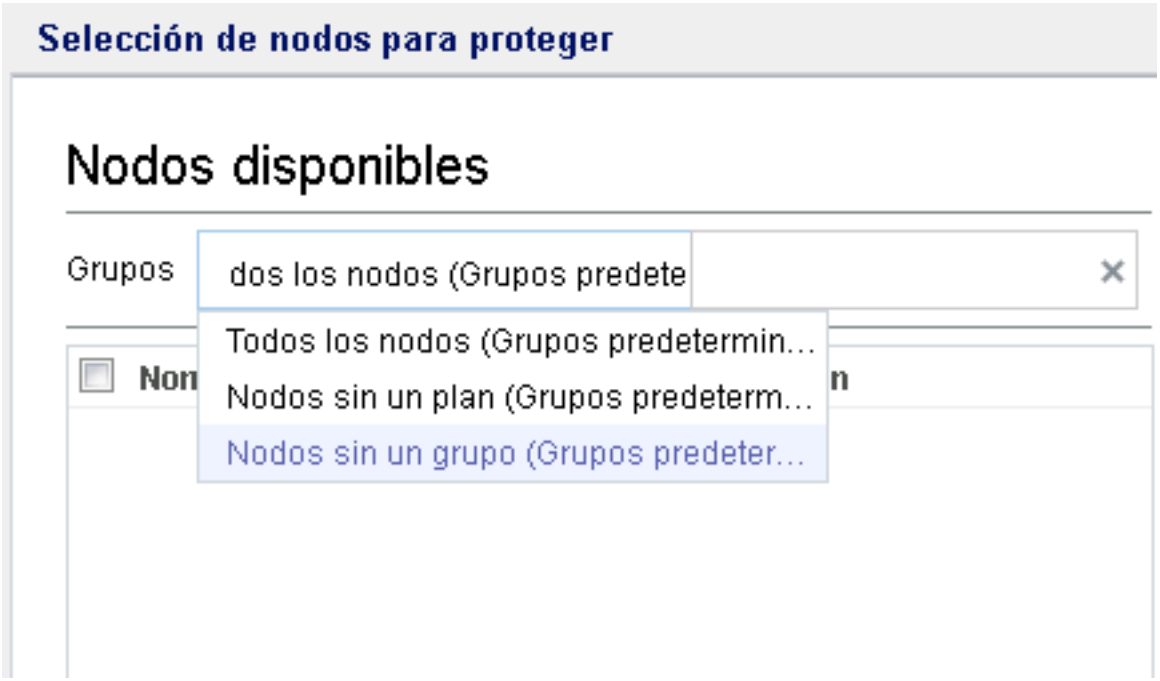
   Se abre el cuadro de diálogo Agregar nodos a la Consola de Arcserve UDP. Seleccione esta opción si desea detectar y agregar nodos en Active Directory.
3. Si ha seleccionado la opción **Seleccionar nodos para proteger en Arcserve UDP**, haga lo siguiente en el cuadro de diálogo Seleccionar nodos para proteger:
   a. (Opcional) Seleccione un filtro en la lista desplegable Grupos para filtrar nodos. Se pueden especificar palabras clave para filtrar más detalladamente los nodos.

      Los nodos se muestran en la columna Nodos disponibles.

   b. Seleccione los nodos en la columna Nodos disponibles y, a continuación, haga clic en la flecha simple hacia la derecha (>) o en la flecha doble hacia la derecha (>>) para mover los nodos seleccionados o todos los nodos respectivamente a la columna Nodos seleccionados.

      Los nodos se muestran en la columna Nodos seleccionados.

   c. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.



4. Para elegir el Tipo de El Protección, seleccione una de las opciones siguientes:

   Realizar copia de seguridad de todos los volúmenes

   Prepara una instantánea de copia de seguridad de todos los volúmenes.

   Realizar copia de seguridad de los volúmenes seleccionados

   Prepara una instantánea de copia de seguridad del volumen seleccionado.

   Se especifica el origen.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Seleccione uno de los siguientes **Tipos de destino**:

   Disco local o carpeta compartida

   Especifica que el destino de la copia de seguridad es un destino local o una carpeta compartida. Si se selecciona esta opción, se pueden guardar datos como puntos de recuperación o como conjuntos de recuperación. Las opciones Puntos de recuperación y Conjuntos de recuperación están disponibles en la ficha **Programación**.

   Servidor de puntos de recuperación de Arcserve UDP

   Especifica que el destino de la copia de seguridad es un servidor de punto de recuperación. Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.

2. Si se ha seleccionado **Servidor de punto de recuperación de Arcserve UDP**, se deben proporcionar los detalles siguientes:
   a. Seleccione un servidor de punto de recuperación.
   b. Seleccione un almacén de datos. La lista muestra todos los almacenes de datos que se han creado en el servidor de punto de recuperación especificado.
   c. Proporcione una contraseña de la sesión.
   d. Confirme la contraseña de la sesión.

3. Si ha seleccionado **Disco local o carpeta compartida**, a continuación proporcione los detalles siguientes:
   a. Proporcione la ruta completa del destino local o de red. Para el destino de la red, especifique las credenciales con acceso de escritura.
   b. Seleccione el algoritmo de cifrado. Para obtener más información, consulte Configuración de cifrado.
   c. Opcionalmente, proporcione una contraseña de cifrado.
   d. Confirme la contraseña de cifrado.

e. Seleccione un tipo de compresión. Para obtener más información, consulte Tipo de compresión.

Nota: Si se almacenan los datos a un disco local o a una carpeta compartida, no se pueden replicar los datos a otro servidor de punto de recuperación. Se es compatible con la replicación solamente si se almacenan los datos en un servidor de punto de recuperación.

Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y se pueden proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

Siga estos pasos:

1. (Opcional) Seleccione la opción para gestionar puntos de recuperación. Esta opción solo está visible si se ha seleccionado la carpeta local o compartida como destino de la copia de seguridad.

   Retener por puntos de recuperación

   Los datos de la copia de seguridad se almacenan como puntos de recuperación.

   Retener por conjuntos de recuperación

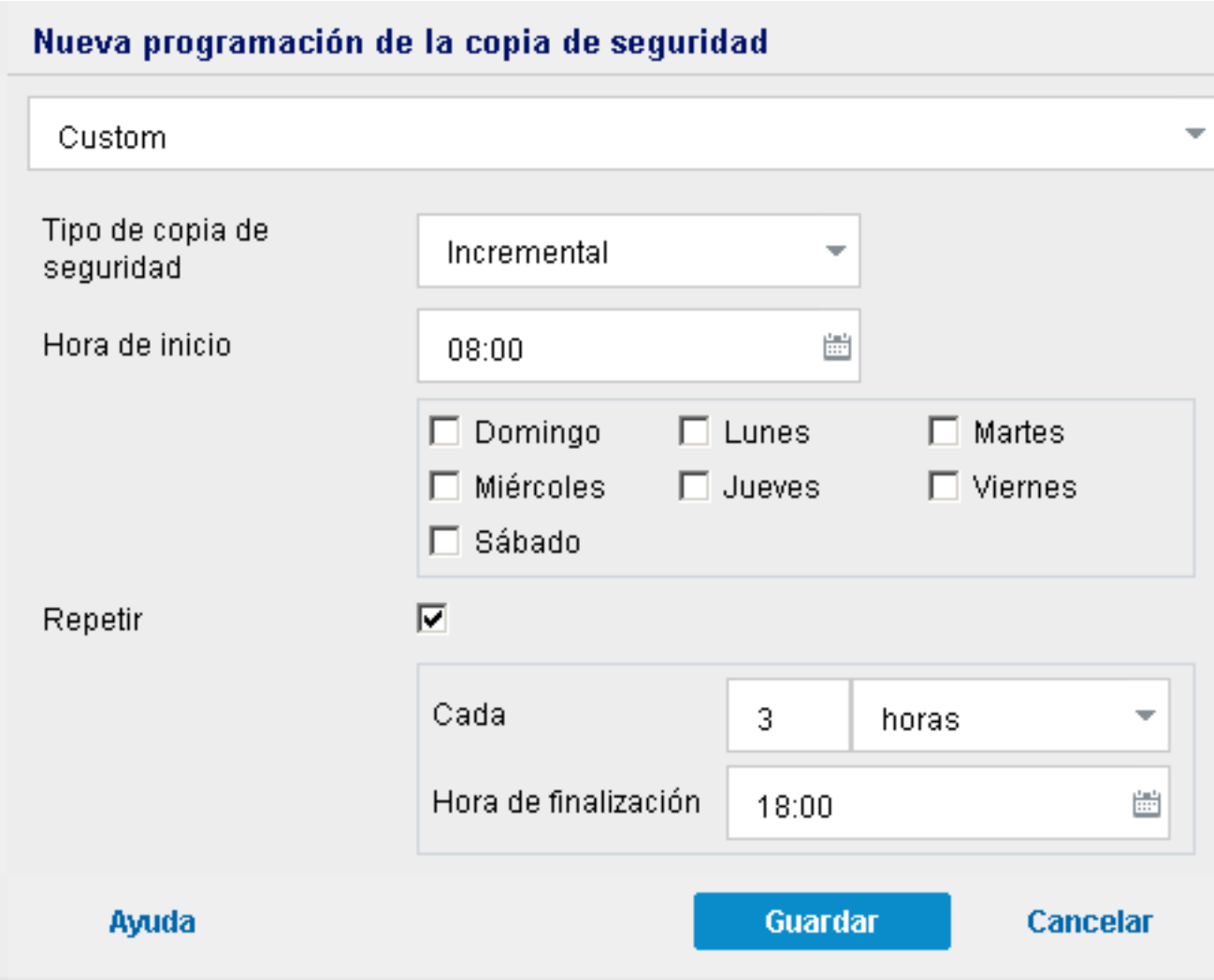
   Los datos de la copia de seguridad se almacenan como conjuntos de recuperación.

2. Agregue las programaciones de la copia de seguridad, de la combinación y del regulador.

   Agregar programación de la copia de seguridad

   a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

      Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Verificar

Especifica la programación de la copia de seguridad para las copias de seguridad de verificación.

Arcserve UDP verifica que los datos protegidos sean válidos y estén completos mediante una comprobación de confianza de la imagen de copia de seguridad almacenada en el origen de la copia de seguridad. Si es necesario, volverá a sincronizar la imagen. Una copia de seguridad de verificación se fijará en la copia de seguridad más reciente de cada bloque individual y comparará el contenido y la información con la de origen. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad de un bloque no coincide con la del origen (posiblemente por cambios en el sistema desde la última copia de seguridad), Arcserve UDP actualiza (resincroniza) la copia de seguridad del bloque que no coincide. Se puede utilizar también una copia de seguridad de verificación (aunque poco frecuentemente) para obtener la garantía de copia de seguridad completa sin utilizar el espacio necesario para una copia de seguridad completa.

Ventajas: produce una pequeña imagen de copia de seguridad si se compara con la copia de seguridad completa porque solamente se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventajas: el tiempo durante el cual se realiza la copia de seguridad es considerable puesto que todos los bloques de origen se comparan con los bloques de la última copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

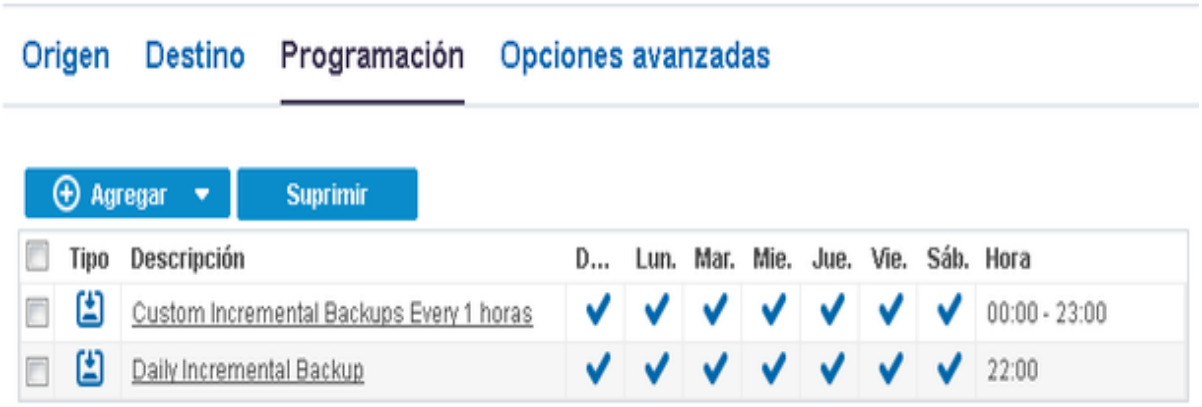
Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en Agregar y seleccione Agregar programación de la combinación.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

b. Especifique la hora de inicio para iniciar la tarea de combinación.

c. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

d. Haga clic en **Guardar**.

La Programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

   Se abre el cuadro de diálogo Agregar nueva programación del limitador.

b. Especifique el límite de rendimiento en MB por minuto.

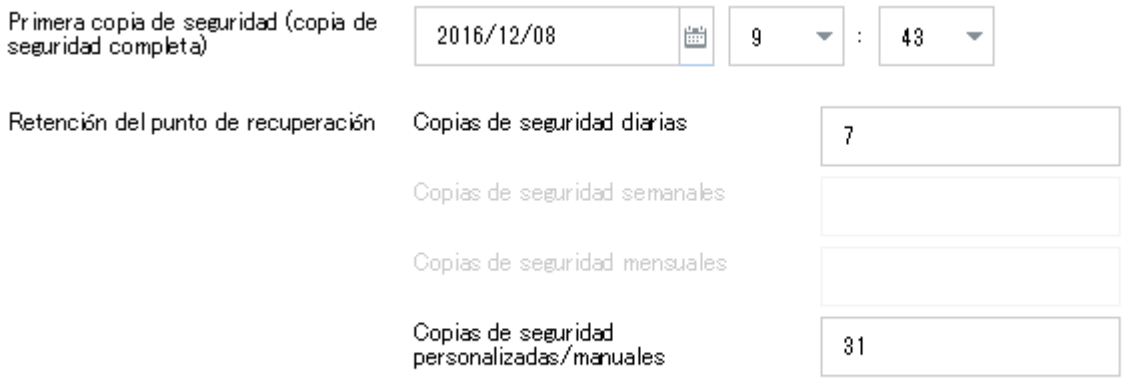
c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

   La programación del limitador se especifica y se muestra en la página **Programación**.

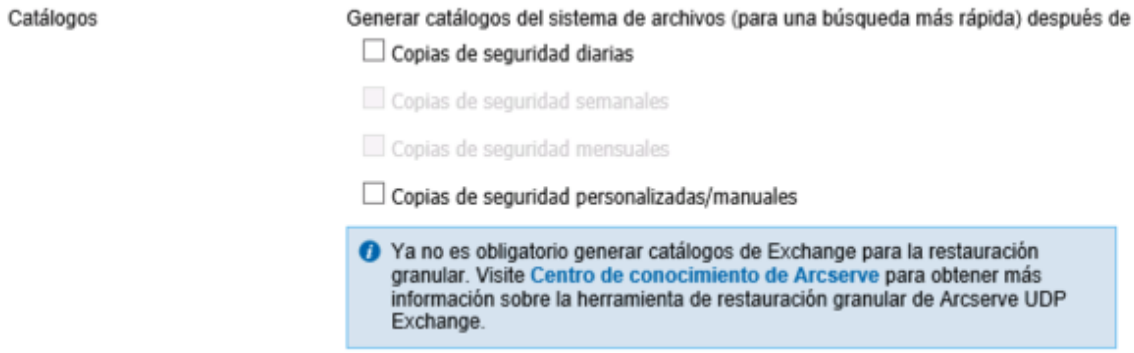
3. Especifique la hora de inicio para la copia de seguridad programada.



4. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

   Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo Programación de la copia de seguridad.

5. Especifique los detalles del catálogo.



Los catálogos permiten generar el catálogo del sistema de archivos. El catálogo del sistema de archivos se requiere para realizar la mejor búsqueda de la forma más rápida. Si se seleccionan las casillas de verificación del catálogo, los catálogos se activan en función del tipo de copia de seguridad especificada. Desactive la casilla de verificación para desactivar la generación del catálogo.

Se especifica la programación.

Funcionamiento de la programación avanzada y de la retención

La opción de programación le permite especificar una programación personalizada, una programación diaria/semanal/mensual o ambas. En la programación personalizada, se puede configurar la programación de la copia de seguridad durante cada día de la semana y se pueden agregar hasta cuatro programaciones de copia de seguridad cada día. Se puede seleccionar un día específico de una semana y crear un período de tiempo para definir cuando se desea ejecutar la copia de seguridad y con qué frecuencia.

Programación	Tarea compatible	Comentarios
Copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para ejecutar las tareas de copia de seguridad.
Regulación de la copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para controlar la velocidad de la copia de seguridad.
Combinar	Tarea de combinación	Defina cuando se deben ejecutar las tareas de combinación.
Programación diaria	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad diarias.
Programación semanal	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad semanales.
Programación mensual	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad mensuales.

Se pueden especificar también los valores de configuración de retención para los puntos de recuperación.

Nota: Establezca la configuración de la retención en cada plan para controlar cómo se retienen los datos para los nodos asignados a ese plan en el almacén de datos de destino.

Las programaciones para las copias de seguridad diarias/semanales/mensuales son independientes de la programación personalizada y de las unas a las otras. Se puede configurar solamente ejecutar una copia de seguridad diaria, una copia de seguridad semanal o una copia de seguridad mensual sin configurar la programación personalizada.

Programación de la tarea de copia de seguridad

Se pueden agregar cuatro períodos de tiempo por día en la programación de la copia de seguridad. Un período de tiempo válido es desde las 12:00 horas hasta las 23:59 horas. No se puede especificar un período de tiempo como, por

ejemplo, de las 18:00 horas a las 06:00 horas. En tales casos, se debe especificar manualmente dos períodos de tiempo diferentes.

Para cada período de tiempo, la hora de inicio está incluida y, en cambio, no se incluye la hora de finalización. Por ejemplo, se ha configurado ejecutar una copia de seguridad incremental ejecutada todas las horas entre las 06:00 horas y las 09:00 horas y la copia de seguridad se iniciará a las 06:00 horas. Esto significa que la copia de seguridad se ejecuta a las 06:00 horas, a las 07:00 horas y a las 08:00 horas, pero NO a las 09:00 horas.

Nota: Si desea ejecutar la tarea de copia de seguridad reiteradamente hasta el final del día, configure la programación hasta las 12:00 horas. Por ejemplo, para ejecutar la tarea de copia de seguridad cada 15 minutos durante todo el día, configure la programación de las 12:00 a las 12:00, cada 15 minutos.

Programación del regulador de la copia de seguridad

La programación del regulador de la copia de seguridad le permite controlar la velocidad del rendimiento de la copia de seguridad, que a su vez controla el uso de recursos (E/S del disco, CPU, ancho de banda de la red) del servidor del que se está realizando la copia de seguridad. Esto es útil si no se desea afectar al rendimiento del servidor durante el horario comercial. Se pueden agregar cuatro períodos de tiempo por día en la programación del regulador de la copia de seguridad. Para cada período de tiempo, se puede especificar un valor en MB por minuto. Este valor se utiliza para controlar el rendimiento de la copia de seguridad. Los valores válidos van desde 1 MB/minuto a 99999 MB/minuto.

Si una tarea de copia de seguridad excede el tiempo especificado, el límite del regulador se ajusta según el período de tiempo especificado. Por ejemplo, se ha definido el límite del regulador de la copia de seguridad en 500 MB/minuto desde las 08:00 horas a las 20:00 horas y en 2500 MB/minuto de las 20:00 horas a las 22:00 horas. Si una tarea de copia de seguridad se inicia a las 19:00 horas y se ejecuta durante tres horas, el límite del regulador es de 500 MB/minuto de las 19:00 horas a las 20:00 horas y de 2500 MB/minuto de las 20:00 horas a las 22:00 horas.

Si no se define ninguna programación de la copia de seguridad ni ninguna programación del rendimiento de la copia de seguridad, la copia de seguridad se ejecuta tan deprisa como pueda.

Programación de la combinación

Le permite combinar puntos de recuperación basándose en la programación proporcionada.

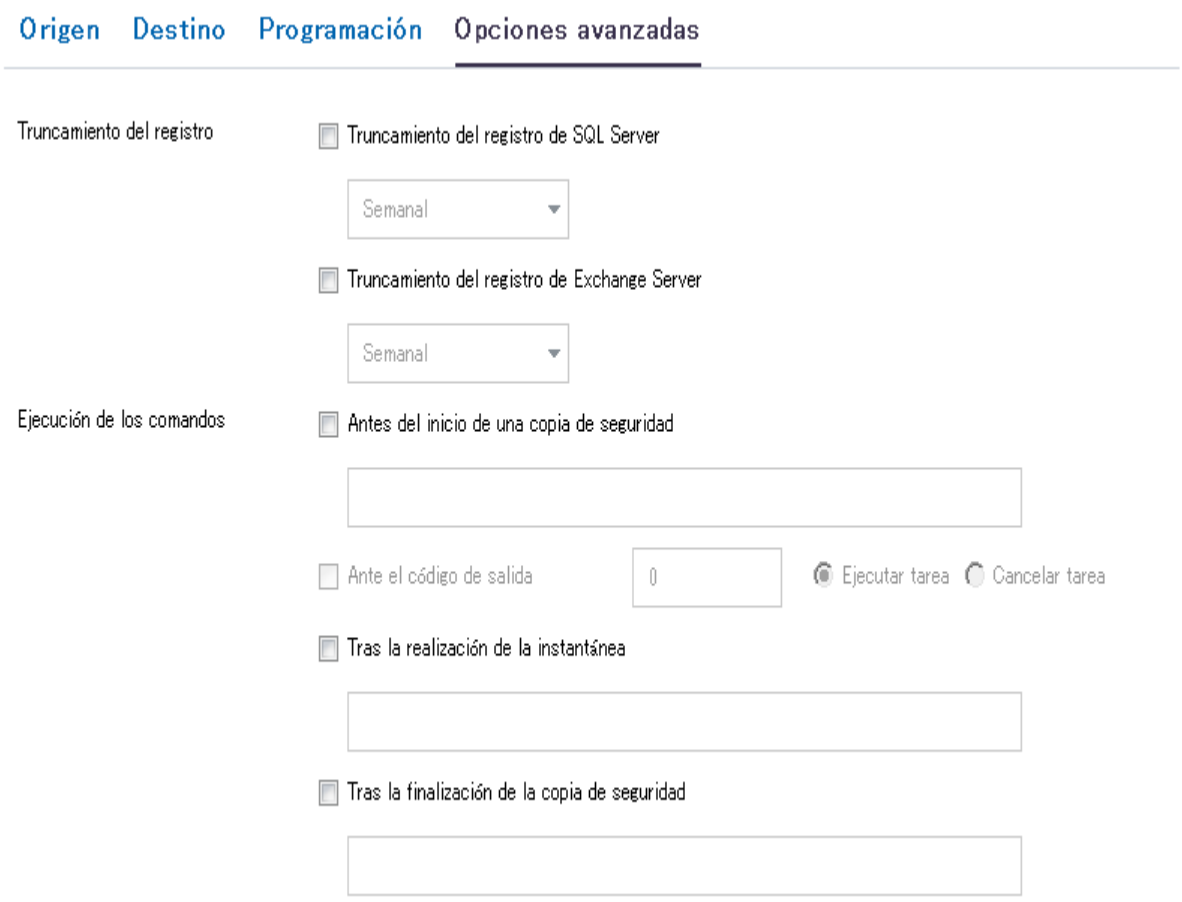
Tenga en cuenta los puntos siguientes para la tarea de combinación:

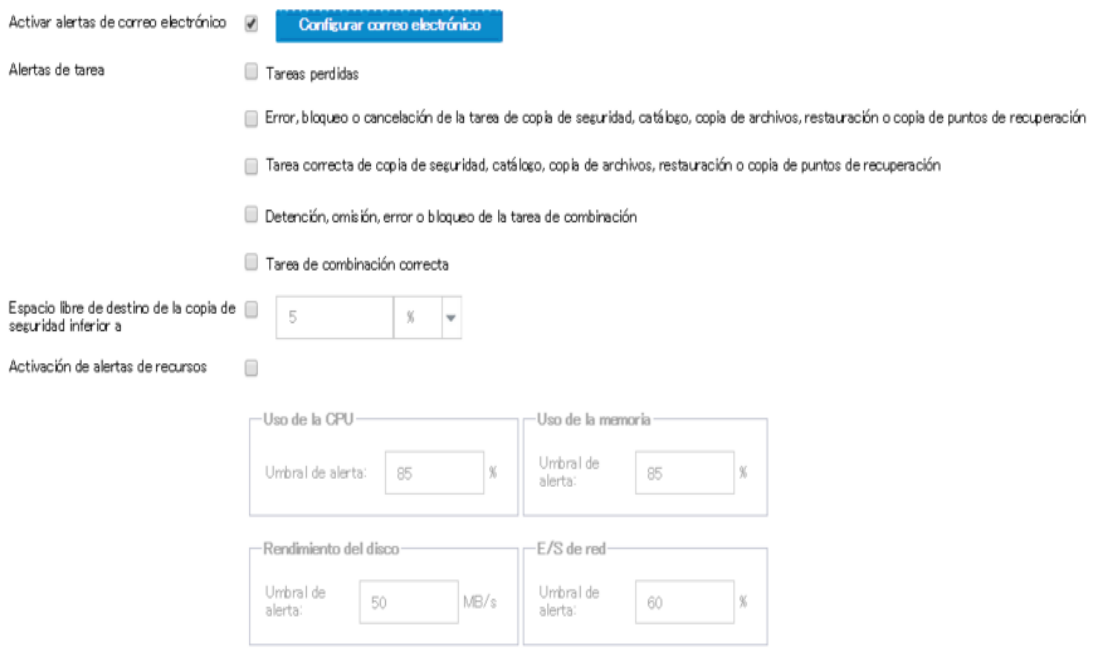
- Solamente una tarea de combinación puede ejecutarse para un nodo en cualquier momento proporcionado.
- Si se inicia una tarea de combinación, se tiene que completar antes de que la siguiente tarea de combinación se pueda iniciar. Esto no significa que, si uno o más conjuntos de puntos de recuperación se combinan, no se pueda agregar un punto de recuperación nuevo a este proceso de combinación hasta que el proceso de combinación del conjunto actual de puntos de recuperación se complete.
- Si una tarea de combinación está procesando más de un conjunto de puntos de recuperación (por ejemplo, el conjunto [1~4], el conjunto [5~11] y el conjunto [12~14] son tres conjuntos), el servidor de puntos de recuperación procesará estos conjuntos uno a uno.
- Si una tarea de combinación se reanuda después de una pausa, la tarea detecta en qué punto se ha pausado y reanuda la combinación a partir del punto de pausa.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye la configuración de registros de truncamiento, proporcionar la ubicación de los scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha Avanzada:





Siga estos pasos:

1. Especifique los siguientes detalles:

Cómo truncar un registro

Le permite especificar la programación para truncar los registros de SQL Server y Exchange Server. Se puede especificar la programación como **Diaria**, **Semanal** o **Mensual**.

Nombre de usuario

Le permite especificar el usuario que se autoriza para ejecutar un script.

Contraseña

Le permite especificar la contraseña del usuario autorizado para ejecutar el script.

Ejecutar un comando antes de empezar una copia de seguridad

Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde el script está almacenado. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de seguridad continuará cuando el script devuelva el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detendrá cuando el script devuelva el código de salida.

Ejecutar un comando después de realizar una instantánea

Le permite ejecutar un script después de realizar la instantánea de la copia de seguridad. Especifique la ruta donde el script está almacenado.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta donde el script está almacenado.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y se pueden especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de tareas que se desea recibir.

Cómo activar las alertas de recurso

Le permite especificar un umbral para el Uso de CPU, Uso de memoria, Rendimiento del disco y E/S de la red. Se puede proporcionar el valor en porcentaje. Se recibirá un correo electrónico cuando se exceda el valor de Umbral de alerta.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en Guardar.

Los cambios se guardan y se muestra una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **Recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar.

El plan de copia de seguridad se crea y se implementa automáticamente en el nodo de origen. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

Cómo agregar una tarea de Virtual Standby al plan

Cree una tarea de Virtual Standby para que los datos de la copia de seguridad se conviertan a un formato de máquina virtual y se cree una máquina virtual. La función de Virtual Standby también controla el latido del nodo de origen para que cuando el nodo de origen esté bloqueado, la máquina virtual tome inmediatamente el control como nodo de origen.

Notas:

- Virtual Standby no puede encender automáticamente las instantáneas de punto de recuperación tomadas de nodos de máquinas virtuales basadas en host o replicados de un servidor de puntos de recuperación remoto, y el origen de la tarea de Virtual Standby es el que se replica en un sitio distinto. Se tiene que encender manualmente las instantáneas de punto de recuperación para dichos nodos.
- Si se pausa el plan, la tarea de Virtual Standby no se iniciará. Cuando se vuelva a reanudar el plan, la tarea de Virtual Standby no se reanudará automáticamente. Se tiene que ejecutar manualmente otra tarea de copia de seguridad para iniciar la tarea de Virtual Standby. También, si el plan se pausa la opción Pausar/reanudar Virtual Standby no estará disponible. Si no se desea que la máquina virtual se inicie automáticamente después de que se haya pausado el plan, se tendrá que pausar manualmente el latido para los nodos.

Siga estos pasos:

1. Haga clic en **Agregar una tarea** en el panel izquierdo.

   Una tarea nueva se agrega al panel izquierdo.

2. En el menú desplegable **Tipo de tarea** seleccione **Virtual Standby**.

   La tarea de Virtual Standby se agrega.

3. En la ficha **Origen** seleccione un origen para la tarea de Virtual Standby.

4. Haga clic en la ficha **Servidor de virtualización** e introduzca el servidor de virtualización y los detalles del servidor de control.

   Tipo de virtualización: VMware

   Host de ESX/vCenter

   Especifique el nombre de host del sistema de servidor de ESX o vCenter.

   Nombre de usuario

Especifique el nombre de usuario necesario para iniciar sesión en el sistema VMware.

Nota: la cuenta especificada debe ser una cuenta administrativa o una cuenta con privilegios administrativos sobre el sistema de servidor de ESX o vCenter.

Contraseña

Especifique la contraseña para el nombre de usuario necesario para iniciar sesión en el sistema VMware.

Protocolo

Especifique HTTP o HTTPS como el protocolo que desea utilizar para la comunicación entre el Agente de Arcserve Unified Data Protection de origen y el servidor de control.

Puerto

Especifique el puerto que se desea utilizar para la transferencia de datos entre el servidor de origen y el servidor de control.

Nodo de ESX

Los valores en este campo varían de acuerdo con el valor especificado en el campo Host de ESX/vCenter:

Sistemas del servidor ESX

Cuando se especifica un sistema del servidor ESX en el campo Host de ESX/-vCenter, este campo muestra el nombre de host del sistema del servidor ESX.

Sistemas del servidor vCenter

Cuando se especifica un sistema del servidor vCenter en el campo Host de ESX/vCenter, este campo permite especificar (desde una lista desplegable) el sistema del servidor ESX que se desea asociar a este plan.

Control

Especifique el nombre de host del servidor que controla el estado del servidor de origen.

Notas:

- Puede utilizar cualquier equipo físico o máquina virtual como servidor de control.
- No puede utilizar el servidor de origen de la copia de seguridad como servidor de control.

- La configuración del servidor de control no es necesaria si los nodos se replican a partir de un servidor de puntos de recuperación remoto o si el origen de la tarea de Virtual Standby es el que se replica en un sitio distinto.
- La configuración del servidor de control no es necesaria si el origen de Virtual Standby es la tarea de replicación y el servidor de puntos de replicación de destino de la replicación se encuentra en Azure.

Nombre de usuario

Especifique el nombre de usuario para iniciar sesión en el sistema de control.

Contraseña

Especifique la contraseña del nombre de usuario para iniciar sesión en el sistema de control.

Protocolo

Especifique HTTP o HTTPS como el protocolo que desea utilizar para la comunicación entre Arcserve Unified Data Protection y el sistema de ESX Server (servidor de control).

Puerto

Especifique el puerto que desea utilizar para la transferencia de datos entre Arcserve Unified Data Protection y el sistema de ESX Server (servidor de control).

Utilizar el servidor de control como proxy para la transferencia de datos

Especifique esta opción para permitir que el servidor de control copie los datos de conversión del nodo del Agente de Arcserve Unified Data Protection al almacén de datos de ESX Server. Con esta opción activada, la función de Virtual Standby transfiere los datos de conversión del nodo del agente al almacén de datos del servidor ESX empleando la comunicación del canal de fibra, que transfiere datos con mayor rapidez que la comunicación LAN. Solamente la operación de escribir para la conversión sucede sobre el canal de fibra. La operación de lectura sucede sobre la LAN.

Nota: La opción Utilizar el servidor de control como proxy para la transferencia de datos aparece activada de forma predeterminada. Se puede desactivar esta opción para permitir que el nodo del Agente de Arcserve Unified Data Protection copie los datos de conversión directamente en el almacén de datos del sistema de ESX Server.

Tipo de virtualización: Hyper-V

Nombre de host de Hyper-V

Especifique el nombre de host del sistema Hyper-V.

Nombre de usuario

Especifique el nombre de usuario necesario para iniciar sesión en el sistema Hyper-V.

Nota: la cuenta especificada debe ser una cuenta administrativa o una cuenta con privilegios administrativos sobre el sistema Hyper-V.

Contraseña

Especifique la contraseña para el nombre de usuario necesaria para iniciar sesión en el sistema Hyper-V.

Protocolo

Especifique HTTP o HTTPS como el protocolo que desea utilizar para la comunicación entre Arcserve Unified Data Protection y el sistema de Hyper-V Server (servidor de control).

Puerto

Especifique el puerto que desea utilizar para la transferencia de datos entre Arcserve Unified Data Protection y el sistema de Hyper-V Server (servidor de control).

Nota: Para validar el sistema Hyper-V, haga clic en **Conectar**.

5. Haga clic en la ficha **Máquina virtual** e introduzca los detalles de los siguientes campos: Configuración básica de la máquina virtual, Almacén de datos de la máquina virtual para VMware, Ruta de la máquina virtual para Hyper-V y Red de la máquina virtual.

   Sistemas VMware:

   Aplique las siguientes opciones de la máquina virtual en sistemas VMware:

   Prefijo del nombre de la máquina virtual

   Especifique el prefijo que se desea agregar al nombre de visualización para la máquina virtual en el sistema del servidor ESX.

   Valor predeterminado: UDPVM_

   Agrupación de recursos

   Especifique el nombre de la agrupación de recursos donde se debe agrupar la máquina de Virtual Standby.

   Número de CPU

   Especifique el número mínimo y máximo de CPU que admite la máquina de Virtual Standby.

Memoria

Especifique la cantidad total de RAM en MB que se debe adjudicar a la máquina de Virtual Standby.

Nota: La cantidad de memoria RAM especificada debe ser un múltiplo de dos.

Instantáneas del punto de recuperación

Especifique el número de instantáneas del punto de recuperación (puntos de recuperación) para la máquina virtual en espera. El número máximo de instantáneas del punto de recuperación es de 29 para los servidores de virtualización de VMware.

Todos los discos virtuales comparten el mismo almacén de datos.

Seleccione esta opción para copiar todos los discos relacionados con la máquina virtual en un almacén de datos.

Desactive la casilla de verificación para copiar la información relacionada con el disco para la máquina virtual en el almacén de datos correspondiente. Especifique la ubicación donde se desea almacenar los datos de conversión.

Red

Le permite definir los NIC, las redes virtuales y las rutas que el sistema del servidor ESX utiliza para comunicarse con las máquinas virtuales.

Nota: La transmisión de SR-IOV de VMware y el adaptador de red flexible no son compatibles.

Mismo número de adaptadores de red que el origen en última copia de seguridad

Seleccione esta opción para definir cómo asignar el NIC virtual a la red virtual. Especifique esta opción cuando la máquina virtual contiene NIC virtuales y una red virtual.

Deseleccione la casilla de verificación para definir el nombre de la red virtual que se desea que el NIC utilice para comunicarse.

Sistemas Hyper-V:

Aplique las siguientes opciones de la máquina virtual en sistemas Hyper-V:

Configuración básica

Complete los siguientes valores de configuración básicos:

Prefijo del nombre de la máquina virtual

Especifique el prefijo que se desea agregar al nombre de visualización para la máquina virtual en el sistema Hyper-V.

Valor predeterminado: UDPVM_

Número de CPU

Especifique el número mínimo y máximo de CPU que admite el sistema de Virtual Standby.

Memoria

Especifique la cantidad total de RAM en MB que se debe adjudicar a la máquina de Virtual Standby.

Nota: La cantidad de memoria RAM especificada debe ser un múltiplo de cuatro.

Instantáneas del punto de recuperación

Especifique el número de instantáneas del punto de recuperación para la máquina virtual en espera. El número máximo de instantáneas del punto de recuperación es de 24 para los servidores de virtualización de Hyper-V.

Todos los discos virtuales comparten la misma ruta.

Seleccione esta opción para especificar la ubicación del servidor Hyper-V donde se desea almacenar los datos de conversión.

Deseleccione la casilla de verificación para especificar la ubicación del servidor Hyper-V donde se desea almacenar los datos de conversión para cada disco virtual.

Nota: La solución Arcserve UDP no es compatible con la creación de imágenes de disco virtuales (archivos VHD/VHDX) en volúmenes comprimidos ni en volúmenes cifrados por el sistema de archivos. Si la ruta especificada reside en volúmenes comprimidos o cifrados de Hyper-V, Arcserve UDP no permite crear la tarea de Virtual Standby.

Red de la máquina virtual

Le permite definir los NIC, las redes virtuales y las rutas que el servidor Hyper-V utiliza para comunicarse con las máquinas virtuales. Especifique una de las opciones siguientes y complete los campos pertinentes.

Mismo número de adaptadores de red que el origen en última copia de seguridad

Seleccione esta opción para definir cómo asignar el NIC virtual a la red virtual. Especifique esta opción cuando la máquina virtual contiene NIC virtuales y una red virtual.

Deseleccione la casilla de verificación para definir el nombre de la red virtual que se desea que el NIC utilice para comunicarse.

6. Haga clic en la ficha **Avanzada** y proporcione los detalles siguientes:

Iniciar automáticamente la máquina virtual

Especifique si se desea iniciar la máquina virtual automáticamente.

Nota: Esta opción no se encuentra disponible para nodos de máquinas virtuales basadas en el host ni para nodos replicados desde un servidor de puntos de recuperación remoto, y el origen de la tarea de Virtual Standby es el que se replica en un sitio distinto.

Tiempo de espera

Especifique el tiempo que el servidor de control debe esperar a un latido antes de encender una instantánea de punto de recuperación.

Frecuencia

Especifique la frecuencia con la que el servidor de origen comunica latidos al servidor de control.

Ejemplo: el valor de Tiempo de espera especificado es 60. El valor de Frecuencia especificado es 10. El servidor de origen comunicará los latidos en intervalos de 10 segundos. Si el servidor de control no detecta ningún latido en 60 segundos desde el último latido detectado, el servidor de controlador enciende una máquina virtual mediante la última instantánea de punto de recuperación.

Activar Alertas de correo electrónico

Le permite recibir alertas de correo electrónico en función de los valores de configuración que se proporcionan. Cuando se selecciona esta opción, se activan otras categorías de alertas de correo electrónico para su selección.

- **Falta el latido del equipo de origen**: Virtual Standby envía notificaciones de alerta cuando el servidor de control no detecta el latido del servidor de origen.

  Nota: Esta opción no está disponible para los nodos de Replicación desde un servidor de puntos de recuperación remoto o si el origen de la tarea de Virtual Standby es el que se va a replicar en un sitio distinto.

- **Máquina virtual encendida para el equipo de origen configurado con encendido automático**: Virtual Standby envía notificaciones de alerta cuando enciende una máquina virtual que está configurada para el encendido automático en el caso de que no se detecte el latido.

  Nota: Esta opción no está disponible para los nodos de Replicación desde un servidor de puntos de recuperación remoto o si el origen de la tarea de Virtual Standby es el que se va a replicar en un sitio distinto. Esta opción tampoco no está disponible para los nodos de máquina virtual basada en el host.

- **Máquina virtual encendida para el equipo de origen configurado con encendido manual**: Virtual Standby envía notificaciones de alerta cuando enciende manualmente una máquina virtual.
- **Errores/bloqueo de Virtual Standby**: Virtual Standby envía notificaciones de alerta cuando detecta que se ha producido un error durante el proceso de conversión.
- **Virtual Standby correcto**: Virtual Standby envía notificaciones de alerta cuando detecta que una máquina virtual se enciende correctamente.
- **Virtual Standby no se ha iniciado correctamente desde la instantánea del punto de recuperación**: Virtual Standby envía notificaciones de alerta cuando detecta que una máquina virtual no se ha encendido automáticamente y se encuentra especificada la opción de recuperación local Iniciar automáticamente la máquina virtual.
- **No se puede acceder al hipervisor**: Virtual Standby envía notificaciones de alerta cuando detecta que no se puede establecer la comunicación con el sistema de servidor ESX o el sistema Hyper-V.
- **Espacio libre de almacenamiento de máquina virtual inferior a**: Virtual Standby envía notificaciones de alerta cuando detecta que no hay suficiente espacio libre en disco en la ruta del hipervisor definida. La detección se produce cuando la cantidad libre de espacio en disco es inferior al umbral definido por el usuario. El umbral se puede definir como un valor absoluto (MB) o como un porcentaje de la capacidad del volumen.

7. Haga clic en **Guardar**.

   Los cambios se guardan y la tarea de Virtual Standby se implementa automáticamente en el servidor de Virtual Standby.

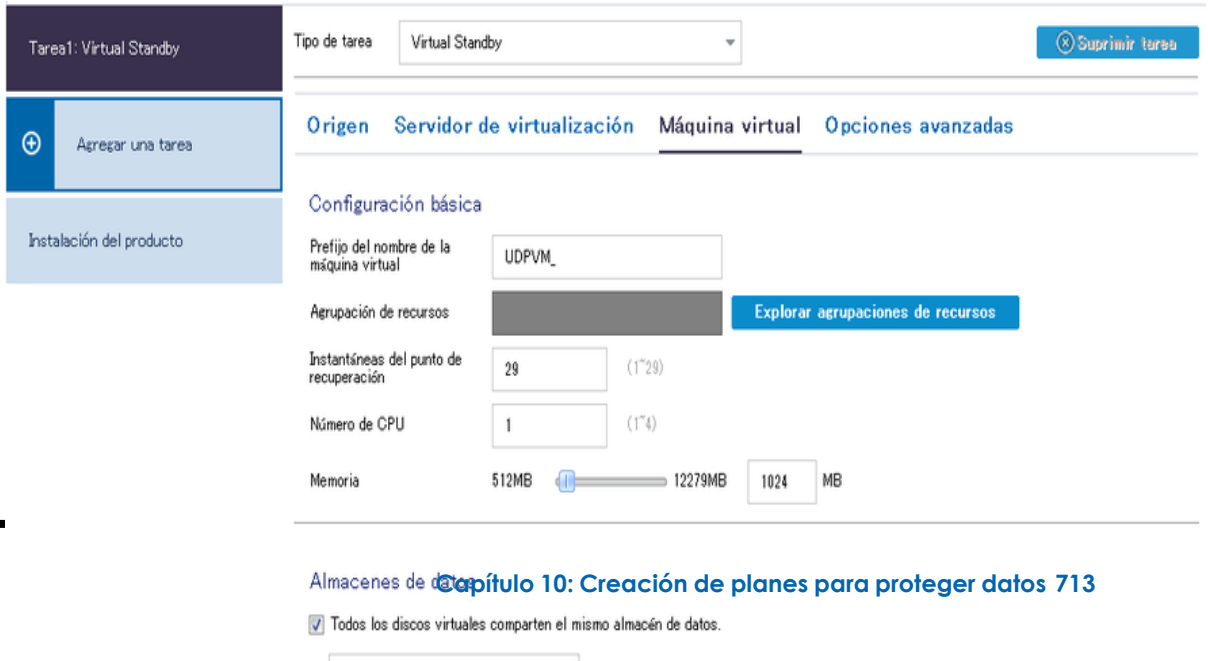
   Se ha creado e implementado correctamente el plan de Virtual Standby.

Cómo determina la aplicación la cantidad de NIC para encender

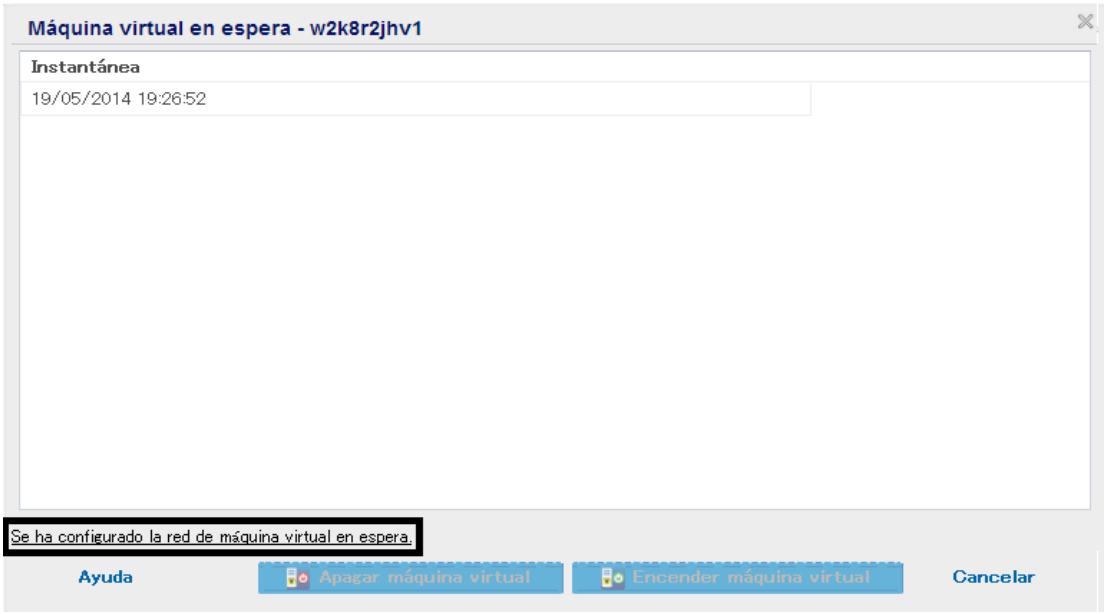
Al encender las máquinas virtuales, Virtual Standby determina la cantidad de NIC (tarjetas de interfaz de red) para encender cuando el encendido de máquinas virtuales remotas se basa en si la red de la máquina virtual en espera se ha configurado. La tabla siguiente ilustra cómo Virtual Standby determina la cantidad de NIC para encender cuando se encienden máquinas virtuales en espera.

Valores definidos en el plan para la red de la máquina virtual	No se ha especificado la opción Encendido de la máquina virtual en espera con la configuración de red personalizada	Se ha especificado la opción Encendido de la máquina virtual en espera con la configuración de red personalizada
Los valores definidos son los mismos que el equipo de origen.	Virtual Standby enciende la cantidad de NIC definidos para el equipo de origen a partir de la última tarea de copia de seguridad.	Virtual Standby enciende la cantidad de NIC según el mayor de los valores siguientes: ■ La cantidad definida en la configuración de red personalizada. ■ La cantidad de NIC definidos para el equipo de origen a partir de la última tarea de copia de seguridad.
Los valores definidos son valores personalizados.	Virtual Standby enciende la cantidad de redes personalizadas que se definen en el plan.	Virtual Standby enciende la cantidad de NIC según el mayor de los valores siguientes: ■ La cantidad definida en la configuración de red personalizada. ■ La cantidad de NIC definidos para la política personalizada.

El cuadro de diálogo siguiente (Editar tarea de Virtual Standby o Modificar un plan) de la tarea de Virtual Standby está formado por configuraciones personalizadas para que se enciendan los NIC:



El cuadro de diálogo siguiente (Máquina virtual en espera - <nombre_host>) ilustra la ubicación en la que se especifica la opción Encendido de la máquina virtual en espera con la configuración de red personalizada:

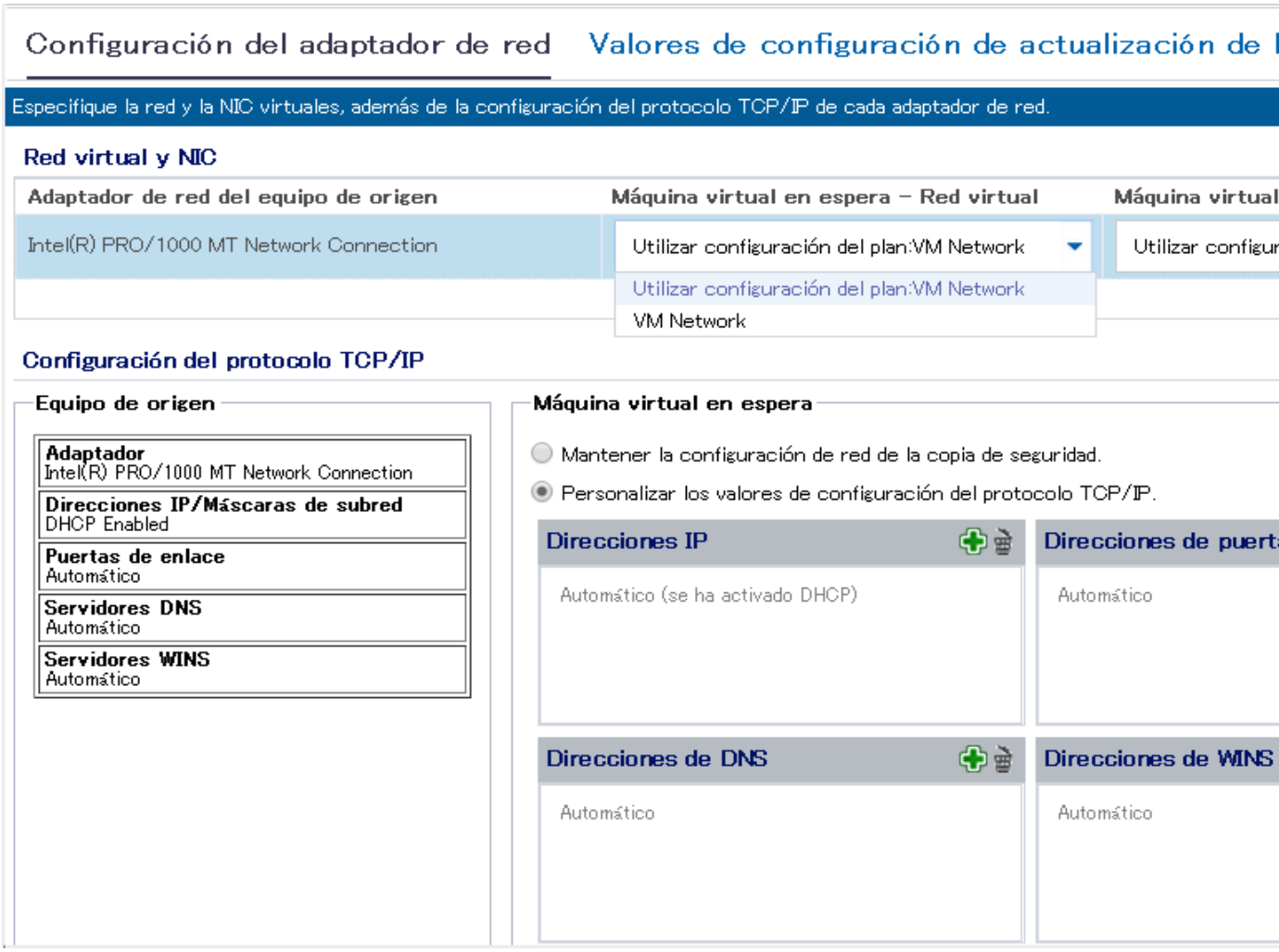


Configuración de la red de máquinas virtuales en espera

Se puede encender la máquina virtual en espera con valores de configuración de red personalizados. Se pueden configurar los siguientes valores de configuración de red en la máquina virtual en espera:

- Especifique la red virtual y la NIC (Tarjeta de interfaz de red) y los valores de configuración de TCP/IP para cada adaptador desde la ficha **Configuración del adaptador de red**.
- Actualice los servidores DNS para volver a dirigir a los clientes del equipo de origen a las máquinas virtuales de Virtual Standby en función de los valores de configuración de TCP/IP desde la ficha **Valores de configuración de actualización de DNS**.

El diagrama siguiente se muestra la ficha **Configuración del adaptador de red** de la **Configuración de red de la máquina virtual en espera**:



Siga estos pasos:

1. En la ficha **Recursos**, vaya al grupo de nodos de **Virtual Standby**.

   Los nodos de Virtual Standby se muestran en el panel central.

2. En el panel central, seleccione el nodo y haga clic en **Configuración de red de la máquina virtual en espera**.

   Se abre la página Configuración de red de la máquina virtual en espera - <nombre de nodo>.

3. En la ficha **Configuración del adaptador de red**, seleccione la red virtual en la lista **Máquina virtual en espera - red virtual**.

4. Seleccione el tipo de NIC en la lista **Máquina virtual en espera - Tipo de NIC**.

5. Seleccione **Personalizar los valores de configuración de TCP/IP**.

6. Haga clic en el botón **Agregar dirección** y agregue **Direcciones IP**, **Direcciones de puerta de enlace**, **Direcciones de DNS** y **Direcciones WINS**.

   Nota: Si se agregan **Direcciones de DNS**, a continuación configure los servidores DNS en la ficha **Valores de configuración de actualización de DNS**.

7. Haga clic en **Guardar**.

   Se cierra la página Configuración de red de la máquina virtual en espera - <nombre de nodo>.

   La red de máquina virtual en espera se ha configurado.

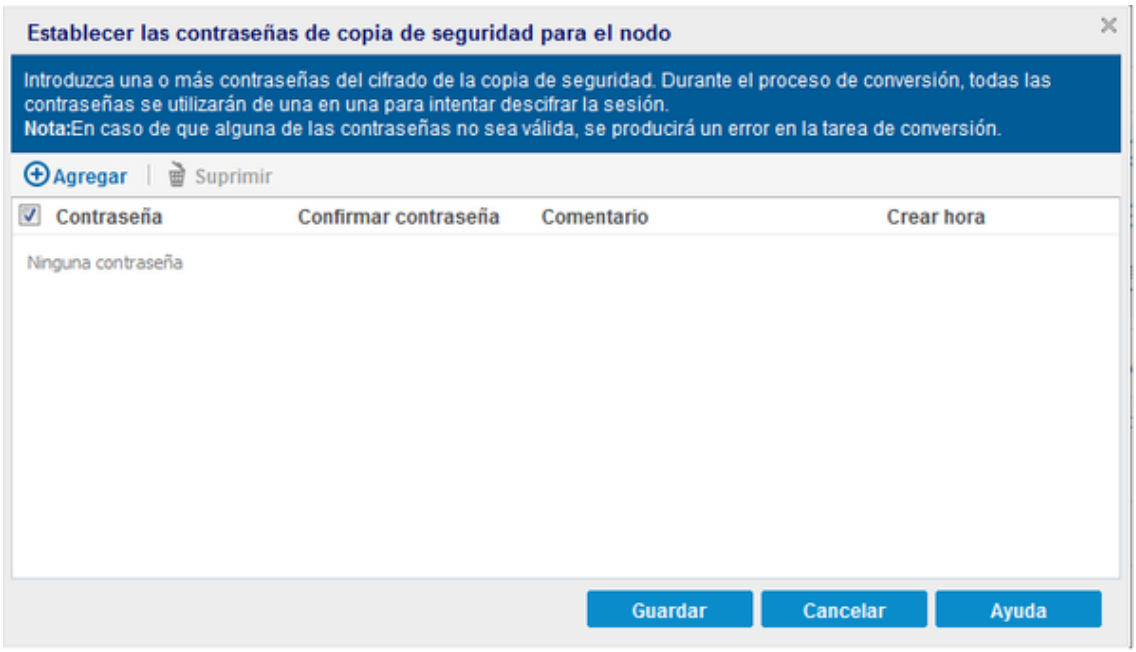
Cómo establecer las contraseñas de copia de seguridad para uno o más nodos

Para garantizar que el conversor pueda convertir los puntos de recuperación replicados, Virtual Standby permite especificar las contraseñas de la copia de seguridad de los datos que el conversor pueda utilizar para convertir los datos.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.
3. En el panel central, haga clic con el botón secundario del ratón en el nodo y haga clic en **Establecer contraseñas de la copia de seguridad**.

   Aparecerá el cuadro de diálogo **Establecer las contraseñas de copia de seguridad para el nodo**.

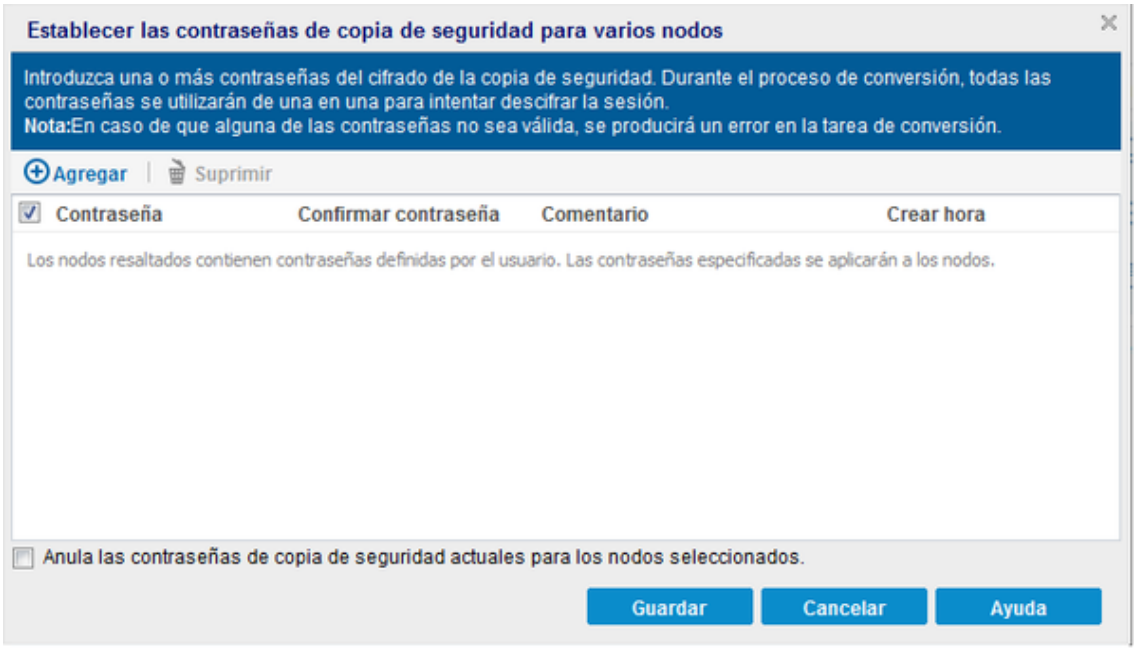


4. Realice las tareas siguientes en el cuadro de diálogo **Establecer contraseñas de la copia de seguridad** para uno o más nodos:

   Agregar: haga clic en **Agregar** para agregar una o más contraseñas de copia de seguridad a los nodos seleccionados.

   Suprimir:haga clic en **Suprimir** para suprimir una o más contraseñas de copia de seguridad de los nodos seleccionados.

Nota: Se pueden anular las contraseñas de copia de seguridad actuales para varios nodos seleccionando la casilla de verificación **Anula las contraseñas de copia de seguridad actuales para los nodos seleccionados**.



5. Haga clic en **Guardar**.

   El cuadro de diálogo desaparece y las contraseñas de copia de seguridad se establecen para los nodos remotos seleccionados.

(Opcional) Ejecución de la tarea de Virtual Standby manualmente

Para ejecutar manualmente una tarea de Virtual Standby, se tiene que realizar primero una copia de seguridad manual. La tarea de Virtual Standby se asocia con una tarea de copia de seguridad. Si un plan incluye una tarea de copia de seguridad y una tarea de Virtual Standby y se ejecuta manualmente la tarea de copia de seguridad, la tarea de Virtual Standby se ejecuta automáticamente después de la terminación de la tarea de copia de seguridad.

Siga estos pasos:

1. Haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Muestra los planes que se han agregado.
3. Seleccione los nodos que de los que desea realizar la copia de seguridad. El nodo seleccionado debe tener asignado un plan.
4. En el panel central, haga clic en **Acciones**, **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo **Ejecutar ahora una copia de seguridad**.
5. Seleccione el tipo de copia de seguridad y proporcione un nombre para la tarea de copia de seguridad.
6. Haga clic en **Aceptar**.

   Se ejecuta la tarea de copia de seguridad.

   La tarea de Virtual Standby se ejecuta inmediatamente después de que se complete la tarea de copia de seguridad.

   La tarea de Virtual Standby se ejecuta manualmente.

Pausa y reanudación de latidos

La solución Arcserve Unified Data Protection permite pausar y reanudar los latidos detectados por el servidor de control. El latido es el proceso a través del cual el servidor de origen y el servidor de control comunican el estado del servidor de origen. Si el servidor de control no detecta ningún latido tras un período de tiempo especificado, la función de Virtual Standby puede aprovisionar la máquina virtual para que funcione como el nodo de origen.

Ejemplos: cuándo pausar o reanudar los latidos

Los ejemplos siguientes describen cuándo pausar y reanudar los latidos:

- Pause el latido cuando desee dejar sin conexión un nodo (servidor de origen) por motivos de mantenimiento.
- Reanude el latido cuando hayan finalizado las tareas de mantenimiento y el nodo (servidor de origen) esté en línea.

Tenga en cuenta el siguiente comportamiento:

- Se pueden pausar y reanudar los latidos a nivel del grupo o a nivel del nodo individual.
- Se pueden pausar y reanudar los latidos para uno o varios nodos en un paso.
- La solución Arcserve Unified Data Protection
- Cuando se actualizan las instalaciones del Agente en los nodos de origen, Arcserve Unified Data Protection Para asegurarse de que los servidores de control controlen los nodos actualizados, reinicie el latido de los nodos una vez que se hayan completado las actualizaciones de los nodos.

Siga estos pasos:

1. Inicie sesión en el Arcserve Unified Data Protection.
2. Haga clic en la ficha **recursos**.
3. En el panel izquierdo, vaya a **Virtual Standby** y haga clic en **Todos los nodos**.

   Si se han agregado algunos nodos, los nodos se mostrarán en el panel central.
4. Seleccione el nodo que se desea pausar o reanudar.
5. En el panel central, haga clic en **Acciones**, **Latido**, **Pausa** o **Reanudación**.

   El latido del nodo seleccionado se pausa o se reanuda.

Pausa y reanudación de la tarea de Virtual Standby

La conversión virtual es el proceso en el cual Virtual Standby convierte puntos de recuperación de Arcserve Unified Data Protection de los nodos de origen a formatos de máquina virtual denominados instantáneas de puntos de recuperación. En el caso de que se produzca un error en un nodo de origen, la función de Virtual Standby utiliza las instantáneas de puntos de recuperación para encender una máquina virtual para el nodo de origen.

Permitir que el proceso de conversión virtual funcione continuamente se considera una práctica recomendable. Sin embargo, si se desea pausar temporalmente el proceso de conversión virtual en servidores de Virtual Standby locales y remotos, se puede hacer desde la consola. Una vez se han corregido los problemas del nodo de origen, se puede reanudar el proceso de conversión virtual.

Cuando se ponen en pausa tareas de Virtual Standby (tareas de conversión), la operación de pausa no pondrá en pausa la tarea de conversión que está en curso actualmente. La operación de pausa se aplica solamente a la tarea que se espera que se ejecute al final de la siguiente tarea de copia de seguridad. Como resultado, la tarea de conversión siguiente no se inicia hasta que se reanuda explícitamente la tarea de conversión (en pausa).

Si se reanuda Virtual Standby para los nodos y si hay varias sesiones de copia de seguridad sin instantánea de punto de recuperación, obtendrá un cuadro de diálogo para seleccionar la opción de copia inteligente. Si se hace clic en Sí, Virtual Standby convertirá la sesión combinada en una instantánea única de punto de recuperación. Si se hace clic en No, Virtual Standby convertirá cada sesión individualmente

Nota: Opcionalmente, se pueden pausar las tareas de Virtual Standby y reanudarlas directamente desde los nodos. Para obtener más información, consulte Pausa y reanudación de tareas de pausa virtual desde los nodos.

Siga estos pasos:

1. Inicie sesión en el Arcserve Unified Data Protection.
2. Haga clic en la ficha **recursos**.
3. En el panel izquierdo, vaya a **Virtual Standby** y haga clic en **Todos los nodos**.

   Si se han agregado algunos nodos, los nodos se mostrarán en el panel central.
4. Seleccione el nodo que se desea pausar o reanudar.

5. En el panel central, haga clic en **Acciones**, **Virtual Standby**, **Pausa** o **Reanudación**.

   La función de Virtual Standby del nodo seleccionado se pausa o se reanuda.

Verificación del plan

Para verificar la función de Virtual Standby, confirme que se ha creado correctamente el plan de Virtual Standby. Después de verificar que el plan se ha creado correctamente, compruebe si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Después de que la tarea de copia de seguridad se complete correctamente, se ejecutará la tarea de Virtual Standby. Se puede comprobar el estado de la tarea de copia de seguridad y de la tarea de Virtual Standby en la ficha **tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga estos pasos para verificar las tareas de Virtual Standby:

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad y la tarea de Virtual Standby se han realizado correctamente.

   El plan de Virtual Standby se ha verificado correctamente.

   Se crea la máquina de Virtual Standby.

Cómo crear un plan de recuperación asegurada

Para verificar la accesibilidad y asegurar la recuperación de los datos, es necesario crear un plan de recuperación asegurada. El plan para la recuperación asegurada se basa en un plan de copia de seguridad/replicación. Esta tarea de recuperación le permite agregar una tarea de recuperación asegurada a un plan de replicación o de copia de seguridad existente. La tarea de recuperación asegurada consta de un origen, los valores de configuración de prueba, la programación y la configuración avanzada. También se puede ejecutar manualmente una tarea de recuperación asegurada.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Adición de una tarea de recuperación asegurada a un plan
3. (Opcional) Ejecución manual de la tarea de prueba de recuperación asegurada

Revisión de las consideraciones y requisitos previos

Verifique que se han realizado las siguientes tareas de los requisitos previos:

- Inicie sesión en la Consola.
- Se ha instalado el componente del servidor y se han creado almacenes de datos si se desea almacenar los datos de la copia de seguridad en servidores de puntos de recuperación.
- Se tiene un punto de recuperación válido para crear una máquina virtual instantánea o un disco virtual instantáneo. Se pueden seleccionar los puntos de recuperación de una de las tareas siguientes:
  - Copia de seguridad de Windows basada en el agente
  - Copia de seguridad sin agente basada en el host
  - Replicación
  - Copia de seguridad, Office 365 Exchange Online
  - Copia de seguridad, Office 365 OneDrive
  - Copia de seguridad, Office 365 SharePoint Online
  - Copia de seguridad, Archivos en una ruta UNC o NFS
  - Copia de seguridad de Linux basada en agentes
- Verifique que los agentes de Arcserve UDP ya estén instalados en el servidor proxy.
- Verifique que el sistema operativo del servidor proxy sea Windows Server 2008 R2 de 64 bits o posterior.

  Nota: Para el plan de copia de seguridad de la ruta UNC y para el plan de copia de seguridad de Office 365 (Exchange Online, OneDrive, SharePoint Online), el servidor proxy de la recuperación asegurada debe ser Windows 2012 o una versión posterior.
- Compruebe que el servidor proxy tenga suficiente espacio para la máquina virtual instantánea o el disco virtual instantáneo.

  Nota: El espacio necesario depende en gran medida del tamaño de la memoria RAM que se ha configurado en la tarea de recuperación asegurada para el tipo de prueba de la recuperación asegurada de la máquina virtual instantánea. Para cada máquina virtual instantánea, el hipervisor necesita como máximo el mismo tamaño de la memoria RAM para contener los datos temporales en los archivos de intercambio de la memoria. Por ejemplo, si se tienen 5 nodos en el mismo plan con la tarea de recuperación asegurada de la máquina virtual

instantánea y el tamaño de la memoria de la máquina virtual se establece en 4 GB, se necesitarán al menos 5 * 4 = 20 GB de tamaño libre para contener los archivos de intercambio de la memoria. Además, es posible que sea necesario tener un tamaño libre de 10 MB para contener los archivos de configuración de la máquina virtual.

- Verifique que la versión del sistema operativo de Windows en el servidor proxy de recuperación asegurada sea la misma o posterior a la versión del sistema operativo de Windows en la máquina virtual de origen.

Adición de una tarea de recuperación asegurada al plan

Una tarea de recuperación asegurada incluye una tarea de recuperación asegurada para un plan de replicación/copia de seguridad existente. Cada tarea está formada por parámetros que definen el origen, la configuración de la tarea, la programación y la configuración avanzada. Cree una tarea de recuperación asegurada en función de la tarea de replicación o de copia de seguridad para verificar la recuperación asegurada y la accesibilidad de los datos y proporcione la comprobación de la integridad de los datos.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, abra un plan de replicación o de copia de seguridad existente.
4. En el plan seleccionado, haga clic en **Agregar una tarea** en el panel izquierdo.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa el plan, la tarea de recuperación asegurada no se iniciará. Cuando se reanuda el plan, la tarea de recuperación asegurada no se reanuda automáticamente. Se debe ejecutar manualmente otra tarea de copia de seguridad para iniciar la tarea de recuperación asegurada.
6. En la lista desplegable **Tipo de tarea**, seleccione **Prueba de recuperación asegurada**.
7. Ahora especifique el Origen, la configuración de la tarea (IVM o IVD), la Programación y los detalles de las opciones Avanzadas.
8. Haga clic en **Guardar**.

   Los cambios se guardan y la tarea de recuperación asegurada se implementa automáticamente.

Especificación del origen

La ficha Origen le permite especificar el punto de recuperación de origen que se desea proteger.

Siga estos pasos:

1. Haga clic en la ficha **Origen**.
2. Haga clic en la lista desplegable del origen del punto de recuperación para la prueba de recuperación asegurada y seleccione la opción deseada.
3. Seleccione los tipos de puntos de recuperación para la prueba de la recuperación asegurada. Puede seleccionar una de las dos siguientes opciones:
   - Prueba de la recuperación asegurada desde los tipos de copia de seguridad seleccionados

     Se puede seleccionar Copias de seguridad diarias, Copias de seguridad semanales o Copias de seguridad mensuales. Las opciones diarias, semanales o mensuales están disponibles en función de la programación de la copia de seguridad de origen. Por ejemplo, si la copia de seguridad de origen solo tiene programadas copias de seguridad mensuales, la prueba de la recuperación asegurada de la opción de los tipos de copia de seguridad seleccionados solo tendrá activada la opción Copias de seguridad mensuales.
   - Prueba de la recuperación asegurada de los puntos de recuperación más recientes

Se especifica el origen

Especificación de la configuración de la tarea para el tipo de prueba: Máquina virtual instantánea

La selección de Máquina virtual instantánea como Tipo de prueba permite iniciar la máquina virtual desde el punto de recuperación y, opcionalmente, ejecuta el script personalizado. Si la máquina virtual se inicia correctamente y el script de verificación devuelve un resultado correcto durante el intervalo de tiempo especificado por el usuario, se considerará que el punto de recuperación está en buen estado.

Nota: Este paso no es necesario si se selecciona **Disco virtual instantáneo** como Tipo de prueba.

Se puede seleccionar un tipo de hipervisor de VMware vSphere y Microsoft Hyper-V e introducir los detalles de configuración del proxy y la configuración de la máquina virtual para especificar la configuración de la tarea para la máquina virtual instantánea.

Siga estos pasos:

1. Seleccione **Máquina virtual instantánea** como Tipo de prueba.

   Nota: Cuando la tarea de origen es una tarea de replicación o copia de seguridad de Linux basada en agente, solamente se puede establecer la opción Máquina virtual instantánea como tipo de prueba.

2. Seleccione una de las opciones de hipervisor e introduzca los detalles relacionados:

   VMware vSphere

   Nota: Si la configuración de la tarea de recuperación asegurada es de máquina virtual instantánea a vSphere, la licencia de VMware necesaria es similar a la licencia necesaria de la característica de la máquina virtual instantánea.

   a. Realice una de las siguientes opciones para proporcionar un servidor vCenter/ESX(i):

      - Si ya se ha agregado un nodo de VMware al sitio seleccionado en la Consola, seleccione dicho nodo en la lista desplegable Servidor vCenter/ESX(i).
      - Si no se ha agregado ningún nodo de VMware, haga clic en **Agregar**.

        Se abrirá el cuadro de diálogo **Especificar el destino de la máquina virtual**.
      - Especifique los detalles de la máquina virtual y haga clic en Aceptar.

Todos los servidores ESX(i) o todas las agrupaciones de recursos se muestran en el panel central de la página Ubicación de la máquina virtual.

b. Seleccione una de las opciones entre ESX(i), clúster, agrupación de recursos o aplicación virtual como la ubicación.

Se especifica el equipo VMware vSphere.

Nota: Especifique el almacén de datos del servidor ESX(i) si la tarea de origen es una tarea de replicación o copia de seguridad de Linux basada en agente o sin agente basada en host.

Especificación de Microsoft Hyper-V

Realice una de las siguientes opciones para proporcionar Microsoft Hyper-V:

- Si ya se ha agregado un nodo de Hyper-V al sitio seleccionado en la Consola, seleccione dicho nodo en la lista desplegable Servidor/clúster de Hyper-V.
- Si no se ha agregado ningún nodo de Hyper-V, haga clic en **Agregar**.

  Se abrirá el cuadro de diálogo Especificar el destino de la máquina virtual.

  Nota: Cuando se conecta a la máquina virtual instantánea de Hyper-V mediante una cuenta de administrador local no integrada, el UAC remoto debe estar desactivado. Para obtener más información acerca de cómo desactivar el UAC remoto para los administradores no integrados, consulte Cómo desactivar un UAC remoto para un administrador no integrado.
- Especifique los detalles del servidor Hyper-V y haga clic en **Aceptar**.

Se especifica la máquina virtual de Hyper-V.

Especificación de Nutanix AHV

Esto solo es para la compatibilidad con máquinas virtuales Linux. Para obtener más información, consulte Protección de una máquina virtual instantánea en Nutanix AHV para el nodo de Linux.

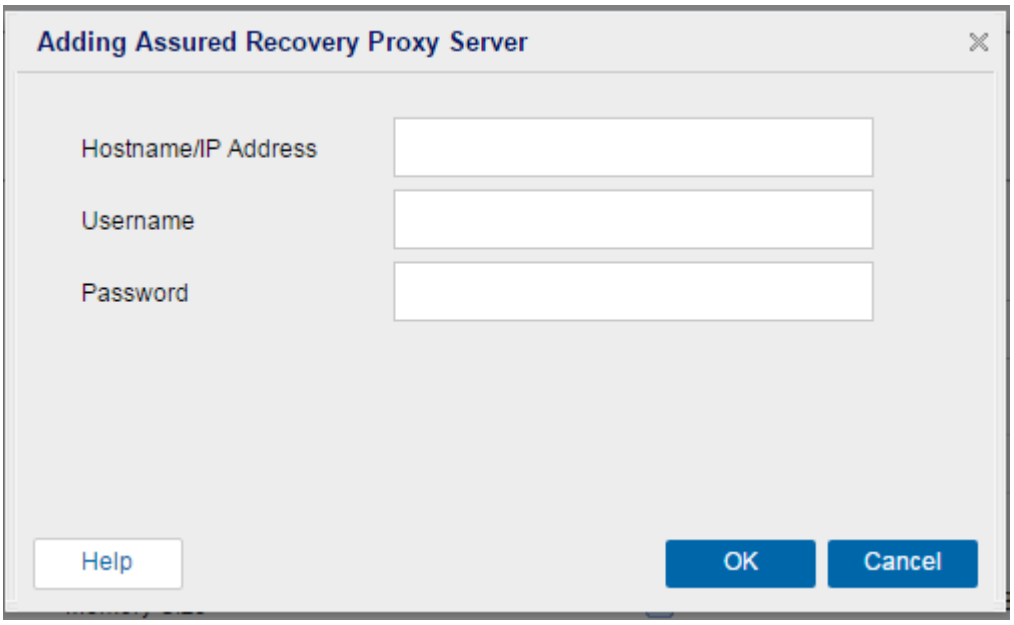
3. Realice una de las siguientes opciones para proporcionar el **Servidor proxy:**

- Si ya se ha agregado un nodo del servidor proxy al sitio seleccionado en la Consola, seleccione dicho nodo en la lista desplegable del servidor proxy.

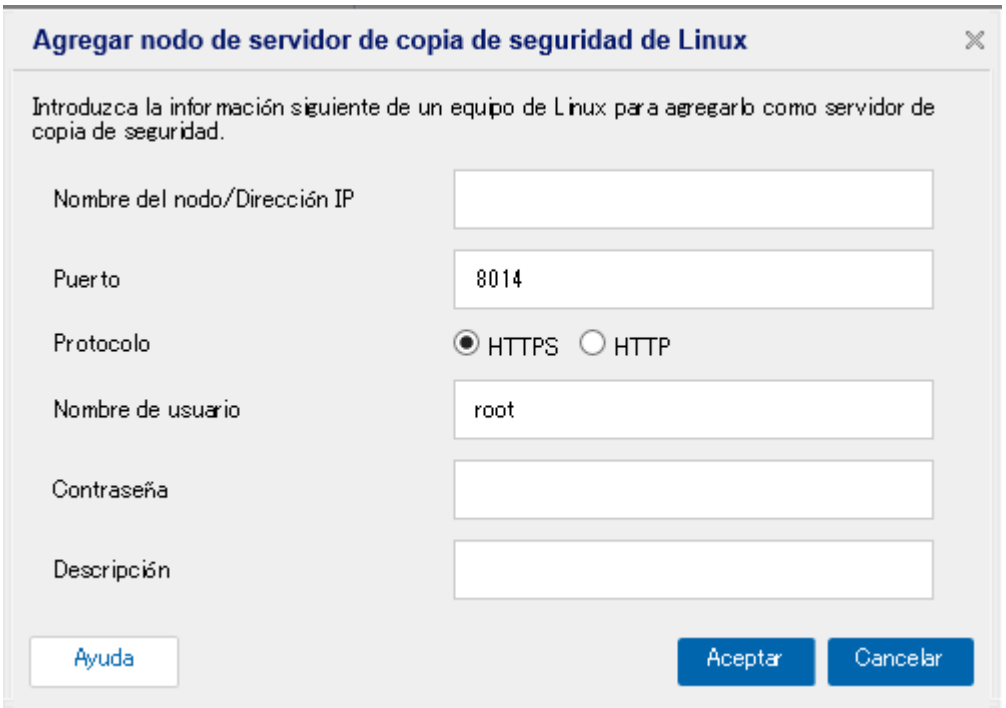
- Si no se ha agregado ningún nodo del servidor proxy, haga clic en **Agregar**.

  Aparecerá el cuadro de diálogo **Agregar servidor proxy de la recuperación asegurada**.

  Para el servidor proxy de Windows



  Para el servidor proxy de Linux



- Especifica los detalles del servidor proxy.
- Haga clic en **Aceptar**.

Los nodos se muestran en el área **Nodos disponibles**.

Notas:

- Se debe seleccionar un servidor proxy solo cuando el hipervisor sea VMware vSphere.
- En estos casos, debe instalarse el rol de Network File System (NFS) de Windows en el servidor de puntos de recuperación. El proceso de la máquina virtual instantánea instala automáticamente el NFS. Para instalarlo de forma manual, consulte Cómo instalar el sistema de archivos de red en Windows Server.
- Seleccione los servidores proxy en función de los tipos de nodo seleccionados incluidos en el plan. Por ejemplo, el servidor proxy de Windows para el nodo de Windows y el servidor proxy de Linux para el nodo de Linux.

4. (Opcional) Realice los pasos siguientes para especificar los valores de configuración de la puerta de enlace para la recuperación asegurada.

   Nota: Se aplica solamente a Linux.

   a. Utilice la configuración de DHCP o especifique la dirección IP, la máscara y la puerta de enlace predeterminada manualmente.

   b. Seleccione un una red virtual de la lista desplegable.

   Nota: La configuración de la puerta de enlace solamente es necesaria cuando el origen de la prueba de recuperación asegurada es una tarea de replicación o copia de seguridad de Linux basada en agente o sin agente basada en host.

5. Especifique los detalles de la **configuración de la máquina virtual** de la recuperación asegurada.

   Prefijo del nombre de la máquina virtual

   Especifica el prefijo del nombre de la máquina virtual. El nombre del nodo de origen con un prefijo es el nombre predeterminado de la máquina virtual instantánea. No se permiten algunos caracteres especiales en el nombre como, por ejemplo, @, \, etc.

   Valor predeterminado: UDPARVM_

   Carpeta de los archivos de la máquina virtual

   Especifique la ubicación de la carpeta de la máquina virtual de la recuperación asegurada en el servidor proxy. Se puede explorar la información sobre el volumen del servidor proxy.

   Número de CPU

Especifica el número de CPU que se necesita en la máquina virtual de la recuperación asegurada.

Tamaño de memoria

Especifica el tamaño de memoria que se necesita en la máquina virtual de la recuperación asegurada.

Configuración de la red

Especifica los valores de configuración de la red en la máquina virtual de la recuperación asegurada. Se puede seleccionar "Conectar máquina virtual de la recuperación asegurada a la red" o no. También se puede utilizar la configuración de DHCP para la máquina virtual de la recuperación asegurada o se puede utilizar la configuración de TCP/IP de la sesión de copia de seguridad.

Tipo de adaptador

Especifica el tipo de adaptador en la máquina virtual de la recuperación asegurada. El tipo de adaptador disponible puede variar según el hipervisor.

Especificación de la configuración de la tarea para el tipo de prueba: Disco virtual instantáneo

La selección de Disco virtual instantáneo como Tipo de prueba para los valores de configuración de la prueba permite montar el punto de recuperación como un disco local, comprueba la integridad del volumen/sistema de archivos y, opcionalmente, ejecuta el script personalizado. Se considera que el punto de recuperación está en buen estado si se monta correctamente el punto de recuperación y todas las pruebas devuelven resultados correctos.

Nota:

- Este paso no es necesario si se selecciona **Máquina virtual instantáneo** como Tipo de prueba.
- La opción **Disco virtual instantáneo** no admite un nodo que no sea de Windows.

Siga estos pasos:

1. Realice uno de los siguientes pasos para proporcionar el servidor en la opción **Servidor proxy de Windows:**
   a. Seleccione uno de los nodos disponibles en la lista desplegable.

      Nota: Si ya se ha agregado un nodo del servidor proxy al sitio seleccionado en la Consola, se puede ver una lista de los nodos en la lista desplegable **Servidor proxy de Windows**.

   b. Si no se ha agregado ningún nodo del servidor proxy, realice los pasos siguientes:
      i. Haga clic en **Agregar**.
      ii. Aparecerá el cuadro de diálogo **Agregar servidor proxy de la recuperación asegurada**.
      iii. Especifique los detalles del servidor proxy y haga clic en **Aceptar**.
2. **Explore** la ubicación de la carpeta del disco duro virtual en el servidor proxy.

Especificación de la programación de la tarea de prueba de la recuperación asegurada

La ficha Programación permite especificar la programación de la tarea de prueba de la recuperación asegurada. Si no se especifica una programación, la tarea se inicia inmediatamente cuando se complete la tarea principal.

Siga estos pasos:

1. Haga clic en la ficha **Programación**.
2. Haga clic en **Agregar** y, a continuación, haga clic en **Agregar programación de la tarea de prueba de la recuperación asegurada**.

   Se muestra el cuadro de diálogo Agregación de la programación de la tarea de prueba de recuperación asegurada.
3. Especifique la programación y haga clic en **Guardar**.

   El cuadro de diálogo se cierra y la ficha Programación muestra la programación especificada.

Notas:

- Si el origen de la recuperación asegurada es Puntos de recuperación más reciente y Activar la programación de la recuperación asegurada, el valor predeterminado es 1. Como resultado, se verifica el más reciente de forma predeterminada.

  Para el valor <= 0, se prueban todos los puntos de recuperación no verificados.
- Si el origen de la recuperación asegurada es diaria/semanal/mensual y Activar la programación de la recuperación asegurada, el valor predeterminado es 9 (diaria 7 + 1 semanal + 1 mensual).

  Para el valor <= 0, se prueban todos los puntos de recuperación no verificados.
- Si no se desea utilizar el valor predeterminado, se puede agregar una clave de registro DWORD de 32 bits en la ubicación siguiente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AssuredRecovery\MaxNumberOfRecoveryPoint

Especificación de la configuración avanzada

La ficha Opciones avanzadas le ayudará a aplicar otros valores de configuración necesarios para completar el plan. Es una ficha opcional si no se necesita agregar más valores de configuración. Algunas de las opciones que se ven en la ficha **Opciones avanzadas** varían en función de las opciones seleccionadas en la ficha anterior. Por ejemplo, la opción Propiedades del latido solo está visible si se ha seleccionado Máquina virtual instantánea como Tipo de prueba en **Valores de configuración de la prueba**.

Propiedades del latido

Nota: La opción es visible solamente si se ha seleccionado Máquina virtual instantánea como el tipo de prueba.

Tiempo de espera

Especifica el tiempo más largo que el servidor proxy puede esperar a obtener el latido de la máquina virtual de la recuperación asegurada. Si la máquina virtual de la recuperación asegurada no está disponible más tiempo que el definido en el tiempo de espera, se produce un error en la tarea de prueba de la recuperación asegurada.

Frecuencia

Especifica la frecuencia con la que el servidor proxy comprueba el estado del latido de la máquina virtual de la recuperación asegurada.

Nota: Esta opción solamente se muestra cuando se ha seleccionado la replicación o la copia de seguridad de Linux basada en agente como el origen del punto de recuperación de la prueba de recuperación asegurada.

Puntos de control

Nota: La opción es visible solamente si se ha seleccionado Disco virtual instantáneo como el tipo de prueba.

Verificar el sistema de archivos

Verifica si el sistema de archivos y el tamaño del volumen son similares a lo que tiene el equipo de origen.

Ejecutar el comando de comprobación de disco

Comprueba la integridad de los datos mediante la ejecución del comando de comprobación de disco en los volúmenes que expone el disco virtual instantáneo.

Ubicación personalizada del comando en el servidor proxy

Nota: Esta opción solamente se muestra cuando se ha seleccionado la replicación o la copia de seguridad de Linux basada en agente como el origen del punto de recuperación de la prueba de recuperación asegurada.

Especifica el script personalizado que se almacena en el servidor proxy. Se puede explorar la información sobre el volumen del servidor proxy. Si se selecciona el tipo de recuperación asegurada de la máquina virtual instantánea, el script se copia en la máquina virtual y se ejecuta cuando se inicia la máquina virtual. Si se selecciona el tipo de recuperación asegurada del disco duro virtual instantáneo , el script se ejecuta en el servidor proxy.

Nota: La tarea de recuperación asegurada solo puede admitir el script .bat ejecutable de Windows o el binario ejecutable. Sin embargo, esta limitación no limita el uso de la tarea de recuperación asegurada. Se puede utilizar un script por lotes de Windows escrito para iniciar el script de PowerShell como, por ejemplo, el nombre test.bat con el contenido siguiente:

Powershell.exe -NoProfile -ExecutionPolicy ByPass -Command "& '%ScriptPath%\AR-check.ps1'"

Además, los siguientes argumentos pasan al script según sus requisitos.

- set PlanName=%1%

- set NodeName=%2%

- set ProxyServer=%3%

- set RecoveryPointName=%3%

- set MountPointRootPathName=%5% (aplicable solamente para el tipo de prueba Disco virtual instantáneo)

Como resultado, el archivo .bat se invoca y se ejecuta de la siguiente manera:

Para el tipo de prueba de la máquina virtual instantánea:

"%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName

Para el tipo de prueba del disco virtual instantáneo:

%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName MountPointRootPathName

Código de salida

Especifica el código de salida para una tarea realizada correctamente o para una tarea errónea.

Tarea correcta

Especifica que la tarea de recuperación asegurada está configurada para realizarse correctamente cuando el script devuelva el código de salida.

Tarea errónea

Especifica que la tarea de recuperación asegurada está configurada para realizarse erróneamente cuando el script devuelva el código de salida.

Tarea errónea si se ejecuta durante más tiempo

Especifica si el script se ejecuta durante más tiempo que el especificado.

Valor predeterminado: 15 minutos

Configuración del script anterior y posterior de Linux en el proxy

Nota: Esta opción solamente aparece cuando se ha seleccionado la replicación o la copia de seguridad de Linux basada en agente o sin agente basada en host como el origen del punto de recuperación de la prueba de recuperación asegurada.

Ejecutar en el servidor de copia de seguridad de Linux tras la finalización de la tarea de recuperación asegurada

Especifica el script ubicado en el proxy de Linux que se ejecuta después de la finalización de la tarea de recuperación asegurada en el servidor de copia de seguridad de Linux.

Ejecutar en la máquina virtual de recuperación asegurada tras el inicio de la máquina virtual de recuperación asegurada

Especifica el script ubicado en el proxy de Linux que se ejecuta tras iniciar la máquina virtual de recuperación asegurada en la máquina virtual de recuperación asegurada.

Interrumpir tarea si se ejecuta más de

Especifica si el script se ejecuta durante más tiempo que el especificado.

alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y especificar el tipo de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Notas: No está disponible para aquellas tareas que se ejecutan con el servidor de copia de seguridad de Linux.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuración del correo electrónico** y configure los detalles del servidor de correo electrónico y del servidor proxy.

Cómo establecer las contraseñas de copia de seguridad para uno o más nodos

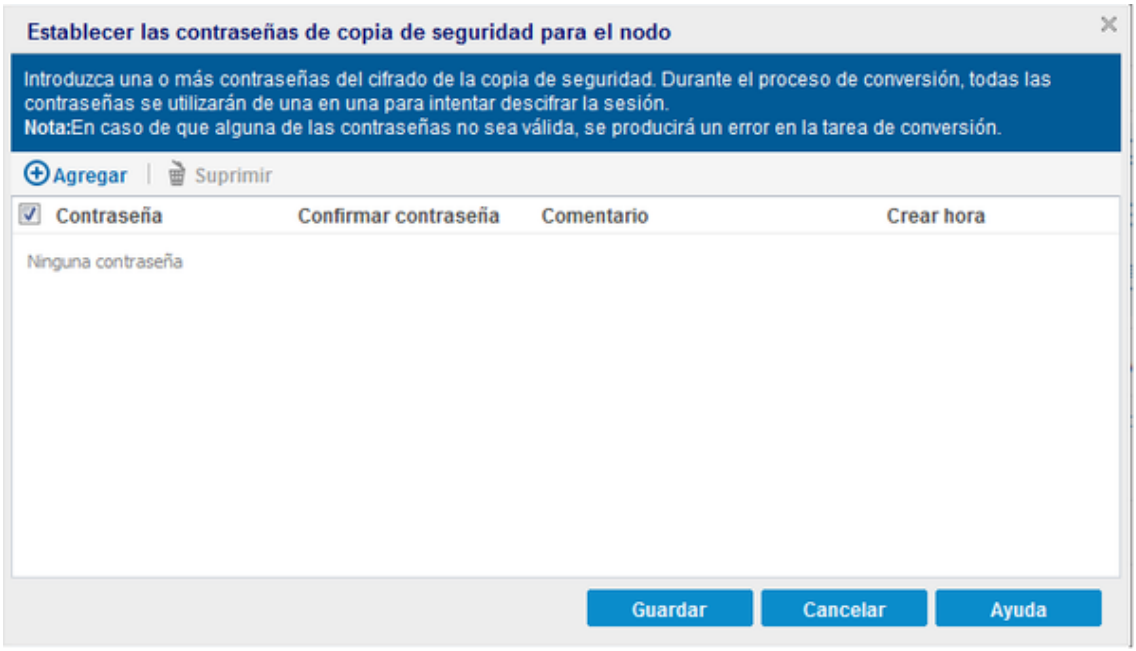
Para asegurarse de que la tarea de recuperación asegurada puede probar los puntos de recuperación replicados, la recuperación asegurada permite especificar contraseñas de la copia de seguridad para los datos. Las tareas que acceden a las sesiones de copia de seguridad utilizan contraseñas continuamente para descifrar la sesión.

Nota: Si ninguna de las contraseñas es válida, se producirá un error en la tarea que accede a la sesión de copia de seguridad.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.
3. En el panel central, haga clic con el botón secundario del ratón en el nodo y haga clic en **Establecer contraseñas de la copia de seguridad**.

   Aparecerá el cuadro de diálogo **Establecer las contraseñas de copia de seguridad para el nodo**.

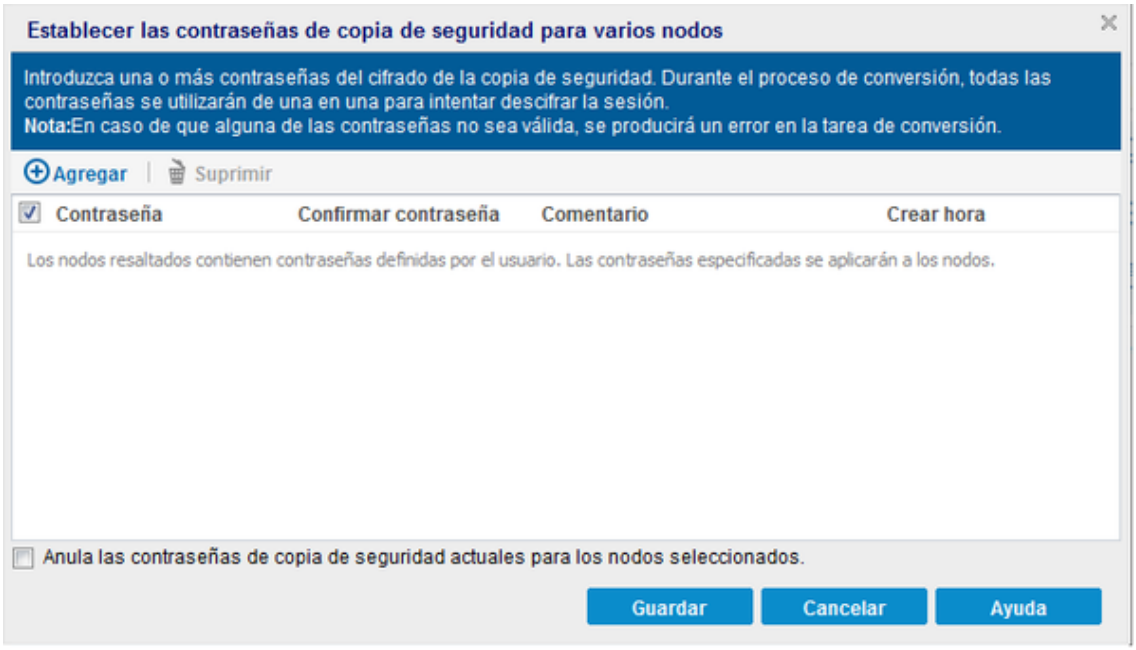


4. Realice las tareas siguientes en el cuadro de diálogo **Establecer contraseñas de la copia de seguridad** para uno o más nodos:

   Agregar: haga clic en **Agregar** para agregar una o más contraseñas de copia de seguridad a los nodos seleccionados.

Suprimir:haga clic en **Suprimir** para suprimir una o más contraseñas de copia de seguridad de los nodos seleccionados.

Nota: Se pueden anular las contraseñas de copia de seguridad actuales para varios nodos seleccionando la casilla de verificación **Anula las contraseñas de copia de seguridad actuales para los nodos seleccionados**.



5. Haga clic en **Guardar**.

   El cuadro de diálogo desaparece y las contraseñas de copia de seguridad se establecen para los nodos remotos seleccionados.

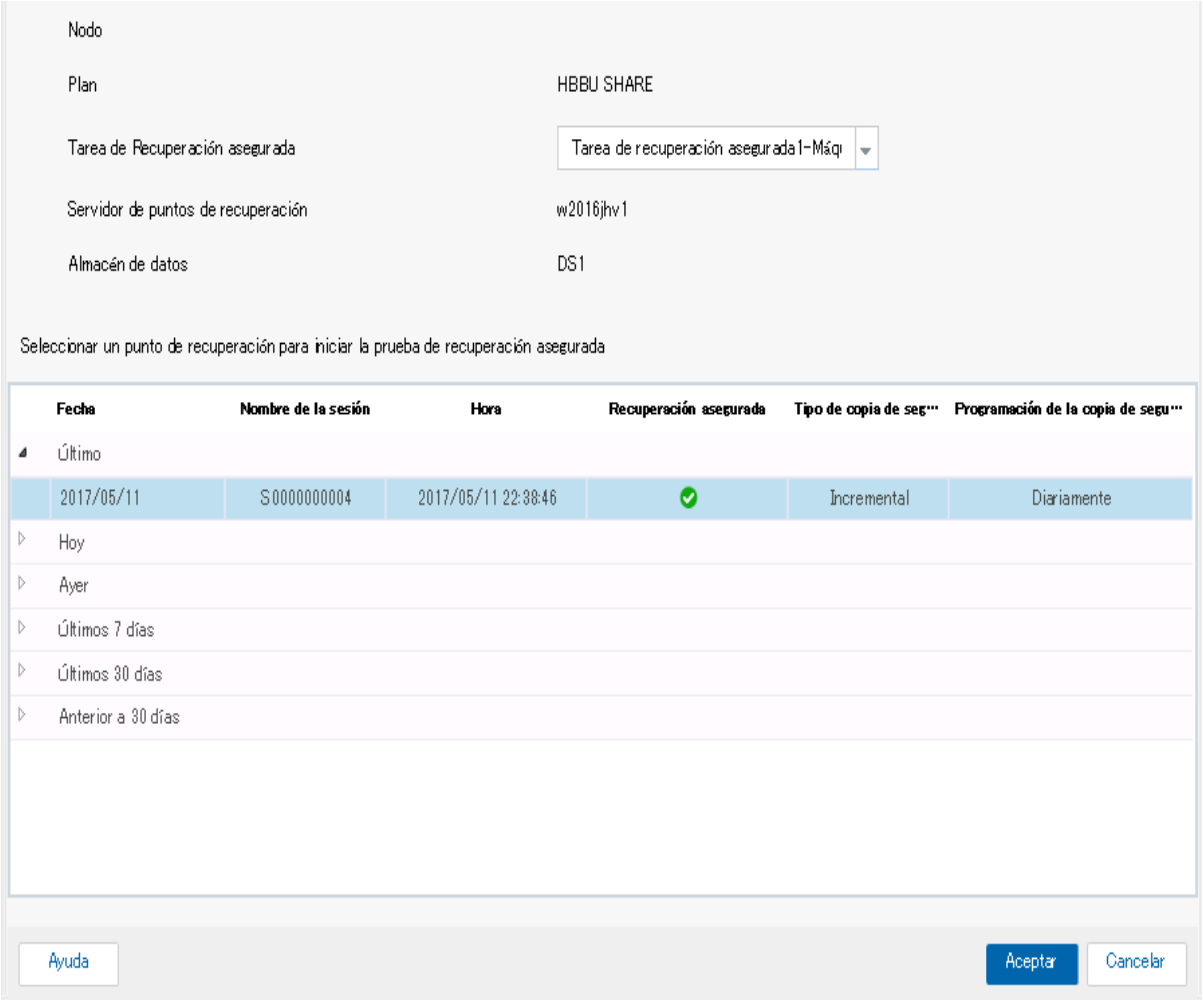
(Opcional) Ejecución manual de la tarea de prueba de recuperación asegurada

En Arcserve UDP, todos los planes, incluidas las tareas de recuperación asegurada, se realizan automáticamente y se controlan mediante la configuración de programación. Para las tareas de recuperación asegurada, además de la ejecución programada, Arcserve UDP le permite realizar una prueba manual de los nodos y planes para la prueba de recuperación asegurada. Este tema ofrece procedimientos independientes para llevar a cabo un prueba de recuperación asegurada manual del nodo y del plan.

Siga estos pasos para realizar una prueba de recuperación asegurada manual del nodo:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a Nodos y haga clic en **Todos los nodos**.
3. En el panel central, seleccione los nodos que tienen asignado un plan de recuperación asegurada y haga clic en **Acciones**.
4. En las opciones que se muestran para las Acciones, haga clic en **Ejecutar ahora la prueba de recuperación asegurada**.

   Se abre el cuadro de diálogo de la recuperación asegurada.



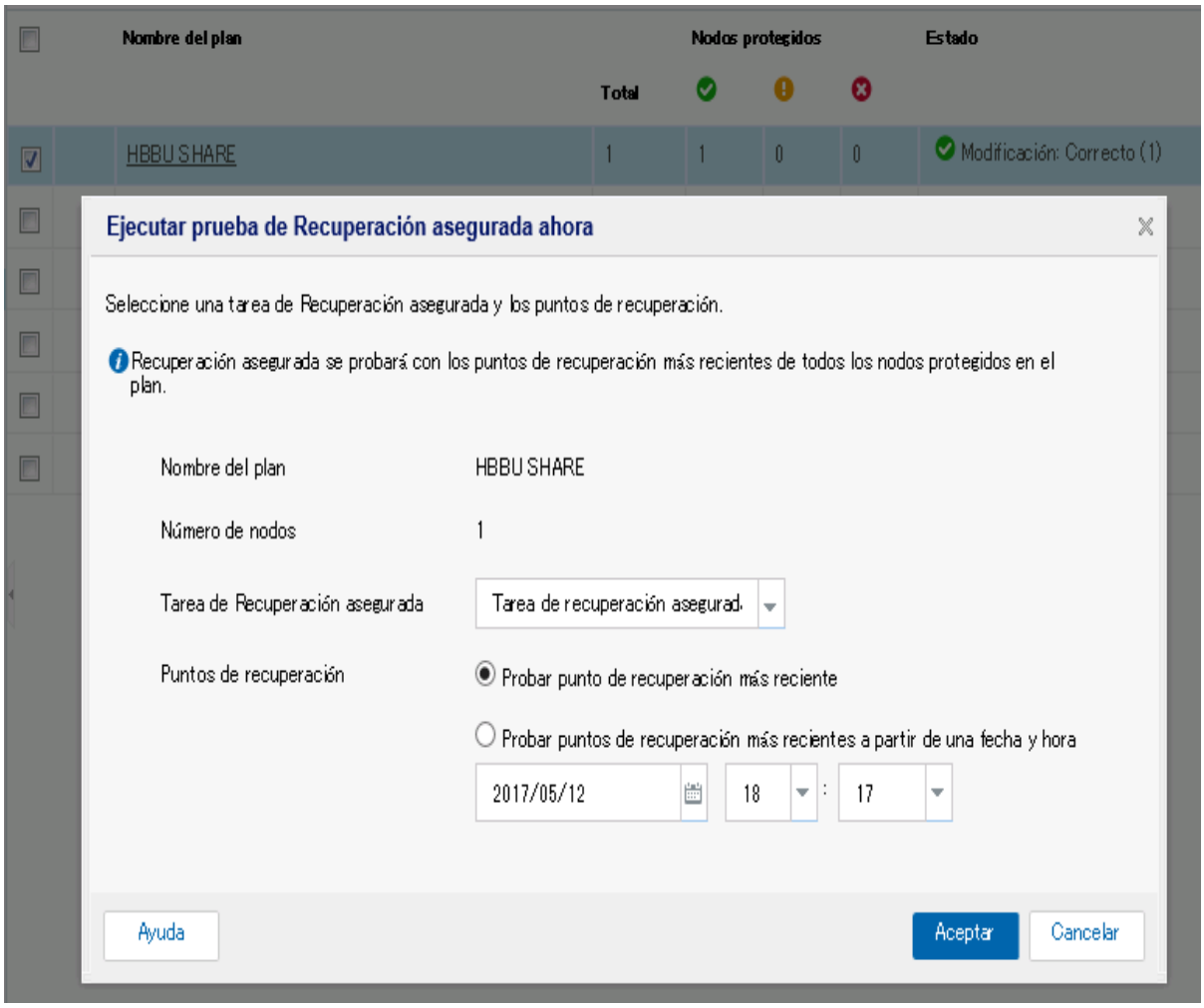
5. Seleccione una tarea de recuperación asegurada y un punto de recuperación, y haga clic en **Aceptar**.

   Se ejecuta la prueba de recuperación asegurada del nodo.

Siga estos pasos para realizar un prueba de recuperación asegurada manual del plan:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a Planes y haga clic en **Todos los planes**.
3. En el panel central, seleccione un plan de recuperación asegurada y haga clic en **Acciones**.
4. En las opciones que se muestran para las Acciones, haga clic en **Ejecutar ahora la prueba de recuperación asegurada**.

   Se abre el cuadro de diálogo de la recuperación asegurada.



5. Seleccione una tarea de recuperación asegurada y una de las opciones para el punto de recuperación, y haga clic en **Aceptar**.

   Se ejecuta la prueba de recuperación asegurada del plan.

Cómo crear un plan de copia de seguridad de la ruta UNC/NFS

Para proteger los directorios y los archivos que se encuentran en la ruta UNC/NFS, se debe crear un plan. El plan para la ruta UNC/NFS está formado por una tarea de copia de seguridad. Esta tarea de copia de seguridad le permite especificar los nodos que se desean proteger, el destino de la copia de seguridad y la programación de la copia de seguridad. El destino de la copia de seguridad es un servidor de punto de recuperación donde se desea almacenar sus datos de copia de seguridad. El destino es una carpeta compartida remota. Para la ruta UNC/NFS, el tamaño máximo de la copia de seguridad es de 128 TB.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Creación de un recurso compartido de archivos
3. Creación de un plan de copia de seguridad
4. (Opcional) Realización de una copia de seguridad manual
5. Creación de otras tareas en el plan UNC/NFS
6. Verificación de la copia de seguridad.

Revisión de las consideraciones y requisitos previos

Verifique que se han realizado las siguientes tareas de los requisitos previos:

1. Inicie sesión en la Consola.
2. Prepare un servidor proxy de copia de seguridad de la ruta UNC/NFS donde esté instalado el Agente de Arcserve Unified Data Protection para Windows.
3. Verifique que las credenciales de usuario disponen de al menos el permiso de lectura para la ruta UNC/NFS que desea proteger.

   Nota: Para agregar, actualizar y suprimir un nodo de la ruta UNC/NFS, consulte Cómo agregar y gestionar una ruta UNC/NFS.
4. Tenga un servidor de puntos de recuperación con un almacén de datos sin deduplicación o con un almacén de datos de deduplicación.
5. Cree un almacén de datos para almacenar los datos de copia de seguridad.
6. Cree un recurso compartido de archivos en el portal web de Nutanix Prism.

Consideraciones:

- Consumo de una licencia extra para rutas UNC. Para solucionar este problema, consulte la sección Solución de problemas.
- El proxy de copia de seguridad siempre es un equipo con Windows.
- Para que el plan de NFS de Nutanix funcione, NfsUtils debe estar preinstalado en el equipo proxy de la copia de seguridad (como es el caso del plan de NFS integrado).
- Para Nutanix File Server, si se produce un error en cualquiera de las FSVM del clúster, la otra FSVM toma la propiedad principal del servidor de archivos y la alta disponibilidad se activa para el clúster de FSVM.

Creación de un recurso compartido de archivos

La página Compartir/Exportar permite crear recursos compartidos de archivos distribuidos o estándares. Un recurso compartido distribuido o un recurso compartido principal es un repositorio donde residen los archivos personales de un usuario, mientras que el recurso compartido estándar o de uso general es un repositorio compartido por el grupo. Un recurso compartido distribuido se distribuye en los directorios de nivel superior mientras que el recurso compartido estándar se encuentra en una única máquina virtual del servidor de archivos (FSVM). Esta sección proporciona información sobre cómo crear un recurso compartido de archivos para realizar la copia de seguridad UNC/NFS para Nutanix Files.

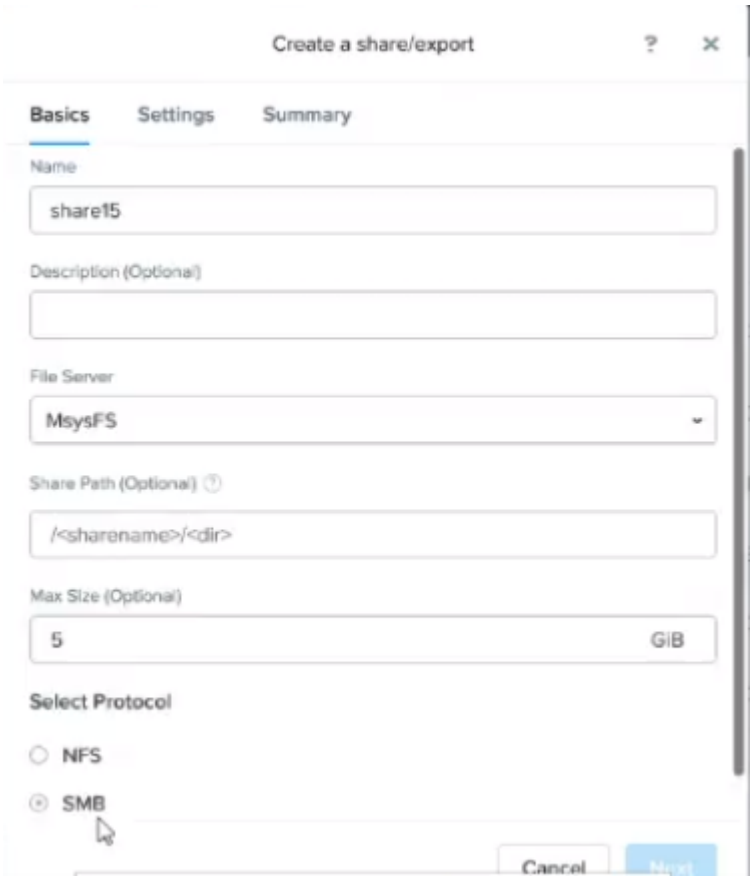
Siga estos pasos:

1. Inicie sesión en el portal web de Nutanix Prism.
2. Vaya a **File Server** en el menú principal y, a continuación, haga clic en **Share/Export** en el panel File Server.

   Aparecerá la ventana Create a share/export con la ficha Basics.
3. En la ficha Basics, haga lo siguiente y, a continuación, haga clic en **Next**:
   - Nombre: Introduzca un nombre para el recurso compartido.

     Nota: Las convenciones de nomenclatura para el nombre del recurso compartido son las siguientes:
     - Cada nombre debe ser exclusivo.
     - Los nombres no distinguen entre mayúsculas y minúsculas.
     - Los archivos admiten caracteres Unicode.
     - La longitud máxima del nombre es de 80 caracteres.
     - Un espacio en blanco o un carácter de espacio no pueden aparecer como primer o último carácter en el nombre.
     - Los nombres que terminan con $ son recursos compartidos ocultos.
   - Description (Opcional): Introduzca una descripción para el recurso compartido si es necesario.
   - File Server: En la lista desplegable, seleccione un servidor de archivos en el que resida el recurso compartido.
   - Share Path (Opcional): Proporcione la ruta del archivo al recurso compartido.
   - Max Size (Opcional): Introduzca el tamaño máximo del recurso compartido. De forma predeterminada, el tamaño está en GiB.
   - Select Protocol: Seleccione **SMB** como protocolo.

     Nota: Para activar la función multiprotocolo, seleccione la casilla de verificación **Enable multiprotocol access for NFS**.



4. En la ficha Settings, conserve los valores predeterminados o realice los cambios necesarios y, a continuación, haga clic en **Next**.

   Use "Distributed" share type instead of "Standard"

   Le permite crear un recurso compartido distribuido.

   Nota: De forma predeterminada, los recursos compartidos en las implementaciones de FSVM son estándar.

   Enable Self Service Restore

   Permite restaurar archivos de instantáneas anteriores.

   Enable File System Compression

   Permite ahorrar espacio y reducir los datos en el recurso compartido mediante la compresión en línea de los datos escritos.

   Nota: Asegúrese de desactivar la compresión a nivel de contenedor. Si se ha activado la compresión, la opción Enable File System Compression se desactiva.

   Enable Access Based Enumeration (ABE)

   Permite activar Access-Based Enumeration (ABE).

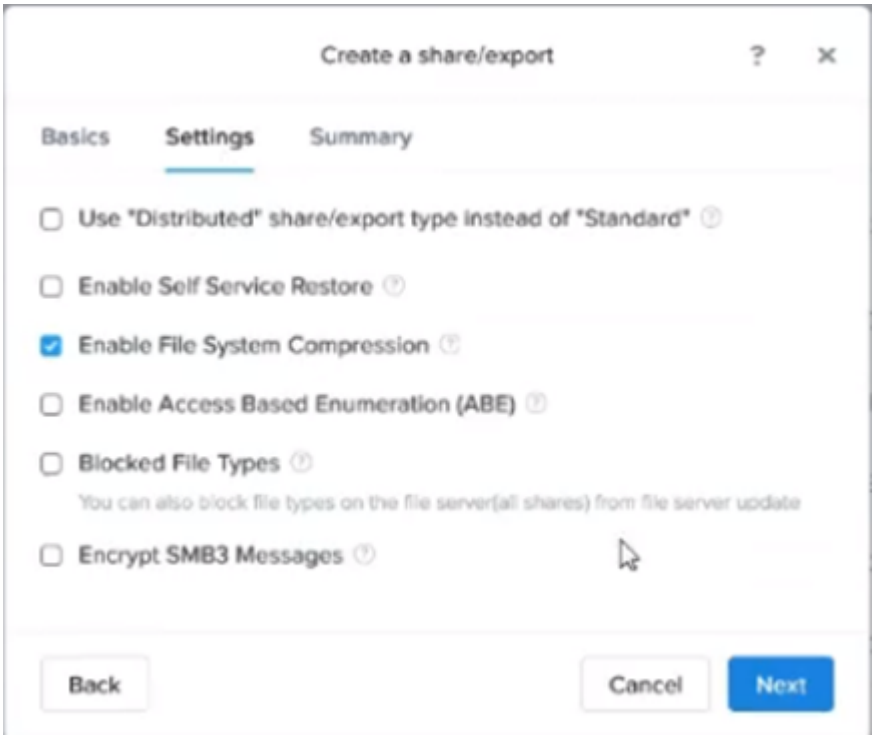
Blocked File Types

Permite especificar los tipos de archivos bloqueados.

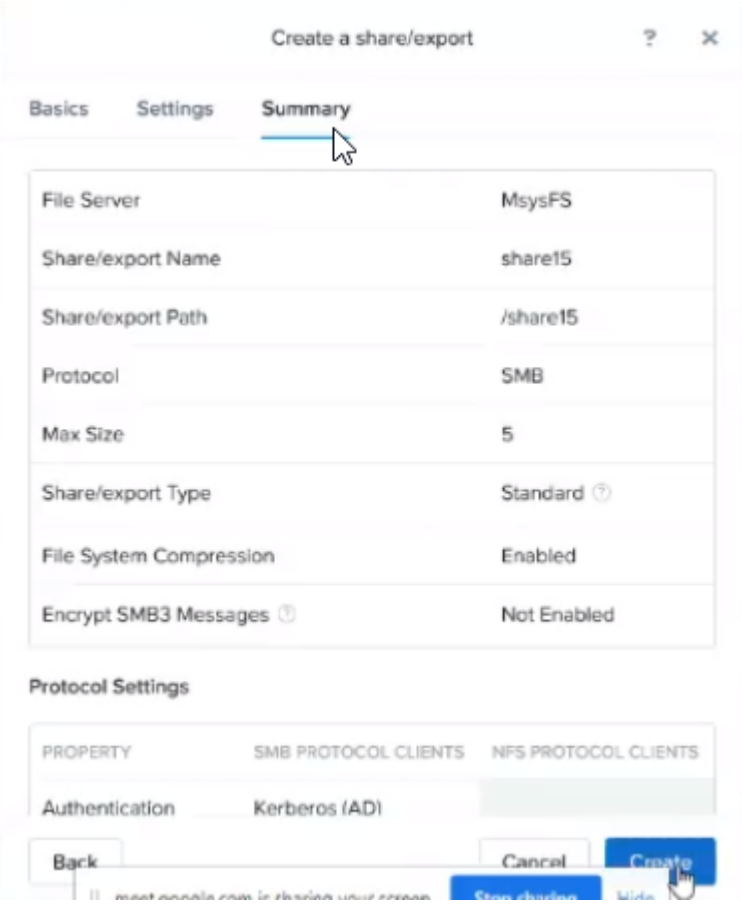
Introduzca una lista de tipos de archivos separados por comas que desee bloquear del recurso compartido.

Encrypt SMB3 Messages

Permite activar el cifrado de mensajes entre el servidor de archivos y el cliente.



5. En la página Summary, verifique los detalles y, a continuación, haga clic en **Create**.



Nota: Para realizar cambios en la configuración de las páginas anteriores, haga clic en **Back**.

El recurso compartido de archivos se crea correctamente.

Nota: A continuación, copie la ruta de montaje y, a continuación, asigne el recurso compartido recién creado en el UDP local. Para obtener más información, consulte el Paso 6 (a1) de Especificación del origen.

Creación de un plan de copia de seguridad con una tarea de la ruta UNC/NFS

Un plan de copia de seguridad incluye una tarea de copia de seguridad que realiza una copia de seguridad de un nodo físico y almacena los datos en un destino especificado. Cada tarea está formada por parámetros que definen el origen, destino, programación y otros detalles de la copia de seguridad.

Siga estos pasos:

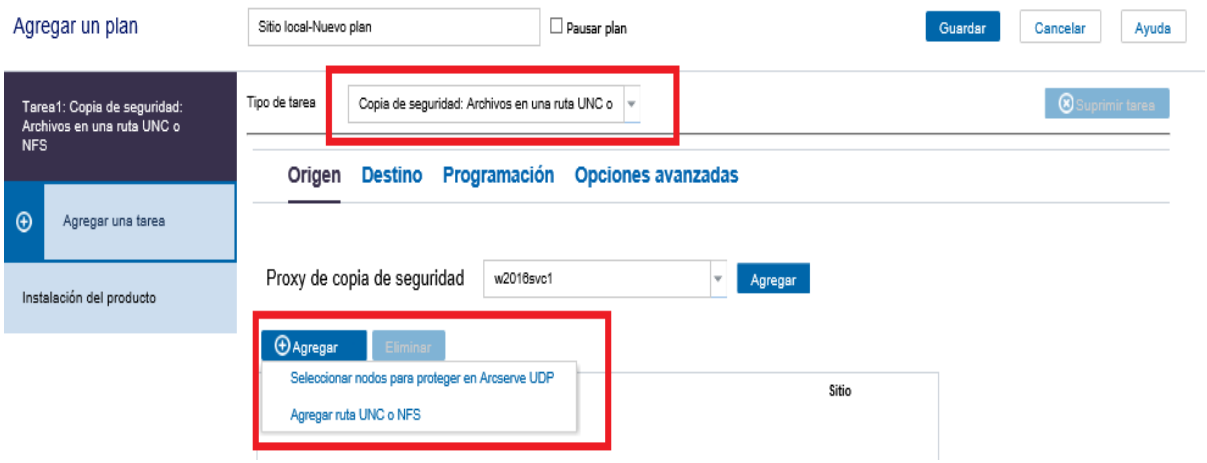
1. Inicie sesión en la Consola de Arcserve UDP.
2. Haga clic en la ficha **recursos**.
3. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
4. En el panel central, haga clic en **Agregar un plan**.

   Se abre la página Agregar un plan.
5. Introduzca un nombre del plan.
6. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
7. En la lista desplegable Tipo de tarea seleccione **Copia de seguridad: Archivos en la ruta UNC/NFS**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

La página Origen le permite especificar los nodos de origen que se desean proteger. Se pueden seleccionar más de un nodo del plan. Si no se ha agregado ningún nodo a la consola, se podrán agregar nodos al crear o modificar un plan en la página Origen. Se puede guardar un plan sin agregar ningún nodo de origen. El plan se implementa solamente después de agregar nodos de origen.

Siga estos pasos:

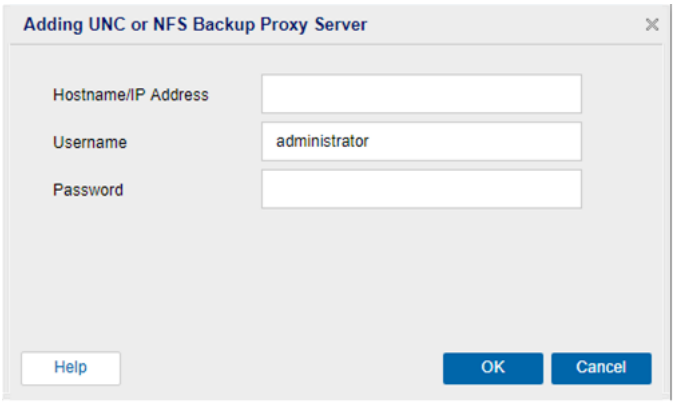
1. Haga clic en la ficha **Origen**.
2. Si se ha agregado el servidor proxy de copia de seguridad, selecciónelo en la lista desplegable Servidor proxy de la copia de seguridad.

   El servidor proxy es un nodo donde se instala el Agente de Arcserve Unified Data Protection para Windows.



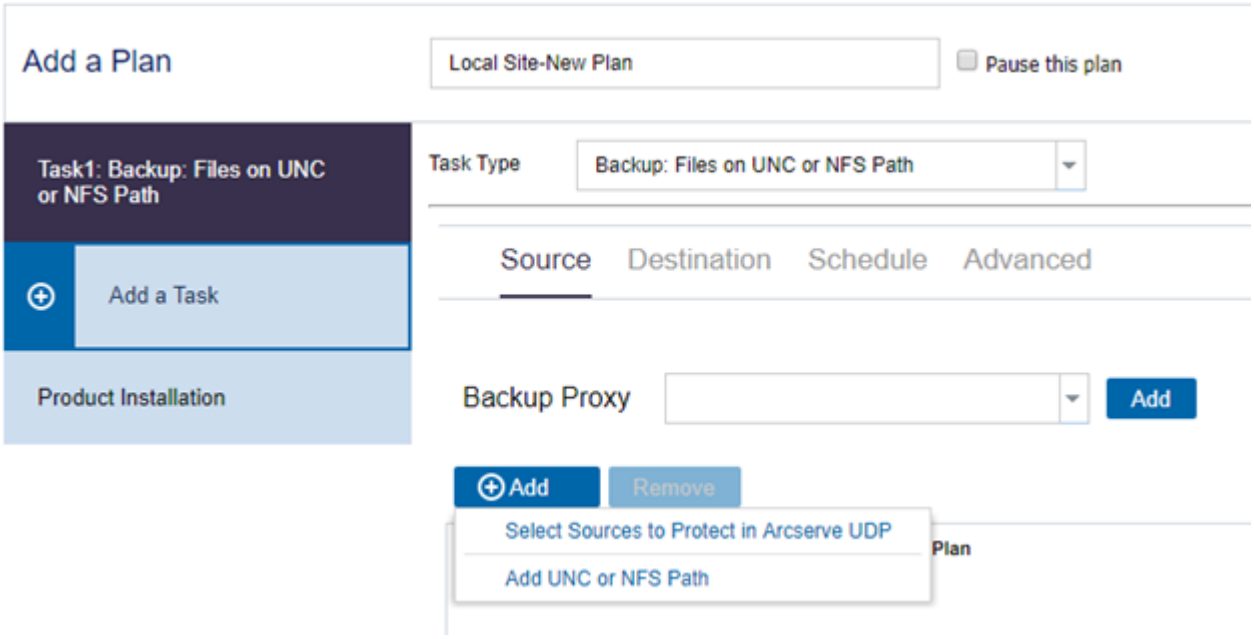
3. Si no se agrega el servidor proxy de la copia de seguridad, realice los pasos siguientes:
   a. Haga clic en **Agregar**.

      Se abre el cuadro de diálogo Agregar el servidor proxy de copia de seguridad de la ruta UNC o NFS.



   b. Especifique los detalles del servidor proxy y, a continuación, haga clic en **Aceptar**.

4. Para agregar el nodo Ruta UNC o NFS, haga clic en **+ Agregar** y, a continuación, seleccione una de las siguientes opciones:



Selección de orígenes para proteger en Arcserve UDP

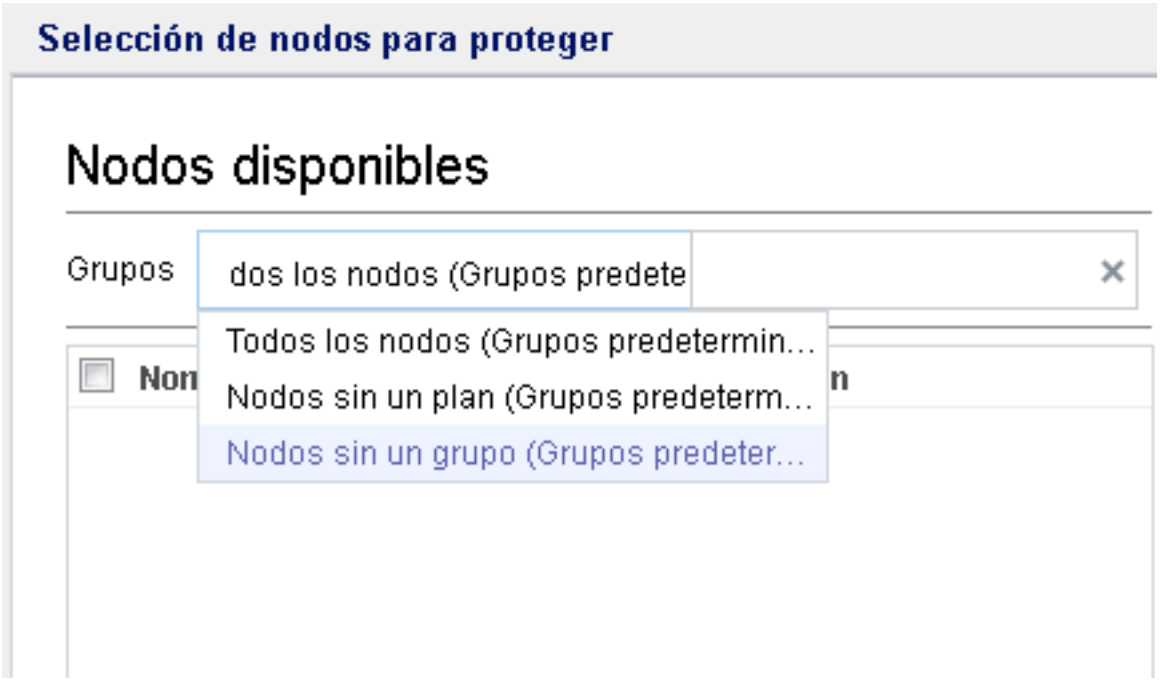
Aparece el cuadro de diálogo Selección de nodos para proteger y se pueden seleccionar los nodos en la lista que aparece. Seleccione esta opción si ya se han agregado los nodos a la consola.

Adición de una ruta UNC o NFS

Se abre el cuadro de diálogo Agregar nodos a la Consola de Arcserve UDP. Seleccione esta opción si no se han agregado los nodos y se desea agregarlos manualmente para la protección.

5. Si se selecciona la opción **Selección de orígenes para proteger en Arcserve UDP**, realice los pasos siguientes:

   a. (Opcional) Seleccione un filtro en la lista desplegable Grupos para filtrar nodos. Se pueden especificar palabras clave para filtrar más detalladamente los nodos.



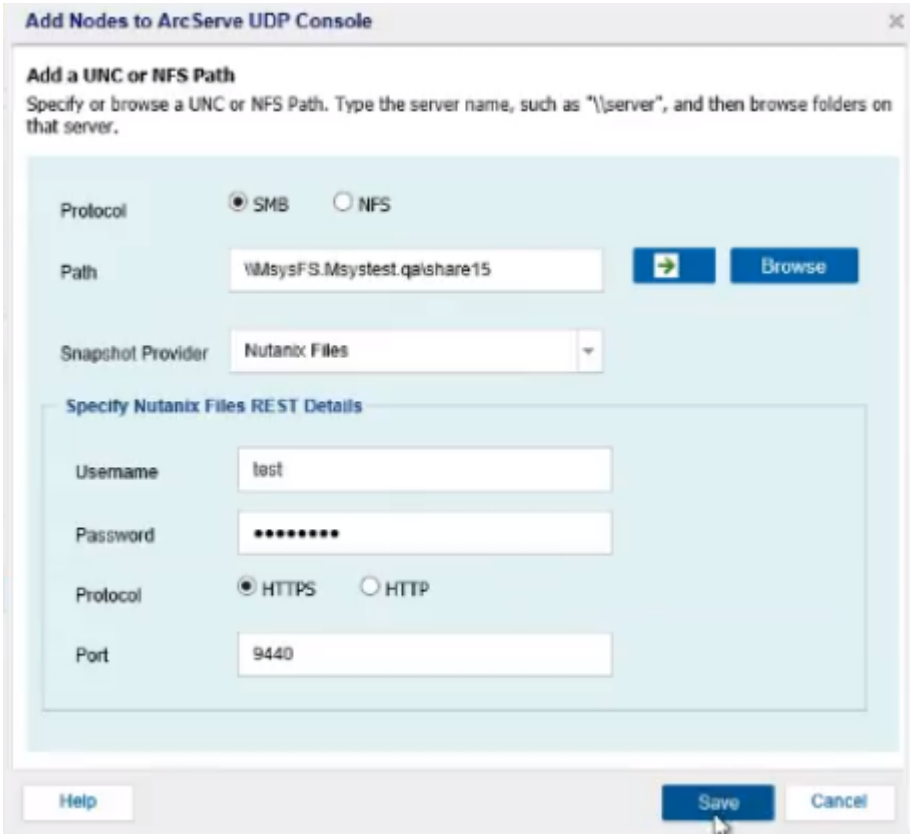
Los nodos se muestran en Nodos disponibles.

b. Seleccione los nodos en Nodos disponibles y, a continuación, haga clic en el botón **Agregar todos los nodos** (>>) o en el botón **Agregar nodos seleccionados** (>).

   Los nodos seleccionados se muestran en Nodos seleccionados.

c. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

6. Si se selecciona la opción **Agregar ruta UNC o NFS**, realice los pasos siguientes en la página Adición de una ruta UNC o NFS:



a. Seleccione **SMB** o **NFS** como protocolo.

- Si selecciona **SMB**, haga lo siguiente:

1. Introduzca la ruta UNC con el siguiente formato:

   *Hostname**share*

   Notas:

   - Al proporcionar el recurso compartido de Nutanix File como origen para la copia de seguridad con los archivos de Nutanix como proveedor de instantáneas, las copias de seguridad solo se pueden realizar en el nivel del recurso compartido pero no en el nivel de subcarpeta.
   - Para obtener la ruta UNC, haga lo siguiente:

     a. Seleccione el recurso compartido recién creado en el panel central.

     b. En la columna COMPARTIR/EXPORTAR DETALLES, en el panel Resumen, vaya a **Ruta**

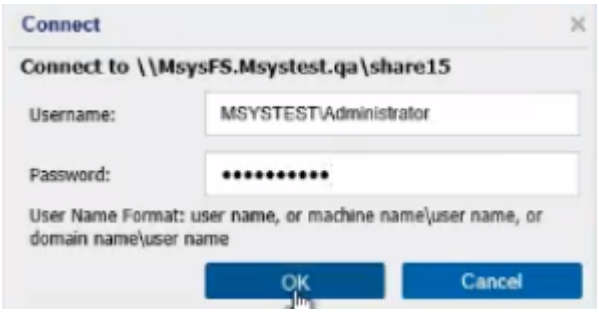
de montaje y, a continuación, copie la ruta de montaje.

Si la ruta UNC es válida, se activarán una flecha hacia la derecha y la opción Explorar.

2. Haga clic en la flecha hacia la derecha (>) para validar la ruta UNC.

   Aparece el cuadro de diálogo Conectar.

3. Introduzca el nombre de usuario y la contraseña según sea necesario y, a continuación, haga clic en **Aceptar**.



   El cuadro de diálogo Adición de nodos en la Consola de Arcserve UDP muestra la ruta UNC verificada.

- Si selecciona NFS, haga lo siguiente:

  1. Introduzca la ruta UNC con el siguiente formato:

     *Hostname**share*

  2. Seleccione una Codificación entre las opciones disponibles: ANSI, GB2312-80, KSC5601, BIG5, SHIFT-JIS, EUC-KR, EUC-TW, EUC-JP.

     El valor predeterminado es ANSI.

     Nota: Durante la copia de seguridad de una carpeta compartida de NFS, se omiten todos los archivos o carpetas cuyo nombre tenga un código de idioma no admitido o su nombre aparecerá como no deseado.

b. En la lista desplegable Proveedor de instantáneas, seleccione **Nutanix Files**.

c. Para el cuadro Especificar detalles de REST de Nutanix Files, especifique las credenciales siguientes:

   Nombre de usuario

Hace referencia al nombre de usuario creado por el usuario de la API de REST mediante Nutanix Prism.

Contraseña

Hace referencia a la contraseña del nombre de usuario.

Protocolo

Especifica el protocolo que se desea utilizar para comunicarse con el servidor de destino. Las opciones disponibles son HTTP y HTTPS.

Nota: Para una comunicación más segura, seleccione el protocolo HTTPS.

Puerto

Se refiere al número de puerto. El valor de puerto predeterminado es 9440 para acceder a las llamadas de la API de REST y a Prism.

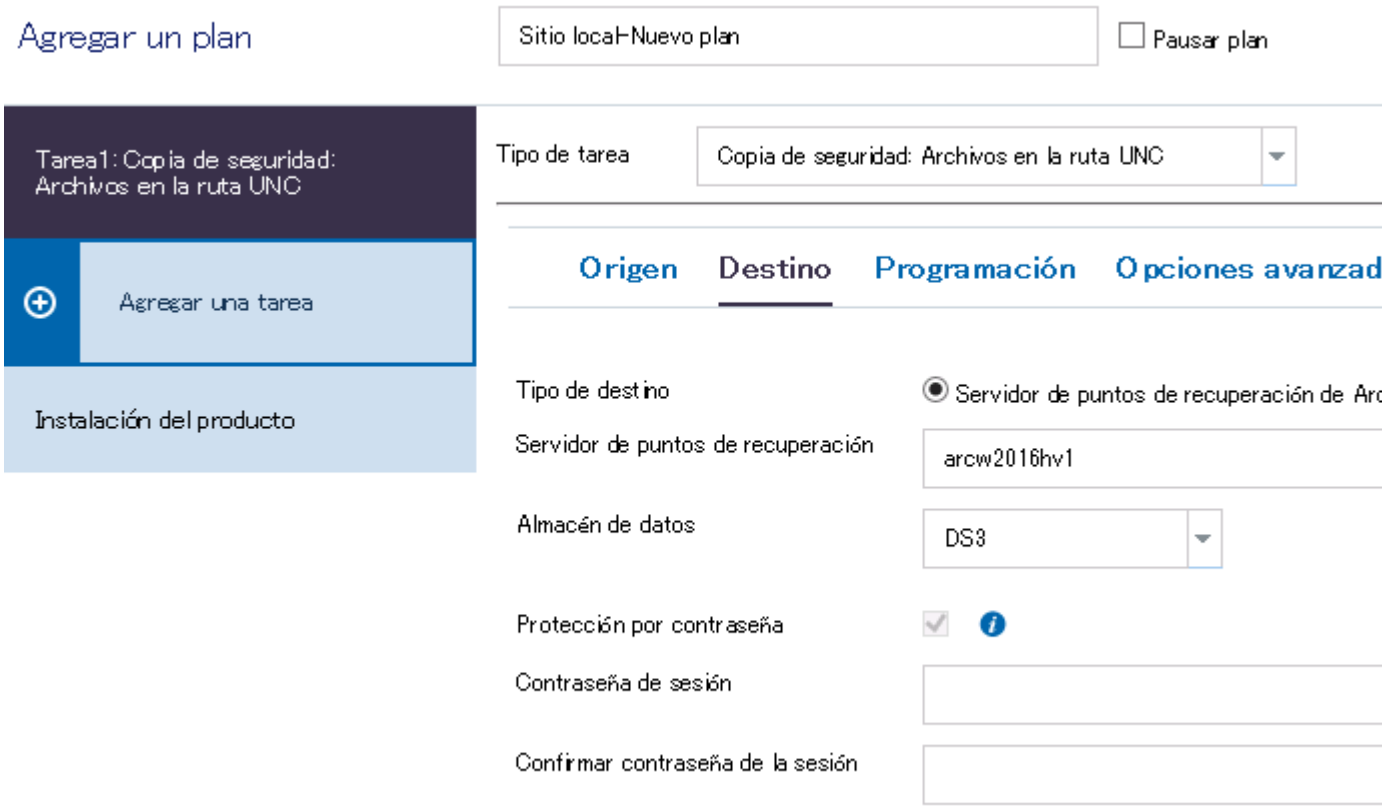
d. Haga clic en **Guardar**.

Nota: Si se produce un error en la conexión a Nutanix File Server, aparecerá un cuadro de diálogo de error o una ventana de notificación. Haga clic en **Aceptar** para cerrar el cuadro de diálogo de error.

Se especifica el origen.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.



Especifique los siguientes detalles:

- Tipo de destino: Compruebe si la opción **Servidor de puntos de recuperación de Arcserve UDP** está seleccionada de forma predeterminada.
- Servidor de punto de recuperación: Seleccione un servidor de puntos de recuperación en la lista desplegable.
- Almacén de datos: Seleccione un almacén de datos de la lista desplegable.

  La lista muestra todos los almacenes de datos que se han creado en el servidor de punto de recuperación especificado.
- Protección mediante contraseña: Proporcione una contraseña de sesión y, a continuación, vuelva a escribirla para confirmarla.

  Nota: La contraseña de la sesión es opcional cuando el destino de copia de seguridad es un almacén de datos del servidor de puntos de recuperación no

cifrado.

Se especifica el destino.

Especificación de la programación

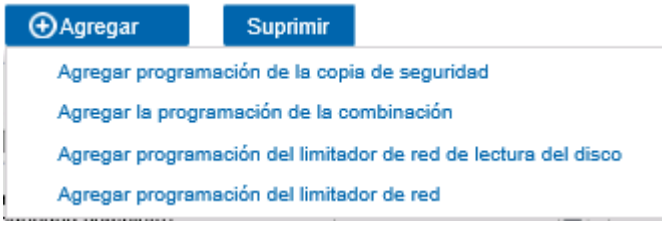
La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y se pueden proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

Siga estos pasos:

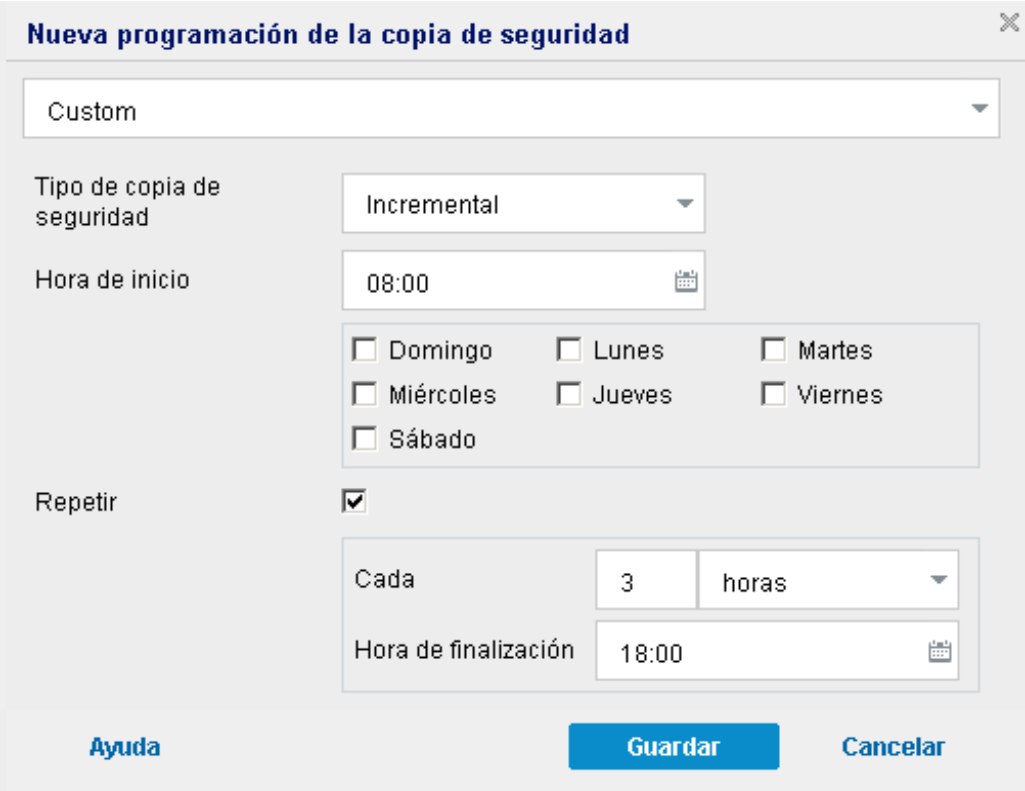
1. Agregue la programación de la copia de seguridad, de la combinación, del regulador de la lectura del disco y del regulador de la red.



Agregar programación de la copia de seguridad

a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

   Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Verificar

Especifica la programación de la copia de seguridad para las copias de seguridad de verificación.

Arcserve UDP verifica que los datos protegidos sean válidos y estén completos mediante una comprobación de confianza de la imagen de copia de seguridad almacenada en el origen de la copia de seguridad. Si es necesario, volverá a sincronizar la imagen. Una copia de seguridad de verificación se fijará en la copia de seguridad más reciente de cada bloque individual y comparará el contenido y la información con la de origen. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad de un bloque no coincide con la del origen (posiblemente por cambios en el sistema desde la última copia de seguridad), Arcserve UDP actualiza (resincroniza) la copia de seguridad del bloque que no coincide. Se puede utilizar también una copia de seguridad de verificación (aunque poco frecuentemente) para obtener la garantía de copia de seguridad completa sin utilizar el espacio necesario para una copia de seguridad completa.

Ventajas: produce una pequeña imagen de copia de seguridad si se compara con la copia de seguridad completa porque solamente se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventajas: el tiempo durante el cual se realiza la copia de seguridad es considerable puesto que todos los bloques de origen se comparan con los bloques de la última copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad

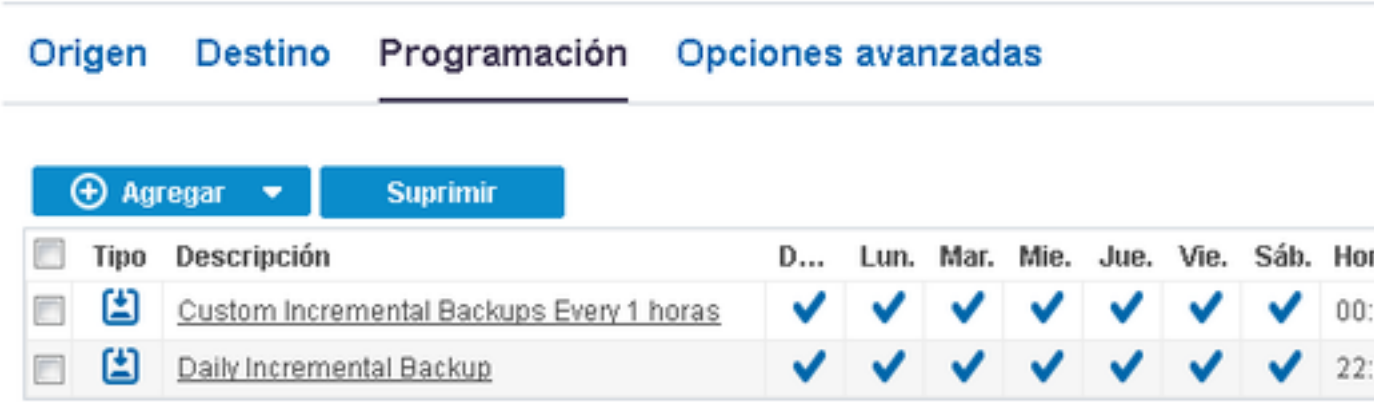
rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

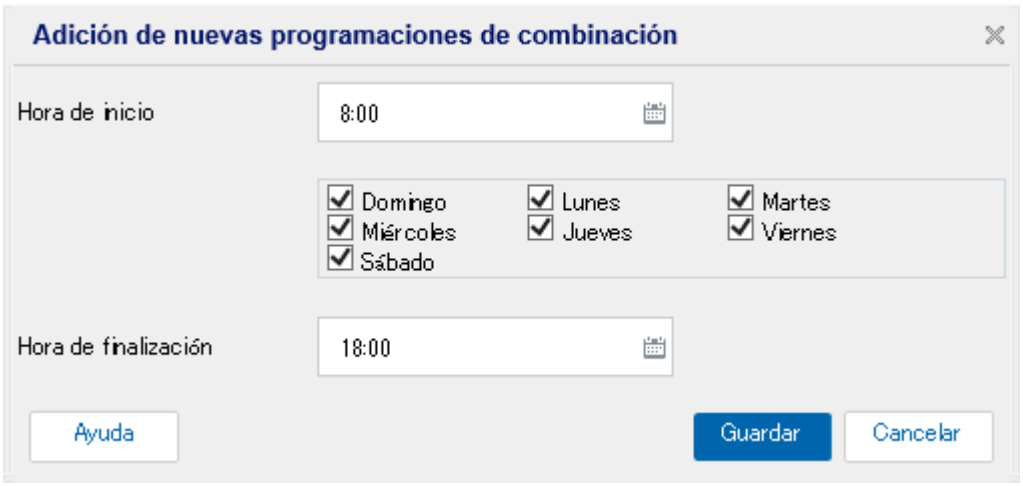
La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en **Agregar** y seleccione **Agregar programación de la combinación**.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.



b. Especifique la hora de inicio para iniciar la tarea de combinación.

c. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

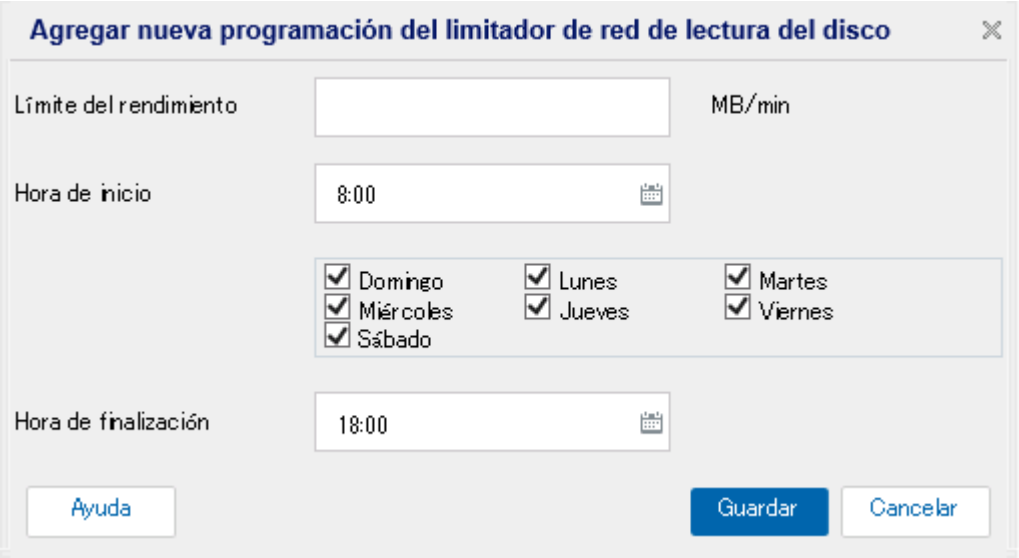
d. Haga clic en **Guardar**.

La Programación de la combinación se especifica y se muestra en la página **Programación**.

Adición de la programación del regulador de la lectura de disco

a. Haga clic en **Agregar** y seleccione **Agregar programación del regulador de la lectura de disco**.

   Se abre el cuadro de diálogo **Agregar nueva programación del regulador de la lectura de disco**.



b. Especifique el límite de rendimiento en MB por minuto.

c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

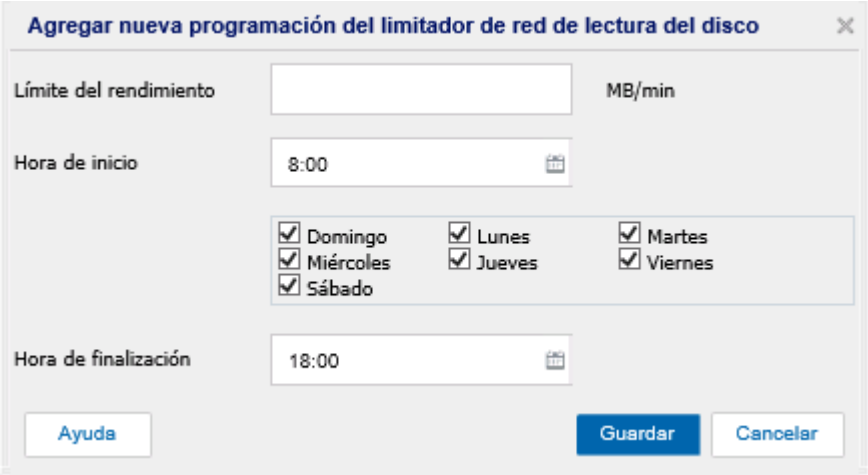
La programación del regulador de la lectura de disco se especifica y se muestra en la página **Programación**.

Adición de la programación del regulador de la red

Nota: La programación del regulador de la red solo aparece para la copia de seguridad basada en el Agente de Windows al definir un almacén de datos con la deduplicación activada como destino para el plan.

a. Haga clic en **Agregar** y seleccione **Agregar programación del regulador de la red**.

   Se abre el cuadro de diálogo **Agregar programación del regulador de la red**.



b. Especifique el límite del rendimiento en MB o kB por segundo.

   Nota: El valor mínimo predeterminado es de 500 kbps. Para cambiar el valor predeterminado, siga estos pasos:

   i. En la ruta del registro SOFTWARE\Arcserve\Unified Data Protection\Management\Console, agregue la clave MinNetworkThrottleValueInKpbs, cuyo tipo es REG_SZ, y establezca el valor.

   ii. Reinicie el servicio de gestión de Arcserve UDP.

   iii. Modifique el plan o cree uno nuevo.

   Se aplica el valor personalizado.

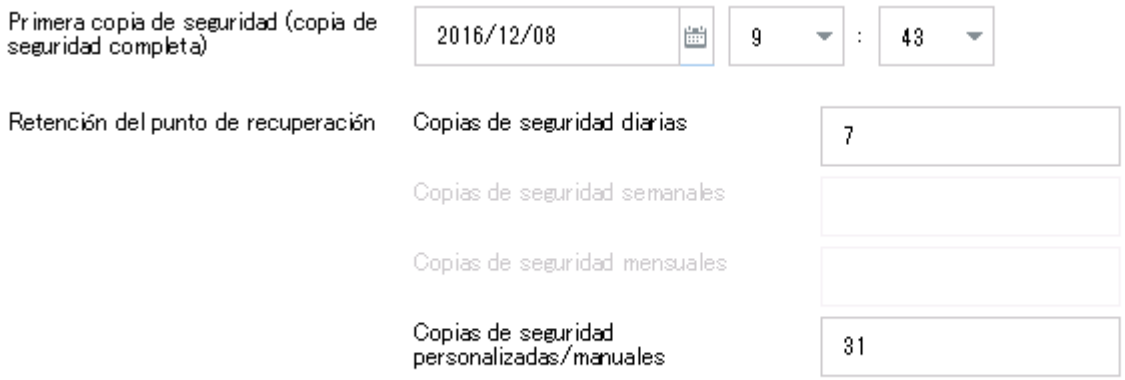
c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

La programación del regulador de la red se especifica y se muestra en la página **Programación**.

2. Especifique la hora de inicio para la copia de seguridad programada.



3. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

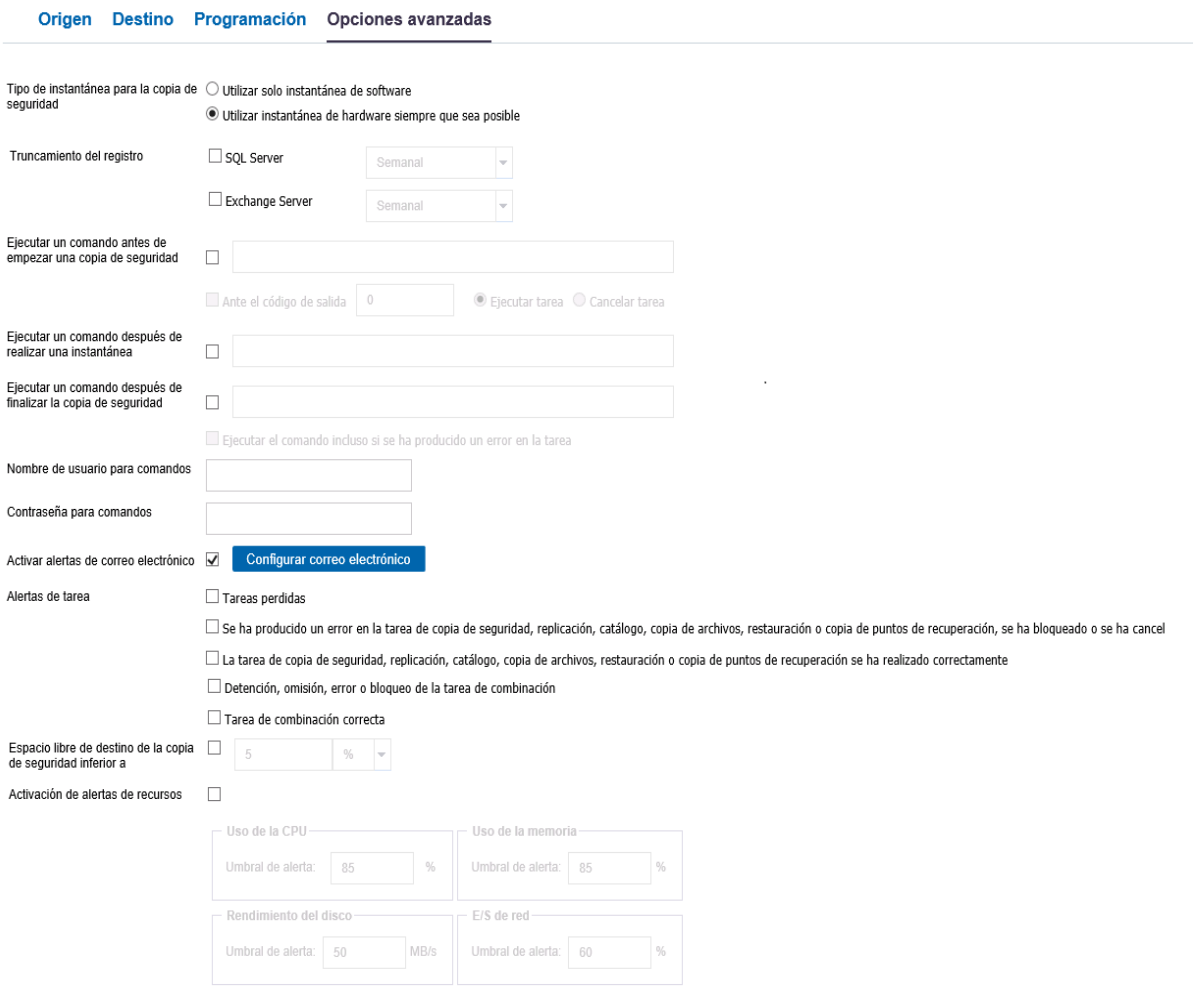
   Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo Programación de la copia de seguridad.

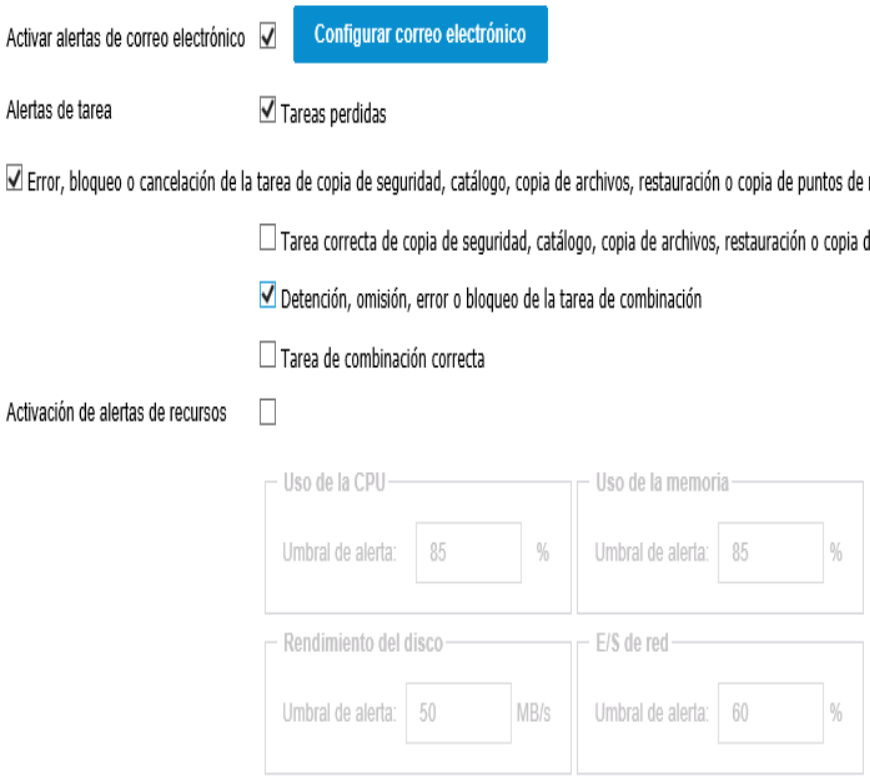
   Se especifica la programación.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye la configuración de registros de truncamiento, proporcionar la ubicación de los scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha Avanzada:


Origen
Destino
Programación
Opciones avanzadas
Tipo de instantánea para la copia de seguridad
Utilizar solo instantánea de software
Utilizar instantánea de hardware siempre que sea posible
Truncamiento del registro
SQL Server
Semanal
Exchange Server
Semanal
Ejecutar un comando antes de empezar una copia de seguridad
Ante el código de salida
0
Ejecutar tarea
Cancelar tarea
Ejecutar un comando después de realizar una instantánea
Ejecutar un comando después de finalizar la copia de seguridad
Ejecutar el comando incluso si se ha producido un error en la tarea
Nombre de usuario para comandos
Contraseña para comandos
Activar alertas de correo electrónico
Configurar correo electrónico
Alertas de tarea
Tareas perdidas
Se ha producido un error en la tarea de copia de seguridad, replicación, catálogo, copia de archivos, restauración o copia de puntos de recuperación, se ha bloqueado o se ha cancel
La tarea de copia de seguridad, replicación, catálogo, copia de archivos, restauración o copia de puntos de recuperación se ha realizado correctamente
Detención, omisión, error o bloqueo de la tarea de combinación
Tarea de combinación correcta
Espacio libre de destino de la copia de seguridad inferior a
5
%
Activación de alertas de recursos
Uso de la CPU
Umbral de alerta:
85
%
Uso de la memoria
Umbral de alerta:
85
%
Rendimiento del disco
Umbral de alerta:
50
MB/s
E/S de red
Umbral de alerta:
60
%



Siga estos pasos:

1. Especifique los siguientes detalles:

   Tipo de instantánea para la copia de seguridad

   Seleccione una de las opciones siguientes para la instantánea de copia de seguridad:

   Utilizar solo instantánea de software

   Especifica que el tipo de copia de seguridad utiliza solo la instantánea de software. Arcserve UDP no buscará la instantánea de hardware. La instantánea de software utiliza menos recursos en las máquinas virtuales. Se puede utilizar esta opción si el servidor tiene una velocidad de configuración y procesamiento menor.

   Utilice la instantánea de hardware siempre que sea posible

   Especifica que el tipo de copia de seguridad primero busca una instantánea de hardware. Si se cumplen todos los criterios, el tipo de copia de seguridad utiliza la instantánea de hardware.

   Nota: Para obtener más información sobre los criterios de instantánea de hardware, consulte los requisitos previos.

   Cómo truncar un registro

Le permite especificar la programación para truncar los registros de SQL Server y Exchange Server. Se puede especificar la programación como **Diaria**, **Semanal** o **Mensual**.

Activación del borrado definitivo de los registros cada hora para SQL a través de un conmutador de registro

- Configure la configuración del plan. Seleccione la opción SQL Server en la sección Truncar registro en la ficha Avanzadas y, a continuación, seleccione Diariamente.
- Establezca la clave de registro en el equipo de SQL Server en los hosts del Agente de UDP. PurgeSqlLogPerHour es el intervalo en horas para borrar definitivamente el registro de SQL.

  Ruta: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

  Nombre del valor: PurgeSqlLogPerHour (indica el intervalo en horas para borrar definitivamente el registro de SQL).

  Tipo de valor: REG_DWORD

Nombre de usuario

Le permite especificar el usuario que se autoriza para ejecutar un script.

Contraseña

Le permite especificar la contraseña del usuario autorizado para ejecutar el script.

Ejecutar un comando antes de empezar una copia de seguridad

Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta completa donde está almacenado el script. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de seguridad continuará cuando el script devuelva el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detendrá cuando el script devuelva el código de salida.

Ejecutar un comando después de realizar una instantánea

Le permite ejecutar un script después de realizar la instantánea de la copia de seguridad. Especifique la ruta completa donde está almacenado el script.

Para ejecutar el script posterior a la instantánea incluso durante un error de instantánea, seleccione **Ejecutar el comando incluso se ha producido un error en la instantánea**.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta completa donde está almacenado el script.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y se pueden especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy. Para obtener más información sobre cómo configurar el correo electrónico, consulte la sección Configuración de la configuración del correo electrónico y alertas.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de tareas que se desea recibir.

Cómo activar las alertas de recurso

Le permite especificar un umbral para el Uso de CPU, Uso de memoria, Rendimiento del disco y E/S de la red. Se puede proporcionar el valor en porcentaje. Se recibirá un correo electrónico cuando se exceda el valor de Umbral de alerta.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en Guardar.

Los cambios se guardan y se muestra una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **Recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar.

El plan de copia de seguridad se crea y se implementa automáticamente en el nodo de origen. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

(Opcional) Realización de una copia de seguridad manual

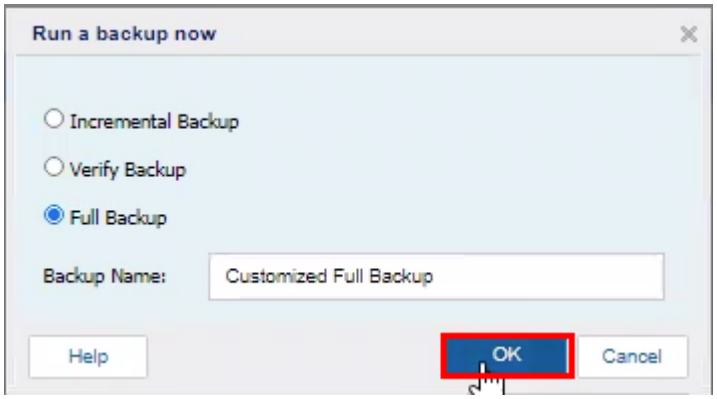
Normalmente se realizan copias de seguridad automáticamente y las controlan los valores de configuración de programación. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario. Por ejemplo, si tiene una programación de repetición para las copias de seguridad completas, incrementales y de resincronización y desea hacer cambios importantes en el equipo, se deberá realizar una copia de seguridad manual inmediata sin necesidad de esperar a la siguiente copia de seguridad programada.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Vaya a **recursos** > **Plan** > **Todos los planes**.

   La lista de todos los planes se muestra en el panel central.
3. Haga clic con el botón secundario del ratón en el plan y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
4. En el cuadro de diálogo Ejecutar una copia de seguridad ahora, seleccione el tipo de copia de seguridad que desea realizar y, a continuación, especifique el nombre de la copia de seguridad si es necesario.



A continuación se especifican las opciones disponibles:

Copia de seguridad incremental

Inicia una copia de seguridad incremental del equipo. Una copia de seguridad incremental sólo hará una copia de seguridad de los bloques que han cambiado desde la copia de seguridad anterior.

Nota: Si está realizando una copia de seguridad por primera vez, la copia de seguridad completa se iniciará automáticamente aunque haya seleccionado la opción Copia de seguridad incremental.

Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Ésta es la manera más óptima de realizar copias de seguridad.

Copia de seguridad de verificación

Inicia una copia de seguridad de verificación de su equipo examinando la copia de seguridad más reciente de cada bloque individual y comparando el contenido y la información con la original. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad para un bloque no coincide con la de origen, el Agente de Arcserve UDP (Windows) actualizará (resincronizará) la copia de seguridad del bloque que no coincida.

Ventaja: Una imagen de copia de seguridad muy pequeña se produce cuando se compara con una copia de seguridad completa porque solo se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventaja: El tiempo de copia de seguridad es lento porque todos los bloques del disco de origen se comparan con los bloques de la última copia de seguridad.

Copia de seguridad completa

Inicia una copia de seguridad completa del equipo o los volúmenes seleccionados.

Notas:

- Si se agrega un nuevo volumen al origen de la copia de seguridad, se realizará una copia de seguridad completa del nuevo volumen agregado, independientemente del método de copia de seguridad general seleccionado.
- Si no se especifica ningún nombre de copia de seguridad, de forma predeterminada se denominará Copia de seguridad completa/incremental/de verificación personalizada.

5. Haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.

6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.

7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   Nota: Solamente se puede restaurar una tarea cada vez. Si intenta iniciar una tarea de copia de seguridad manualmente cuando se está ejecutando otra tarea al mismo tiempo, aparecerá un mensaje de alerta para informar de que otra tarea está en ejecución y solicitará intentarlo de nuevo más tarde.

   La copia de seguridad manual se realiza correctamente.

Otras tareas en el plan UNC/NFS

Se puede seguir la tarea del plan de la ruta UNC/NFS con otras tareas. Se pueden crear tareas de seguimiento como, por ejemplo, la copia del punto de recuperación, la copia en cinta, la replicación en la nube de Arcserve, la replicación y la replicación a un servidor de puntos de recuperación gestionado remotamente.

Tarea de copia de puntos de recuperación

Le permite copiar los puntos de recuperación a una carpeta local o compartida, o a la nube.

Copia en cinta

Le permite almacenar el punto de recuperación en cinta mediante la integración con Arcserve Backup.

Tarea de replicación

Le permite crear una tarea de replicación de los datos de la copia de seguridad desde un servidor de punto de recuperación a otro servidor de punto de recuperación.

Replicar a un servidor RPS remoto

Le permite crear una tarea para replicar o enviar datos a un servidor de puntos de recuperación remoto.

Replicar en la nube de Arcserve

Le permite crear una tarea para replicar o enviar datos a un servidor de puntos de recuperación de la nube.

Prueba de recuperación asegurada

Permite verificar la accesibilidad y asegurar la recuperación de los datos.

Verificación de la copia de seguridad.

Para verificar la tarea de copia de seguridad, confirme que se ha creado correctamente el plan de copia de seguridad. Después de verificar que el plan se ha creado correctamente, confirme si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Se puede verificar el estado de las tareas de copia de seguridad en la ficha **Tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga uno de estos métodos para verificar las tareas de copia de seguridad:

Método 1

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas finalizadas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Método 2

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Tareas correctas**.

   La lista de tareas de copia de seguridad completadas aparecerá en el panel central.
3. Haga clic en la tarea que desea verificar.

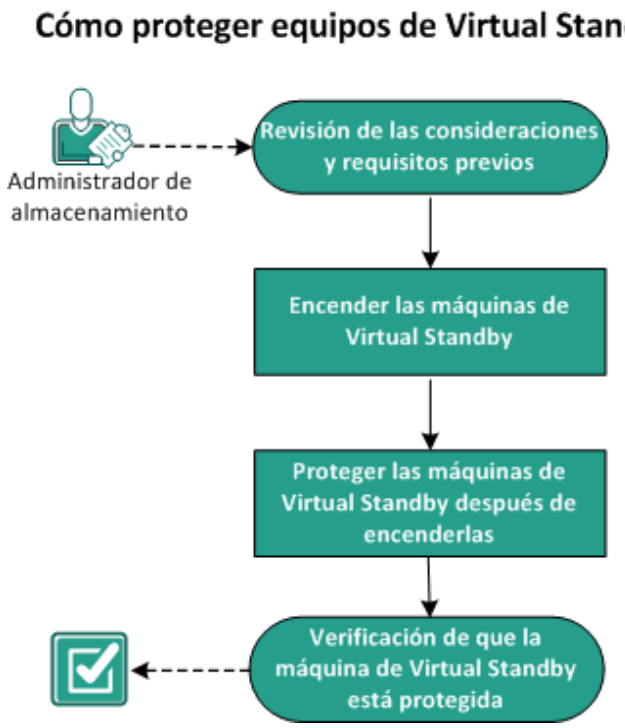
   Se actualiza el panel derecho.
4. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
5. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Cómo proteger equipos de Virtual Standby

Se puede realizar una copia de seguridad de equipos de Virtual Standby y evitar que los datos se corrompan. Antes de proteger el equipo, tiene que encenderlo.

El diagrama siguiente muestra el proceso para proteger máquinas de Virtual Standby:



¿Qué hacer a continuación?

- Revisión de las consideraciones y requisitos previos
- Encendido de las máquinas de Virtual Standby
- Protección de las máquinas de Virtual Standby después de encenderlas
- Verificación de que la máquina de Virtual Standby está protegida

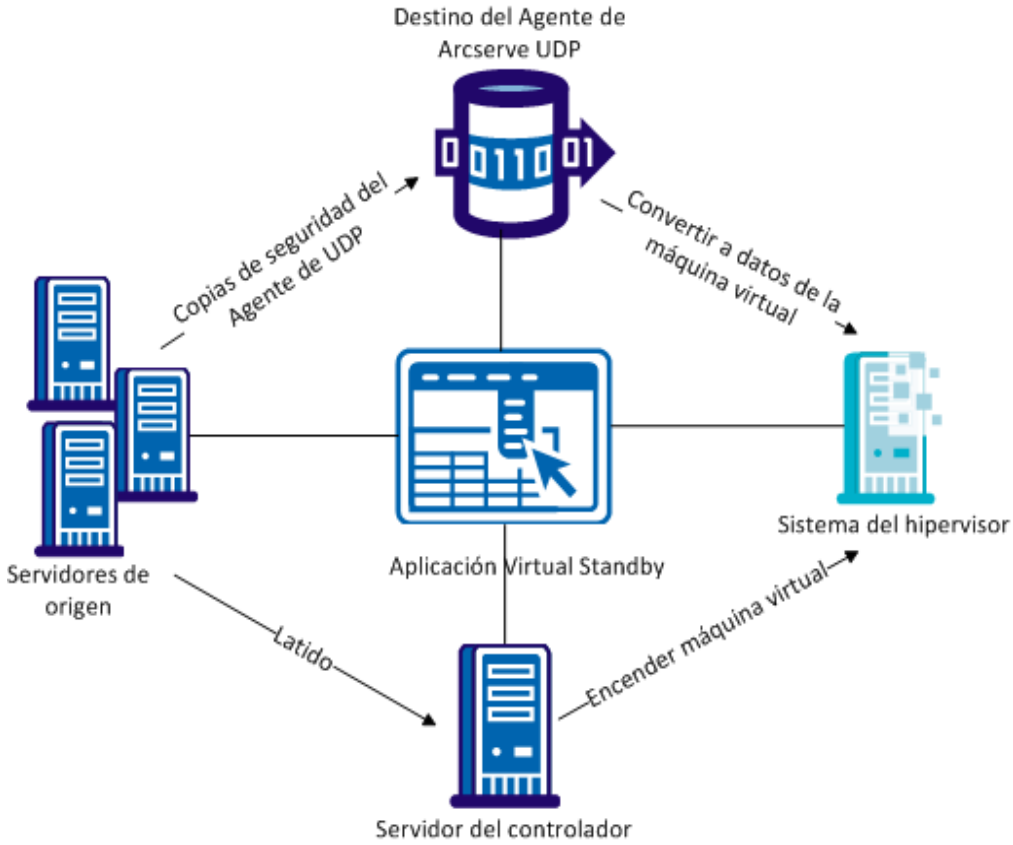
Revisión de las consideraciones y requisitos previos

Verifique que se han realizado las siguientes tareas de los requisitos previos:

- Se ha iniciado sesión en la Consola
- Se tiene preparada un una máquina de Virtual Standby.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Encendido de las máquinas de Virtual Standby

Se pueden encender máquinas de Virtual Standby y proteger las máquinas virtuales después de que se enciendan las máquinas. El diagrama siguiente describe el flujo del proceso para encender las máquinas virtuales:



Encendido de las máquinas de Virtual Standby a partir de instantáneas de puntos de recuperación

Virtual Standby se puede configurar de manera que encienda máquinas de Virtual Standby a partir de las instantáneas de puntos de recuperación de forma automática cuando el servidor controlador no detecta ninguna pulsación del servidor de origen. Opcionalmente, se pueden encender máquinas de Virtual Standby a partir de las instantáneas de puntos de recuperación de forma manual en el caso de que se produzca una emergencia o un error en el servidor de origen, o en el caso de que sea conveniente dejar sin conexión un servidor de origen para realizar tareas de mantenimiento.

Nota: Los pasos siguientes describen cómo encender manualmente las máquinas de Virtual Standby a partir de instantáneas de puntos de recuperación. Para obtener más información sobre cómo permitir que Virtual Standby encienda de forma automática instantáneas de puntos de recuperación, consulte Adición de una tarea de Virtual Standby a EC2 al plan.

Siga estos pasos:

1. En la ficha **Recursos**, vaya al grupo de nodos de **Virtual Standby**.

   Los nodos de Virtual Standby se muestran en el panel central.

2. En el panel central, seleccione el nodo y haga clic en **Máquina virtual en espera**.

   Se abre el cuadro de diálogo **Máquina virtual en espera**.

3. En el cuadro de diálogo **Máquina virtual en espera**, realice las tareas siguientes:

   - Seleccione una fecha y hora de inicio de la instantánea del punto de recuperación para encender la máquina virtual.

     Nota: Si la máquina virtual en espera no se ha configurado todavía, aparecerá el vínculo La red de la máquina virtual en espera no se ha configurado.

     a. Haga clic en este vínculo para configurar la red.

     b. Haga clic en **Guardar**. Se guardan los valores de configuración de la máquina virtual de Virtual Standby.

     c. Haga clic en **Cerrar** y aparecerá el cuadro de diálogo **Instantáneas del punto de recuperación**.

   - Haga clic en **Encender la máquina virtual**.

     La máquina virtual se encenderá utilizando los datos de la instantánea del punto de recuperación.

Nota: Tras encender la máquina virtual es posible que el sistema solicite reiniciar el equipo una o más veces. Este comportamiento ocurre porque el controlador de Amazon PV está instalado en la máquina virtual.

Tras encender máquinas de Virtual Standby a partir de instantáneas de puntos de recuperación, puede que sea necesario completar las siguientes tareas:

- Activar el sistema operativo de Windows que se está ejecutando en la máquina virtual.
- Iniciar el Agente de Arcserve Unified Data Protection para Windows en la máquina virtual.
- Actualizar Arcserve UDP con el nombre de host, dirección IP y credenciales de inicio de sesión para la máquina virtual.
- Asignar el nodo a un plan.

Nota: Esta tarea solamente es necesaria cuando se desean crear instantáneas de puntos de recuperación para la máquina virtual que se ha encendido.

Encendido de máquinas de Virtual Standby desde el Administrador de Hyper-V

Para encender manualmente máquinas virtuales de Virtual Standby, una buena práctica es realizar el encendido desde la pantalla Máquina virtual en espera del servidor de Arcserve Unified Data Protection. Para obtener más información, consulte Encendido de máquinas virtuales de Virtual Standby a partir de instantáneas de puntos de recuperación. Sin embargo, si desea iniciar las máquinas virtuales de Virtual Standby a partir del servidor Hyper-V, lo puede hacer mediante el Administrador de Hyper-V.

Nota: El Administrador de Hyper-V permite acceder a las instantáneas de puntos de recuperación creadas por Virtual Standby para proteger el nodo. No se deberían suprimir las instantáneas. Cuando se suprimen las instantáneas, la relación entre los datos de las instantáneas pierde la coherencia en el momento en que se vuelve a ejecutar una tarea de Virtual Standby. Si existe incoherencia en los datos no es posible encender máquinas virtuales de Virtual Standby correctamente.

Siga estos pasos:

1. Inicie sesión en el servidor de Hyper-V que controla los nodos que se están protegiendo.
2. Inicie el gestor de Hyper-V y realice los pasos siguientes:
   a. Haga clic en Inicio, Todos los programas, Herramientas administrativas y a continuación seleccione Administrador de Hyper-V.

      Se abrirá el Administrador de Hyper-V.

   b. Desde el árbol del directorio del Administrador de Hyper-V, expanda el Administrador de Hyper-V y haga clic en el servidor de Hyper-V Server que contiene la máquina virtual que desea encender.

      Las máquinas virtuales asociadas con el servidor de Hyper-V especificado aparecen en la lista Máquinas virtuales, en el panel central.
3. Realice una de las tareas siguientes:
   - **Para encender la máquina virtual utilizando la instantánea más reciente:** En la lista Máquinas virtuales, haga clic con el botón secundario del ratón en la máquina virtual que desee encender y seleccione Iniciar en el menú emergente.
   - **Para encender una máquina virtual utilizando una instantánea antigua:**

a. En la lista Máquinas virtuales, haga clic en la máquina virtual que desea encender.

   Las instantáneas asociadas con la máquina virtual aparecerán en la lista Instantáneas.

b. Haga clic con el botón secundario del ratón en la instantánea que desee utilizar para encender la máquina virtual y haga clic en Aplicar, en el menú emergente.

   Se abrirá el cuadro de diálogo Aplicar instantánea.

c. Haga clic en Aplicar.

d. En la lista Máquinas virtuales, haga clic con el botón secundario del ratón en la máquina virtual que desea encender y seleccione Iniciar en el menú emergente.

   La máquina de Virtual Standby está encendida.

Si es necesario, se puede realizar la copia de seguridad de las máquinas virtuales y crear instantáneas de puntos de recuperación después de encender la máquina virtual.

Encendido de máquinas de Virtual Standby desde el cliente de VMware vSphere

Para encender manualmente máquinas de Virtual Standby, una buena práctica es realizar el encendido de las máquinas virtuales desde cuadro de diálogo Máquinas virtuales en espera de Arcserve UDP. Para obtener más información, consulte Encendido de máquinas virtuales de Virtual Standby a partir de instantáneas de puntos de recuperación. Sin embargo, si desea iniciar las máquinas de Virtual Standby desde el servidor de ESX o desde el sistema del servidor de vCenter, lo puede hacer a través del cliente de VMware vSphere.

Nota: El cliente de VMware vSphere permite acceder a las instantáneas de puntos de recuperación creadas por Virtual Standby para proteger el nodo. No se deberían suprimir las instantáneas. Cuando se suprimen las instantáneas, la relación entre los datos de las instantáneas pierde la coherencia en el momento en que se vuelve a ejecutar Virtual Standby. Si existe incoherencia en los datos no es posible encender máquinas de Virtual Standby correctamente.

Siga estos pasos:

1. Abra el cliente de VMware vSphere e inicie sesión en el servidor de ESX o en el sistema del servidor vCenter que controla los nodos que se están protegiendo.
2. En el árbol de directorio, expanda el sistema del servidor de ESX o del vCenter. A continuación busque y haga clic en la máquina virtual que desea encender.
3. Realice una de las tareas siguientes:

   Para encender una máquina virtual utilizando la instantánea más reciente: Haga clic en la ficha Procedimientos iniciales y, a continuación, haga clic en Encender la máquina virtual que aparece en la parte inferior de la pantalla.

   Para encender una máquina virtual utilizando una instantánea antigua:

   a. Haga clic en el botón Gestor de instantáneas en la barra de herramientas.

      Se abrirá el cuadro de diálogo Instantáneas para (nombre de la máquina virtual) y mostrará una lista de las instantáneas que se encuentran disponibles para la máquina virtual.

   b. En la lista de instantáneas, haga clic en la instantánea que desea utilizar para encender la máquina virtual y a continuación haga clic en Ir a.

      La máquina de Virtual Standby está encendida.

   Si es necesario, se puede realizar la copia de seguridad de las máquinas virtuales y crear instantáneas de puntos de recuperación después de encender la máquina virtual.

Protección de las máquinas de Virtual Standby después de encenderlas

Tras el encendido de una máquina de Virtual Standby (manual o automáticamente), la tarea de copia de seguridad del Agente de Arcserve Unified Data Protection para Windows y la tarea de Virtual Standby no se ejecutan de acuerdo a su programación. Se tiene que configurar manualmente la máquina de Virtual Standby para protegerla.

Siga estos pasos:

1. Modifique el **Prefijo del nombre de la máquina virtual** en la tarea de Virtual Standby.

   Cuando se encienden máquinas de Virtual Standby, la aplicación define los nombres de máquina virtual de las máquinas virtuales encendidas como una concatenación de la opción **Prefijo del nombre de la máquina virtual**, especificada en la tarea de Virtual Standby, y el nombre de host del nodo de origen.

   Ejemplo:

   - Prefijo del nombre de la máquina virtual: AA_
   - Nombre de host del nodo de origen: Servidor1
   - Nombre de la máquina virtual en espera: AA_Servidor1

   Tras encender las máquinas de Virtual Standby, se pueden producir conflictos en el nombre de las máquinas virtuales si no se modifica el **Prefijo del nombre de la máquina virtual** en la tarea de Virtual Standby. Este tipo de problemas se producen cuando los nodos de origen y las máquinas de Virtual Standby se encuentran en el mismo hipervisor.

   Si es necesario, se pueden actualizar otros valores de configuración de la tarea de Virtual Standby. Opcionalmente, se puede crear una nueva tarea de Virtual Standby para proteger la máquina virtual de Virtual Standby.

2. Una vez implementado el plan en la máquina de Virtual Standby, se debe reanudar la tarea de Virtual Standby.

   Para obtener más información, consulte Pausa y reanudación de tareas de Virtual Standby.

3. Después de implementar el plan, inicie sesión en el Agente de Arcserve Unified Data Protection para Windows en la máquina en espera virtual y programe un método de repetición para la tarea de copia de seguridad del Agente de Arcserve Unified Data Protection para Windows.

Para obtener más información, consulte la *Guía del usuario del Agente de Arcserve Unified Data Protection para Windows*.

Nota: Pausa y reanudación de tareas de Virtual Standby.

Verificación de que la máquina de Virtual Standby está protegida

Verifique que las máquinas de Virtual Standby están protegidas confirmando que los puntos de recuperación válidos están disponibles en el destino de la copia de seguridad.

Siga estos pasos:

1. Inicie sesión en el destino de la copia de seguridad y vaya a la carpeta del destino de la copia de seguridad.
2. Verifique que la copia de seguridad de la máquina de Virtual Standby ha tenido y que los puntos de recuperación están disponibles.

   Se ha verificado la máquina de Virtual Standby.

   Las máquinas de Virtual Standby están correctamente protegidas.

Cómo proteger máquinas virtuales instantáneas

Se puede realizar una copia de seguridad de máquinas virtuales instantáneas y evitar que los datos se corrompan. Antes de proteger la máquina virtual instantánea, es posible que se tenga que encender.

El diagrama siguiente muestra el proceso para proteger máquinas virtuales instantáneas:



¿Qué hacer a continuación?

- Revisión de las consideraciones y requisitos previos
- Encendido de las máquinas virtuales instantáneas
- Protección de las máquinas virtuales instantáneas
- Verificación de que la máquina virtual instantánea está protegida

Revisión de las consideraciones y requisitos previos

Verifique que se han realizado las siguientes tareas de los requisitos previos:

- Se ha iniciado sesión en la Consola.
- Hay una máquina virtual instantánea preparada.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Encendido de máquinas virtuales instantáneas a partir de un punto de recuperación

Se pueden crear máquinas virtuales instantáneas y proteger las máquinas virtuales manualmente desde el punto de recuperación después de que se enciendan las máquinas.

Cuando se crea una máquina virtual instantánea, se puede seleccionar Iniciar ahora o Iniciar más tarde. Seleccione la opción Iniciar ahora para iniciar la máquina virtual instantánea inmediatamente después de la creación correcta. En caso contrario, se deberá encender la máquina virtual instantánea de forma manual.

Solo se pueden encender máquinas virtuales instantáneas a partir de un punto de recuperación cuando se desea crear un punto de recuperación para la máquina virtual que se ha encendido.

Siga estos pasos:

1. Desde la ficha **recursos**, vaya a la página **Infraestructura**: Grupo del nodo **Máquinas virtuales instantáneas**.

   Los nodos de la máquina virtual instantánea aparecen en el panel central.

2. En el panel central, seleccione el nodo, haga clic en **Acciones** y, a continuación, haga clic en **Encender** en la lista desplegable.

   La máquina virtual se encenderá utilizando los datos de la instantánea del punto de recuperación.

   Nota: Tras encender la máquina virtual es posible que el sistema solicite reiniciar el equipo una o más veces. Este comportamiento ocurre porque VMware instala VMware Tool en la máquina virtual o Windows Hyper-V instala los servicios de integración en la máquina virtual.

   Una vez encendidas las máquinas virtuales de Virtual Standby desde las instantáneas de puntos de recuperación, es posible que deba completar las tareas siguientes:

   - Activar el sistema operativo de Windows que se está ejecutando en la máquina virtual.
   - Iniciar el Agente de Arcserve Unified Data Protection para Windows en la máquina virtual.
   - Actualizar Arcserve UDP con el nombre de host, dirección IP y credenciales de inicio de sesión para la máquina virtual.

Protección de una máquina virtual instantánea al encenderse

Tras el encendido de una máquina virtual instantánea (manual o automáticamente), la tarea de copia de seguridad de Agente de Arcserve Unified Data Protection para Windows y la tarea de Virtual Standby no se ejecutan de acuerdo con su programación. Se tiene que configurar manualmente la máquina virtual instantánea para protegerla.

Siga estos pasos:

1. Agregue una máquina virtual instantánea a la Consola.

   Nota: Se puede agregar un nodo especificando manualmente los detalles del nodo o importando máquinas virtuales desde servidores de ESX/vCenter y servidores de Hyper-V.

   Para obtener más información, consulte Adición de nodos.

2. Agregar un destino.

   Un destino puede ser un servidor de punto de recuperación, carpeta local o carpeta compartida remota.

3. Cree un plan para proteger el nodo de la máquina virtual instantánea.

   Un plan es un grupo de tareas para gestionar la copia de seguridad, la replicación y la creación de equipos de Virtual Standby.

   Nota: Se puede crear un plan con la tarea de copia de seguridad de Windows basada en el agente o con la tarea de copia de seguridad sin agente basada en el host.

4. Realizar tareas como copia de seguridad, crear Virtual Standby y replicación.

   Para obtener más información, consulte la *Guía del usuario del Agente de Arcserve UDP (Windows)*.

Verificación de que la máquina virtual instantánea está protegida

Verifique que la máquina virtual instantánea está protegida confirmando que los puntos de recuperación válidos están disponibles en el destino de la copia de seguridad.

Siga estos pasos:

1. Inicie sesión en el destino de la copia de seguridad y vaya a la carpeta del destino de la copia de seguridad.
2. Verifique que la copia de seguridad de la máquina virtual instantánea se ha realizado correctamente y que los puntos de recuperación están disponibles.

   Se ha verificado la máquina virtual instantánea.

   La máquina virtual instantánea se ha protegido correctamente.

Cómo replicar datos entre almacenes de datos gestionados desde una Consola de UDP

Mediante Arcserve UDP, se pueden replicar los datos de copia de seguridad de un almacén de datos a otro. Estos almacenes de datos se gestionan en la misma Consola de UDP pero se encuentran en servidores de punto de recuperación diferentes. Es necesario crear un plan con dos tareas: copia de seguridad y replicación. La tarea de copia de seguridad realizará la copia de seguridad de los datos basándose en la programación y la tarea de replicación replicará los datos de los que se ha realizado la copia de seguridad al servidor de punto de recuperación especificado. La tarea de replicación se ejecuta por la programación que se especifica en la tarea de replicación. Se pueden crear varias tareas de replicación en un plan.

Si la tarea de replicación produce un error por algunos motivos (como problema de red), la tarea de replicación errónea se reanuda primero antes de transferir cualquier sesión nueva. Las tarea de replicación se reanuda desde el punto de rotura de la última tarea de replicación errónea.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Creación de un plan con una tarea de copia de seguridad
3. Cómo agregar una tarea de replicación al plan
4. (Opcional) Realización de una replicación manual
5. Verificación del plan

Revisión de las consideraciones y requisitos previos

Verifique si se han completado los requisitos previos siguientes:

- Inicie sesión en la Consola.
- Instale el componente del servidor y cree almacenes de datos.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Creación de una tarea de copia de seguridad

Un plan incluye tipos diferentes de tareas que se desea realizar. Por lo general, un plan incluye una tarea primaria seguida de una tarea secundaria. Normalmente, una tarea principal es una tarea de copia de seguridad o de replicación desde una tarea remota de la Consola. El rol de una tarea de copia de seguridad es crear una copia de seguridad de los nodos de origen que se desean proteger. Puede realizar copias de seguridad de máquinas físicas y virtuales de Windows y Linux. A continuación, se pueden guardar los datos de copia de seguridad a otra ubicación, como una medida de precaución adicional.

Para obtener más información, consulte:

- Cómo crear un plan de copia de seguridad en Windows para realizar copias de seguridad de un nodo de Windows.
- Cómo crear un plan de copia de seguridad de máquina virtual basada en el host para realizar copias de seguridad de máquinas virtuales.
- Cómo crear un plan de copia de seguridad en Linux para realizar copias de seguridad de nodos de Linux.

Cómo agregar una tarea de replicación al plan

Cree una tarea de replicación para proteger los datos copiando los datos de la copia de seguridad de un servidor de punto de recuperación a otro servidor de punto de recuperación. También es posible copiar los datos de la copia de seguridad desde un almacén de datos a otro almacén de datos en el mismo servidor de puntos de recuperación. El destino de la replicación debe ser un almacén de datos en el servidor de punto de recuperación. Se pueden crear varias tareas de replicación para realizar varias replicaciones.

Notas:

- **Para la tarea de combinación:** Cuando se configura una tarea de replicación y se ejecuta una tarea de combinación a petición desde el almacén de datos de origen, la tarea no comprueba si las sesiones se han replicado o no. Como consecuencia, no se pueden replicar las sesiones combinadas al almacén de datos de destino y se acaban replicando más datos. Por ejemplo, supongamos que hay cinco sesiones, s1, s2, s3, s4 y s5 respectivamente. Se replican las sesiones s1 y s2. Ahora, ejecute una tarea de combinación a petición en el origen y retenga dos sesiones. Se retienen las sesiones s4 y s5. La sesión s4 es una sesión completa. Por lo tanto, cuando se inicia la siguiente tarea de replicación, esta necesita replicar una sesión completa.
- **Para la tarea de borrado definitivo:** Cuando se configura una tarea de replicación y si se ejecuta una tarea de borrado definitivo en el almacén de datos de destino, la siguiente tarea de replicación replica todas las sesiones al almacén de datos de destino.
- No se puede replicar desde un almacén de datos con la deduplicación activada a un almacén de datos con la no deduplicación activada.
- No se puede replicar desde un almacén de datos con el cifrado activado a un almacén de datos sin cifrado activado.

Siga estos pasos:

1. Haga clic en **Agregar una tarea** en el panel izquierdo.

   Una tarea nueva se agrega al panel izquierdo.

2. En el menú desplegable **Tipo de tarea**, seleccione **Replicación**.

   La tarea de replicación se agrega. No se tiene que configurar la ficha **Origen** en la tarea de replicación porque se muestra el destino de la copia de seguridad en la tarea de copia de seguridad.

Nota: No se puede replicar una tarea sin la tarea principal como Copia de seguridad en el servidor de puntos de recuperación.

3. Haga clic en la ficha **Destino** e introduzca los detalles del servidor de punto de recuperación y los detalles de programación de reintento.



Servidor de puntos de recuperación

Seleccione el servidor de punto de recuperación en la lista.

Almacén de datos

Seleccione el almacén de datos en la lista.

Iniciar reintento

Especifique el tiempo (en minutos) restante para reiniciar la tarea de replicación después de que se produzca un error en la tarea. Por ejemplo, si se especifican 10 minutos, la tarea de replicación se reiniciará después de que pasen 10 minutos del error.

Límite: 1 a 60

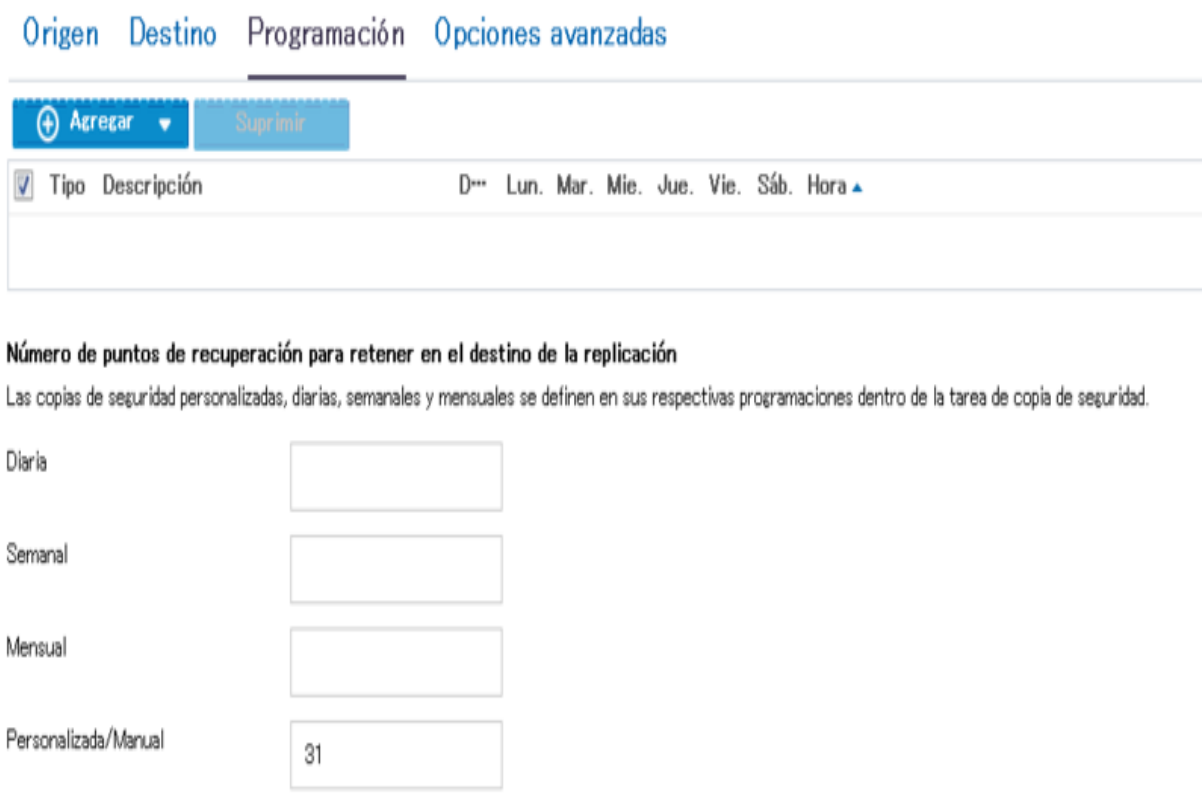
Reintentar

Especifique el número de veces que se desea iniciar la tarea de replicación cuando la tarea produzca un error. La tarea de replicación se ejecuta hasta que la tarea sea correcta o hasta que se alcance el límite.

Límite: 1 a 99

4. Haga clic en la ficha **Programación** y agregue **Programación de la tarea de replicación**, **Programación del regulador de la replicación**, **Programación de la combinación** y **Valores de configuración de la retención**.

   Nota: La cuota del regulador de la replicación se comparte normalmente entre todas las tareas de replicación iniciadas desde todos los nodos de un plan actual.



5. Haga clic en la ficha **Avanzada** e introduzca los detalles.
6. Haga clic en **Guardar cambios** o **Agregar una tarea**.

   Si se ha agregado una tarea, entonces se podrá crear otra tarea de replicación para realizar varios niveles de replicación. Se pueden agregar varias tareas de replicación al plan.

   Si se guardan los cambios, el plan se guardará y la tarea de replicación se implementará en el destino de la replicación.

   La tarea de replicación se crea.

   Se ha creado correctamente e implementado automáticamente un plan de replicación.

(Opcional) Realización de una replicación manual

Para ejecutar manualmente una tarea de replicación, debe tener al menos unos datos correctos de copia de seguridad. Si no se ha establecido la programación de replicación, la tarea de replicación se ejecutará inmediatamente después de la tarea de copia de seguridad, de lo contrario, se ejecutará según la configuración de la programación de replicación.

Siga estos pasos:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Si se han agregado algunos planes, estos planes se mostrarán en el panel central.
3. Seleccione los nodos de los que desea realizar la copia de seguridad y que tienen un plan asignado.
4. En el panel central, haga clic en **Acciones**, **Replicar ahora**.

   Se abrirá el cuadro de diálogo **Replicar nodo**.
5. Seleccione el servidor de punto de recuperación de origen y el servidor de punto de recuperación de destino para la tarea.
6. Haga clic en **Aceptar**.

   Se ejecuta la tarea de replicación.

   La replicación manual se realiza correctamente.

Verificación del plan

Para verificar la función de replicación, confirme que se ha creado correctamente el plan de replicación. Después de verificar que el plan se ha creado correctamente, compruebe si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Después de que la tarea de copia de seguridad se complete correctamente, se ejecutará la tarea de replicación. Se puede comprobar el estado de la tarea de copia de seguridad y de a tarea de replicación en la ficha **tareas**.

Siga estos pasos: para verificar los planes.

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga estos pasos: para verificar las tareas de replicación.

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad y la tarea de replicación se han realizado correctamente.

Cómo replicar datos entre almacenes de datos gestionados desde consolas de UDP diferentes

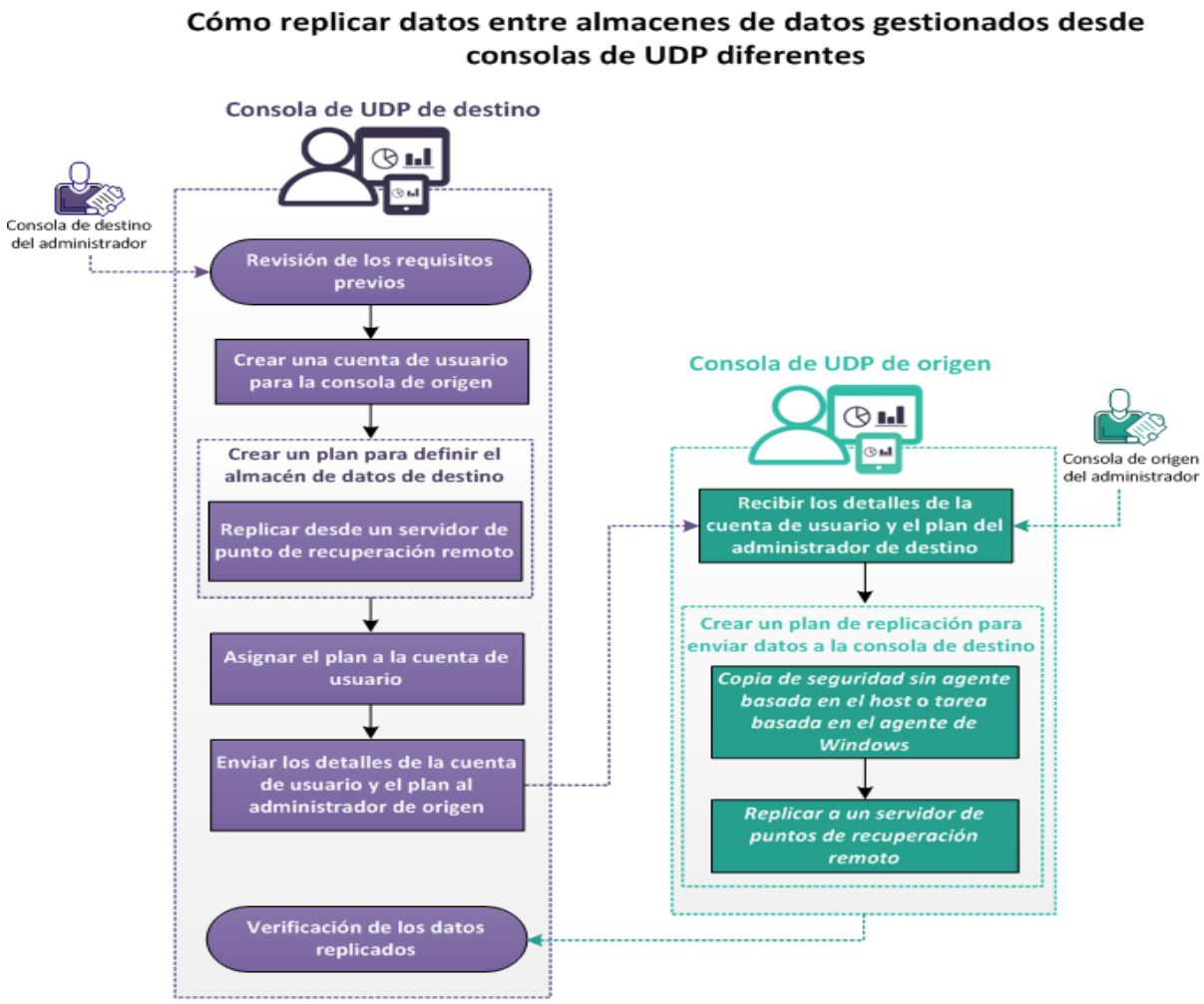
Para proteger los datos, es posible que se deban replicar los datos de copia de seguridad en otro servidor de puntos de recuperación que se gestione desde una consola de Arcserve UDP diferente. Por ejemplo, se pueden replicar los datos en un proveedor de servicios que ofrezca sus servicios de replicación a varios clientes. En este ejemplo, los datos se replican desde un almacén de datos de origen (en la consola de origen) a uno de destino (en la consola de destino).

El administrador de la consola de destino debe crear un nombre de usuario, una contraseña y un plan únicos para la consola de origen. El plan define el almacén de datos de destino, y el nombre de usuario y la contraseña ayudan al administrador de origen a conectarse al servidor y replicar datos.

El administrador de la consola de origen debe crear un plan de replicación de datos para el almacén de datos de destino. Mientras se crea el plan, conéctese al servidor de destino y seleccione el plan que le ha asignado el administrador de destino.

Nota: Como práctica recomendada, se recomienda configurar los parámetros de multitransmisión. Para obtener más información, consulte Configuración de los parámetros de multitransmisión.

El siguiente diagrama muestra cómo replicar datos en otro almacén de datos que se gestione desde una consola diferente:



¿Qué hacer a continuación?

1. Revise de los requisitos previos
2. Creación de una cuenta de usuario para la consola de origen
3. Creación de un plan para definir el almacén de datos de destino
4. Asignación del plan a la cuenta de usuario
5. Envío de los detalles de la cuenta de usuario y el plan al administrador de origen

6. Recepción de los detalles de la cuenta de usuario y el plan del administrador de destino
7. Creación de un plan de replicación para enviar datos a la consola de destino
8. Verificación de los datos replicados

Revisión de los requisitos previos

Revise los siguientes requisitos previos antes de replicar volúmenes:

- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Administrador: consola de destino

- Verifique que se ha instalado Arcserve UDP en el servidor de destino.
- Verifique que tiene privilegios completos para crear cuentas de usuario de Windows en el servidor de destino.
- Compruebe que se ha activado la casilla de verificación **Permitir la recuperación de puntos de recuperación** en la Configuración avanzada durante la replicación desde la creación de un plan del servidor de puntos de recuperación gestionado remotamente.

  Nota: Si no activa la casilla de verificación **Permitir la recuperación de puntos de recuperación** e inicia la tarea de replicación inversa para la Consola remota, se le pedirá que active el indicador remoto Permitir recuperación para la replicación inversa.

Administrador: consola de UDP de origen

- Verifique que se ha instalado Arcserve UDP en el servidor de origen.
- Verifique que dispone de al menos una copia de seguridad entera completada en un almacén de datos.

Creación de una cuenta de usuario para la consola de origen

Administrador de destino

Para identificar y gestionar los datos replicados en el servidor de destino, debe crearse una cuenta de usuario de Windows. Si se gestiona más de una consola de origen, a continuación, debe crearse una cuenta de usuario para cada consola de origen.

El administrador de la consola de origen utiliza los detalles de esta cuenta para conectarse al servidor de destino.

Para crear una cuenta de usuario en un sistema operativo Windows, debe utilizarse la sección Cuentas de usuario del Panel de control de Windows. Para obtener más información sobre la creación de cuentas de usuario en Microsoft Windows, puede consultarse la documentación de Microsoft.

Creación de un plan para definir el almacén de datos de destino

Administrador de destino

Los datos de origen se replican a este almacén de datos de destino. Para definir este almacén de datos de destino, debe crearse un plan. Con él, se pueden definir el almacén de datos de destino y la programación de combinación.

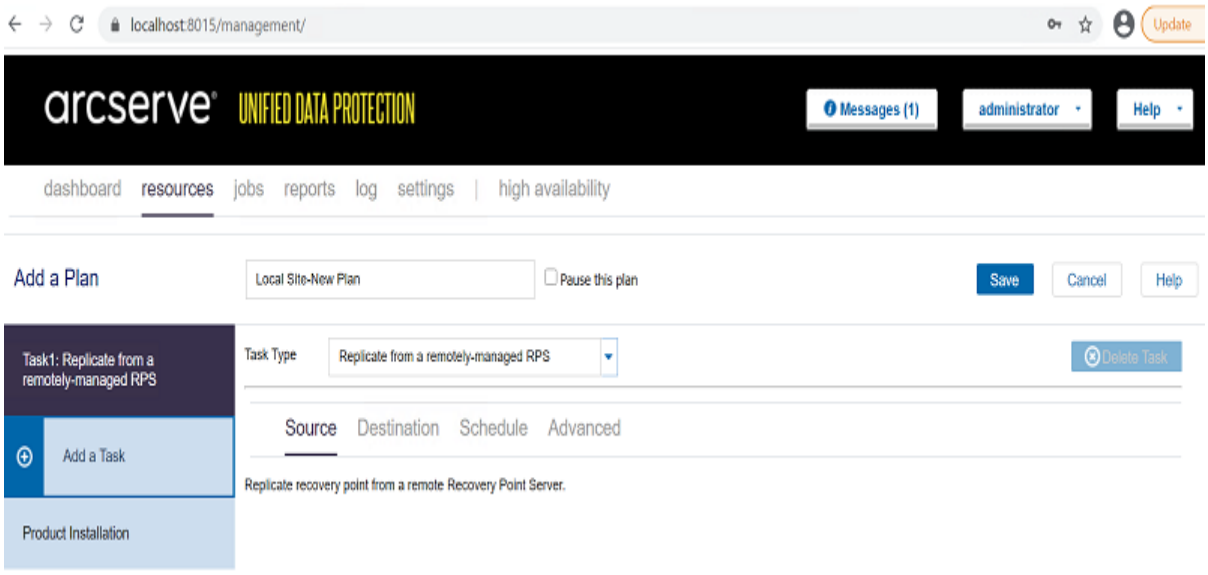
Siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se ha agregado algún plan, se mostrará en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre la página **Agregar un plan**.
4. Introduzca un nombre de plan en el campo **Nuevo plan**.
5. En el menú desplegable **Tipo de tarea**, seleccione **Replicar desde un servidor de puntos de recuperación gestionado remotamente**.

   Se muestra la ficha **Origen.** No se pueden proporcionar detalles sobre la ficha Origen. El administrador de origen en la consola de origen proporciona los detalles de origen.



6. Haga clic en la ficha **Destino** y especifique el servidor de punto de recuperación y el almacén de datos.

7. (Opcional) Seleccione la casilla de verificación **El servidor está detrás del enrutador de NAT** y proporcione la dirección del servidor y el número de puerto.
8. Haga clic en la ficha **Programación**.

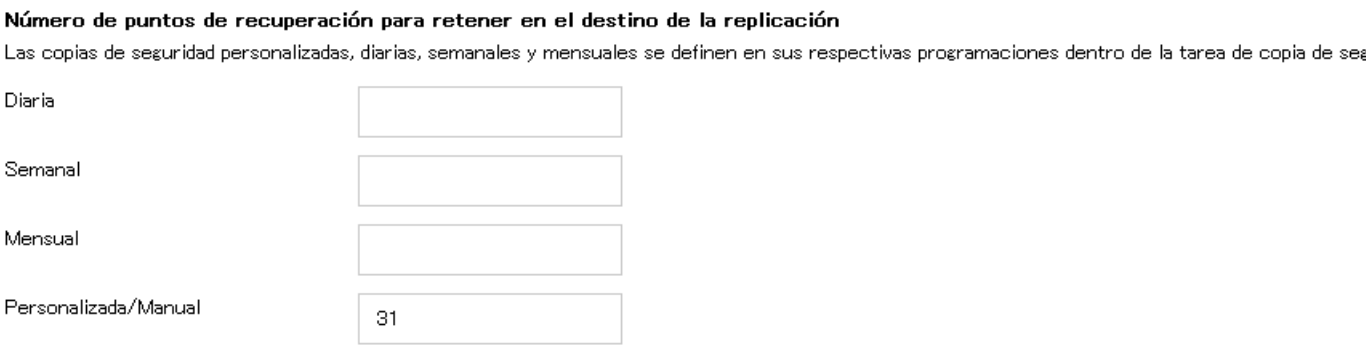


9. Haga clic en **Agregar** y seleccione **Agregar programación de la combinación de la replicación**.

   Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.
10. Introduzca la programación de combinación.

    Nota: Para saber más sobre las programaciones, consulte Funcionamiento de la programación avanzada y de la retención.
11. Haga clic en **Guardar**.

    Se cierra el cuadro de diálogo **Agregar nueva programación de la combinación**.
12. Introduzca los detalles de la retención de los puntos de recuperación.



13. Haga clic en la ficha **Avanzada** y proporcione los detalles siguientes:

    Configuración de la recuperación

    Permite realizar la recuperación de puntos de recuperación. Para activarla, seleccione la casilla de verificación **Permitir la recuperación de puntos de recuperación**.

    Activar Alertas de correo electrónico

    Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y se pueden especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

    Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy.

Alertas de tarea

Le permite seleccionar los tipos de alertas de tareas que se desean recibir.

14. Haga clic en **Guardar**.

    Los cambios se guardan y el plan se crea.

    El plan de replicación se ha creado correctamente. También se pueden agregar al plan tareas de replicación, tareas de replicación en un servidor de puntos de recuperación gestionado de forma remota o tareas de Virtual Standby.

Asignación del plan a la cuenta de usuario

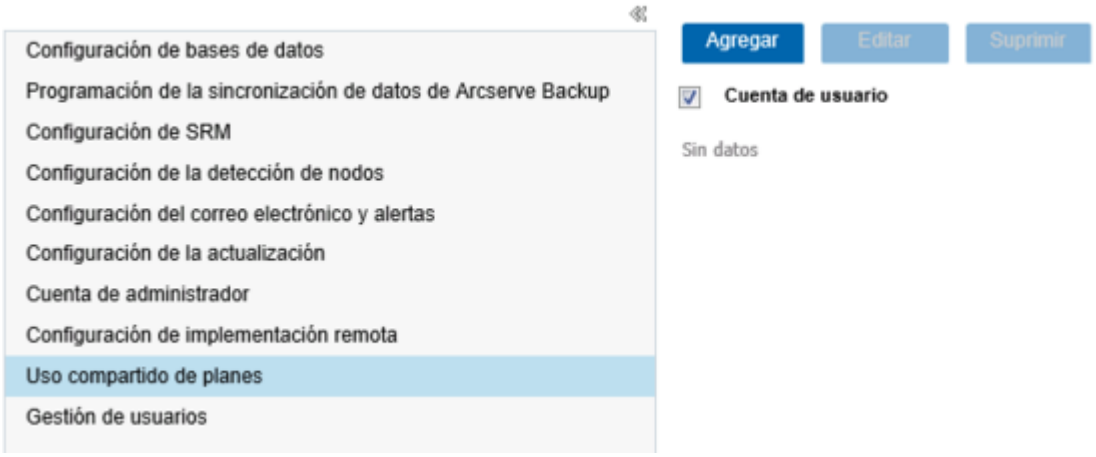
Administrador de destino

Ya se ha creado una cuenta de usuario y un plan para una consola de origen. Para identificar y gestionar datos replicados, debe asignarse el plan a la cuenta de usuario.

Nota: Se puede asignar más de un plan a una cuenta de usuario, pero dos cuentas diferentes no pueden compartir un plan. Sin embargo, se recomienda asignar un solo plan a una cuenta de usuario para que se puedan identificar y gestionar los datos replicados fácilmente.

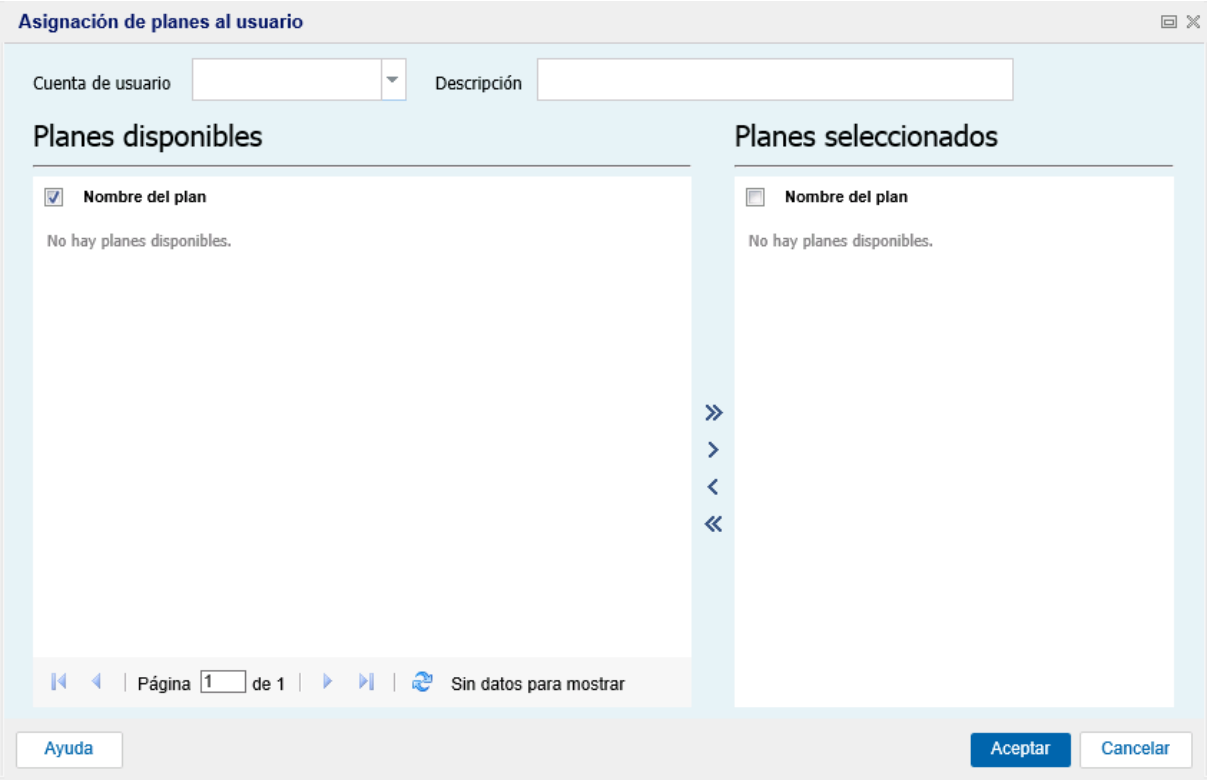
Siga estos pasos:

1. En la Consola, haga clic en la ficha **configuración**.
2. En el panel izquierdo, haga clic en **Compartir plan**.



3. En el panel central, haga clic en **Agregar**.

   Se abre el cuadro de diálogo **Asignar plan al usuario**.



4. Seleccione la **Cuenta de usuario**.
5. Seleccione un plan en la columna **Planes disponibles**.

   Nota: Si un plan ya se ha agregado a un nombre de usuario, ese plan no se muestra en la columna **Planes disponibles**.
6. Haga clic en **Agregar todos los planes** o en **Agregar planes seleccionados** para agregar los planes de la columna **Planes seleccionados**.
7. Haga clic en **Aceptar**.

   Se cierra el cuadro de diálogo **Asignar plan al usuario.** El nombre de usuario y los planes asociados se muestran en la página **Compartir plan**.

   La cuenta de usuario se asigna al plan creado para la consola de origen.

   Se puede utilizar **Editar** para modificar la configuración del usuario o **Suprimir** para eliminar la cuenta de usuario de la lista.

Envío de los detalles de la cuenta de usuario y el plan al administrador de origen

Administrador de destino

Después de asociar el plan a la cuenta de usuario, deben enviarse los detalles de cuenta de usuario y el plan al administrador de origen. El administrador de origen utiliza estos detalles para conectarse a la consola de destino.

El administrador de destino ha realizado todas sus tareas.

Recepción de los detalles de la cuenta de usuario y el plan del administrador de destino

Administrador de origen

Para replicar datos en la consola de origen, se precisan los detalles de la cuenta de usuario, el plan y el servidor de destino por parte del administrador de destino. Se reciben los detalles del administrador de destino. Deben comprenderse los detalles y solucionarse las preguntas por parte del administrador de destino antes de empezar a crear planes de replicación.

Creación de un plan de replicación para enviar datos a la consola de destino

Administrador de origen

Para replicar sus datos de copia de seguridad en el servidor de puntos de recuperación de destino que se gestiona desde una consola diferente, debe crearse un plan de replicación. Dicho plan de replicación incluye una tarea de copia de seguridad y otra de replicación gestionada en remoto. En la tarea de replicación, deben especificarse el servidor remoto y los detalles del plan, y conectarse al servidor remoto. Si la conexión se realiza correctamente, el usuario debe seleccionar el plan que el administrador de destino le ha creado.

Siga estos pasos:

1. En la consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.
3. Haga clic en **Agregar un plan**.

   Se abre la página **Agregar un plan**.
4. Introduzca un nombre de plan, seleccione una de las tareas de copia de seguridad siguientes y cree la tarea:
   - **Copia de seguridad: Windows, basada en agentes**
   - **Copia de seguridad: sin agentes, basada en host**
   - **Copia de seguridad: Linux, basada en agentes**

     Nota: Para obtener más información sobre cómo crear una tarea de copia de seguridad, consulte los temas siguientes:

     – Cómo crear un plan de copia de seguridad en Windows

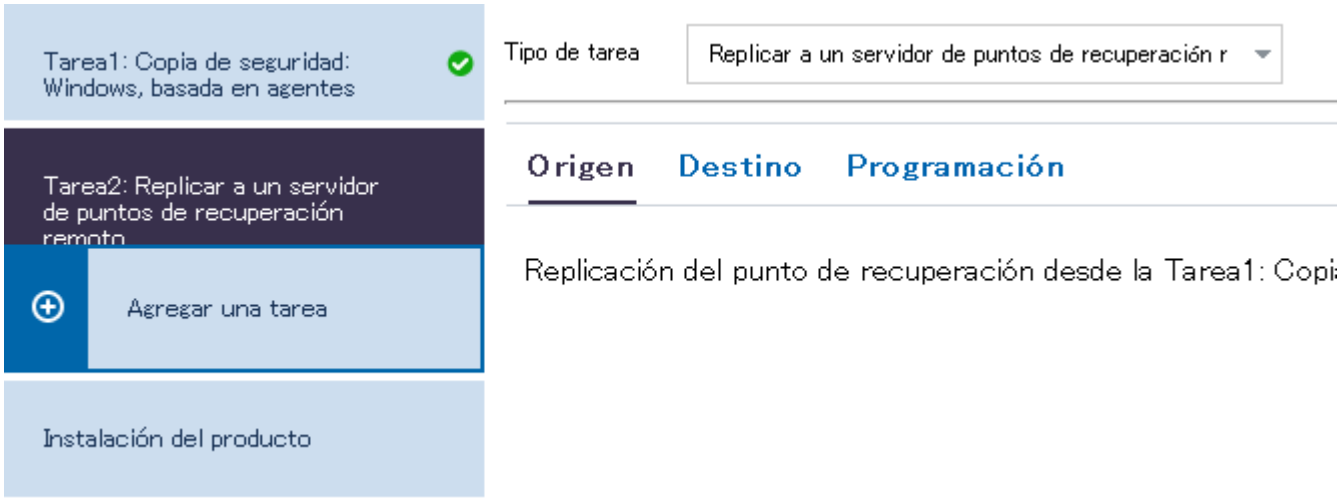
     – Cómo crear un plan de copia de seguridad de máquina virtual basada en el host

     – Cómo crear un plan de copia de seguridad en Linux
5. En el panel izquierdo, haga clic en **Agregar una tarea**.

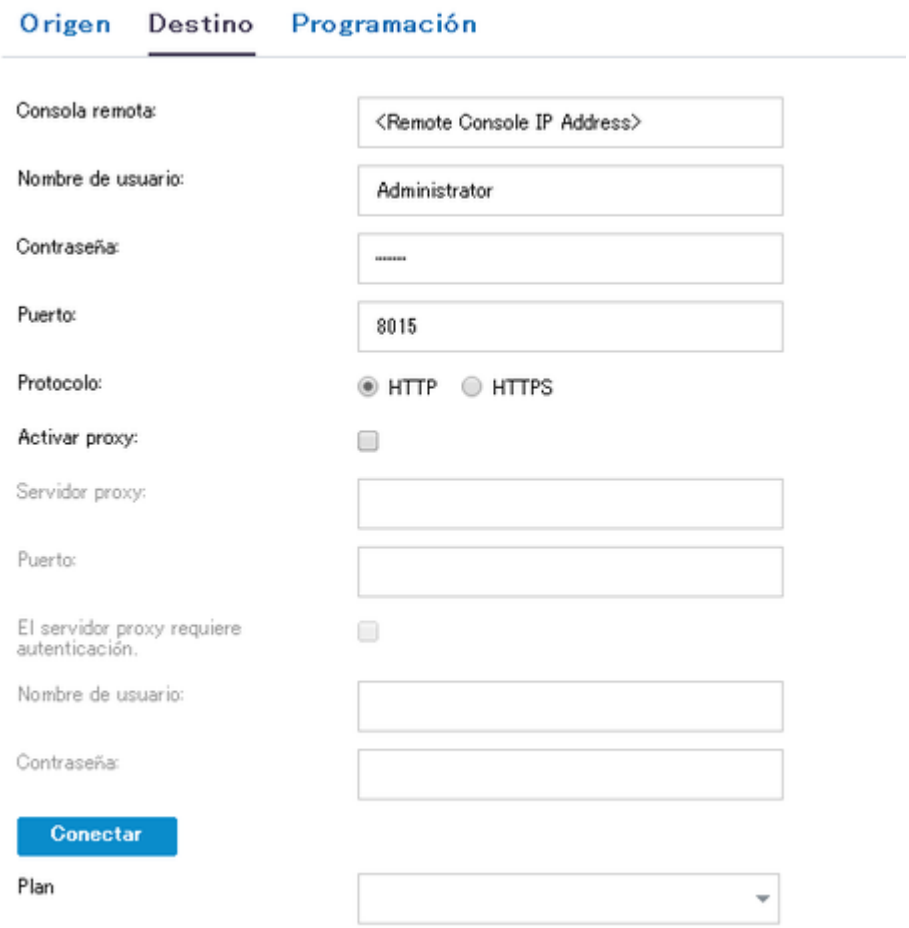
   Una tarea nueva se agrega al panel izquierdo.
6. En el menú desplegable **Tipo de tarea**, seleccione **Replicar a un servidor de punto de recuperación gestionado remotamente**.

   Se agrega la tarea Replicar y se abre la página **Origen.** En la ficha **Origen**, el destino de la tarea de copia de seguridad (por ejemplo, Copia de seguridad: Windows,

basada en agentes) es el origen de la tarea **Replicar a un servidor de puntos de recuperación remoto**.



7. Haga clic en la ficha **Destino** y proporcione los detalles siguientes.



Consola remota

Seleccione una cuenta de consola remota en la lista desplegable o agregue una nueva cuenta de consola remota haciendo clic en el botón **Agregar**.

Para obtener más información, haga clic en Agregar consola remota.

Nombre de usuario

Especifique el nombre de usuario que ha creado el administrador de destino. El administrador de destino proporciona el nombre de usuario.

Contraseña

Especifique la contraseña que ha creado el administrador de destino. El administrador de destino proporciona la contraseña.

Puerto

Especifique el número de puerto de la consola de destino. El administrador de destino proporciona el número de puerto de la consola de destino.

Protocolo

Especifique el protocolo que ha utilizado el administrador de destino para conectarse a la consola de destino.

Activar proxy

Seleccione la casilla de verificación para activar la selección del servidor proxy.

Servidor proxy

Especifica la dirección del servidor proxy.

Puerto

Especifica el número de puerto del servidor proxy.

El servidor proxy requiere autenticación

Seleccione la casilla de verificación para permitir los campos de autenticación para el servidor proxy.

Nombre de usuario

Especifique el nombre del usuario para conectarse al servidor proxy.

Contraseña

Especifique la contraseña para autenticar la conexión del servidor proxy.

Conectar

Verifica la conexión entre la consola de origen y la de destino. Si la conexión se realiza correctamente, se podrá ver el nombre del plan en el campo **Plan.** El administrador de destino asigna el nombre de este plan a esta consola.

Plan

Especifique el plan que el administrador de destino ha creado. Si existen varios planes en la lista, póngase en contacto con el administrador de destino para conocer el plan correcto.

Iniciar reintento

Vuelve a ejecutar la tarea de replicación tras el tiempo especificado si se produce un error. Introduzca un valor del 1 al 60 y el tiempo se define en minutos.

Reintentar

Especifique el número de reintentos que desea realizar si se produce un error de tarea. Tras superar el número de reintentos, la tarea de replicación se ejecutará solamente en el siguiente período programado. Introduzca un valor del 1 al 99.

8. Haga clic en la ficha **Programación** y proporcione la programación de la tarea de replicación y la programación del regulador de la replicación.

   Programación de la tarea de replicación

   Especifique la fecha y hora para iniciar las tareas de replicación. Se puede editar o suprimir una programación de la tarea de replicación.

   Programación de regulador de replicación

   Especifique la velocidad máxima (MB/s) a la que se realiza replicación. Es posible limitar la velocidad de la replicación para reducir el uso de la CPU o de la red. En una tarea de replicación, la ficha **tareas** muestra la velocidad media de lectura y escritura de la tarea en curso y el límite de velocidad que se ha configurado.

   Se puede editar o suprimir una programación del regulador de la replicación.

9. Haga clic en **Guardar**.

   Se guarda el plan y se ejecuta según la programación.

   Se ha creado correctamente e implementado automáticamente un plan de replicación. Cuando se ejecuta el plan, los datos se replican desde la ubicación de origen a la de datos de destino en una red.

   Nota: Después de que se complete el proceso de replicación, se agregarán automáticamente los detalles del nodo replicado a la consola de destino.

   Se habrán replicado correctamente los datos entre dos almacenes de datos gestionados mediante consolas de UDP diferentes.

Verificación de los datos replicados

Administrador de destino

Después de que se repliquen los datos, se puede verificar si la replicación se ha realizado correctamente.

Siga estos pasos:

1. En la consola de destino, diríjase al almacén de datos de destino en el servidor de puntos de recuperación.
2. Verifique que el tamaño de los datos replicados coincide con los datos de origen.

   Se habrán replicado correctamente los datos entre dos almacenes de datos gestionados mediante consolas de UDP diferentes.

Cómo realizar una replicación de datos sin conexión mediante el servidor de puntos de recuperación Jump-start

Replicar un almacén de datos grande en otro servidor de puntos de recuperación (gestionado desde una consola de UDP diferente) requiere mucho tiempo en una red (LAN, WAN o Internet). Para replicar un almacén de datos grande rápidamente, Arcserve UDP proporciona un método de replicación de datos sin conexión. Este método se denomina Servidor de puntos de recuperación JumpStart.

El servidor de puntos de recuperación JumpStart es un método de replicación sin conexión que utiliza un dispositivo de almacenamiento externo, como una unidad flash USB, para replicar un almacén de datos. Esta replicación se produce entre dos almacenes de datos que se gestionan desde consolas de UDP diferentes. Por ejemplo, un proveedor de servicios ofrece sus servicios de replicación a varios clientes. El cliente replica los datos en un dispositivo de almacenamiento y envía el dispositivo de almacenamiento al proveedor de servicios. El proveedor de servicios replica los datos del dispositivo de almacenamiento en el servidor de destino. Tanto el proveedor de servicios como el cliente deben tener Arcserve UDP instalado en sus ubicaciones.

La replicación sin conexión requiere que ambos administradores (los de origen y de destino) sigan estos pasos en su respectiva ubicación.

Importante: Si va a replicar desde una carpeta compartida a un almacén de datos seleccionado en el servidor de puntos de recuperación, consulte Cómo migrar los puntos de recuperación de la versión r16.5 a Arcserve UDP.

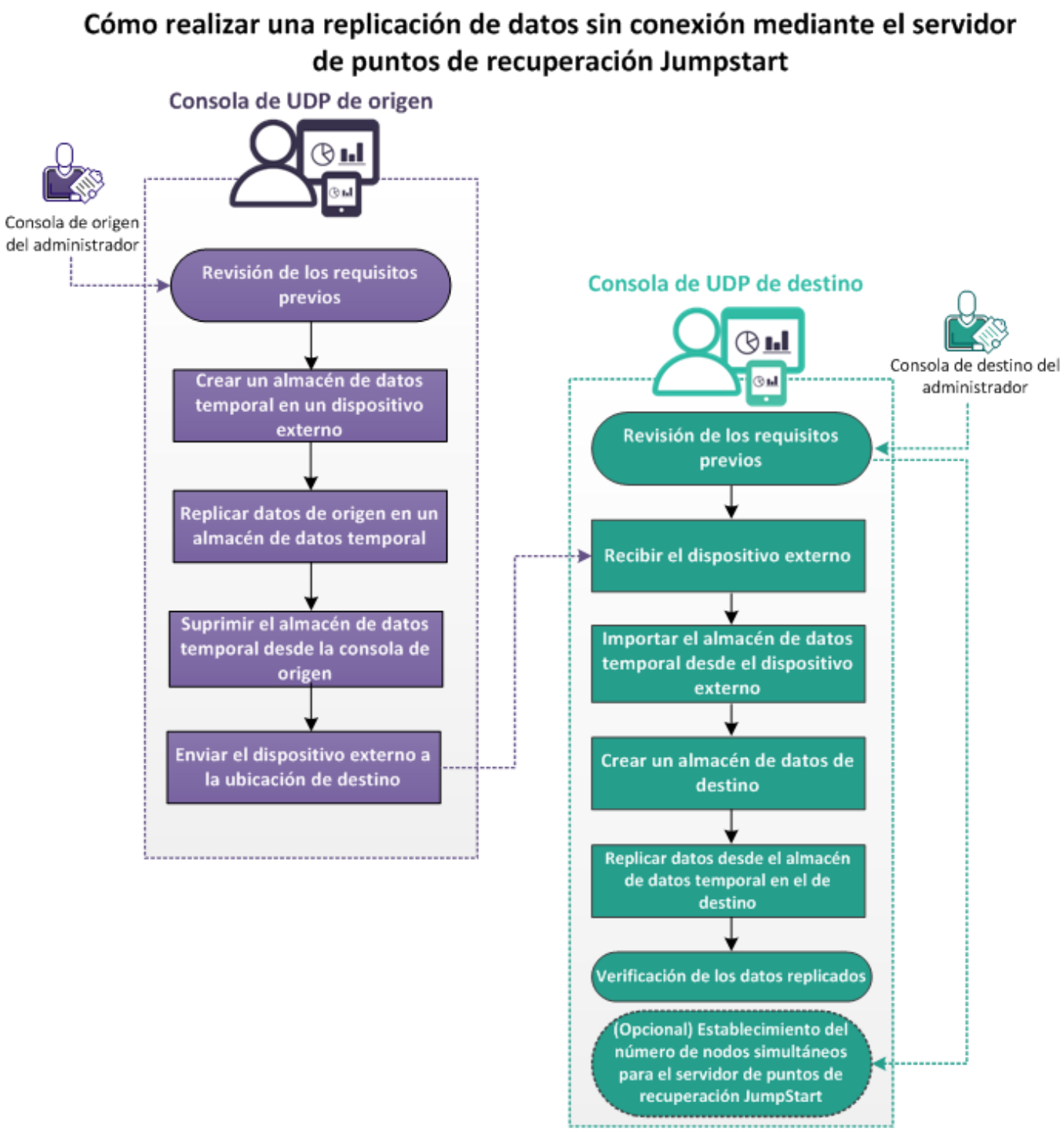
Administrador de origen

1. Replique el almacén de datos de origen en un dispositivo externo.
2. Envíe el dispositivo externo a la ubicación de destino.

Administrador de destino

1. Reciba el dispositivo externo.
2. Replique el almacén de datos de origen desde dispositivo externo en el servidor de punto de recuperación de destino.

El siguiente diagrama muestra cómo realizar una replicación de datos sin conexión mediante el servidor de puntos de recuperación JumpStart.



¿Qué hacer a continuación?

- Revisión de los requisitos previos
- Creación de un almacén de datos temporal en un dispositivo externo
- Replicación de datos de origen en un almacén de datos temporal
- Supresión del almacén de datos temporal desde la consola de origen

- Envío del dispositivo externo a la ubicación de destino
- Recepción del dispositivo externo
- Importación de los datos temporales desde el dispositivo externo
- Creación de un almacén de datos de destino
- Replicación de datos desde el almacén de datos temporal en el de destino
- Verificación de la replicación de los datos
- (Opcional) Establecimiento del número de nodos simultáneos para el servidor de puntos de recuperación JumpStart

Revisión de los requisitos previos

Revise los siguientes requisitos previos antes de realizar una replicación de datos sin conexión:

- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.
- Si el origen es un almacén de datos con la deduplicación activada, el destino también debe ser un almacén de datos con la deduplicación activada.
- Si el origen es un almacén de datos con el cifrado activado, el destino también debe ser un almacén de datos con el cifrado activado.

Administrador: consola de origen

- Verifique que ha creado el almacén de datos de origen.
- Verifique que dispone de al menos una copia de seguridad completada en un almacén de datos.
- (Opcional) Verifique que ha configurado el número de nodos simultáneos para el servidor de puntos de recuperación JumpStart. Para obtener más información sobre cómo configurar el número de nodos simultáneos, consulte Establecimiento del número de nodos simultáneos para el servidor de puntos de recuperación JumpStart.

Administrador: consola de destino

- Verifique que dispone de suficiente espacio disponible para la replicación.
- Verifique que cuenta con los privilegios requeridos en el dispositivo externo.

Creación de un almacén de datos temporal en un dispositivo externo

Administrador de origen

Para importar datos desde un almacén de datos existente a un dispositivo externo, primero, debe crearse un almacén de datos temporal en el dispositivo externo. Para crear el almacén de datos temporal, debe conectarse el dispositivo externo al equipo.

Siga estos pasos:

1. Inicie sesión en la consola de UDP.
2. Vaya a **Destinos**, **Servidor de punto de recuperación**.
3. Seleccione el servidor de punto de recuperación.
4. Haga clic con el botón secundario del ratón y seleccione **Agregar un almacén de datos**.
5. Introduzca los detalles en la página **Adición de almacenes de datos**.

   Nota: Asegúrese de que las carpetas de destino de la copia de seguridad se encuentren en el dispositivo externo.
6. Guarde el almacén de datos.

   El almacén de datos temporal se crea en el dispositivo externo.

Replicación de datos de origen en un almacén de datos temporal

Administrador de origen

Después de crear el almacén de datos temporal en el dispositivo externo, se pueden replicar los datos de origen en el dispositivo externo mediante el servidor de puntos de recuperación JumpStart.

Nota: Antes de que dé comienzo el proceso del servidor de puntos de recuperación JumpStart, debe detenerse el plan relacionado. Esta detención del plan garantiza que no se cargan tareas de replicación programadas cuando el proceso de JumpStart está en curso.

Siga estos pasos:

1. Haga clic en **Acciones** y, a continuación, haga clic en **Servidor de puntos de recuperación JumpStart**.

   Se abrirá el **Asistente del servidor de punto de recuperación Jumpstart**.
2. Seleccione si desea migrar del mismo almacén de datos o de una ubicación compartida.
3. Seleccione el servidor del punto de recuperación de origen, el almacén de datos de origen y el plan.

   Aparecerán los nodos que pertenecen al plan.
4. Seleccione los nodos que desee migrar.
5. Haga clic en **Siguiente**.

   Se abre la página **Selección del almacén de datos de destino**. Si se cifra el almacén de datos de origen, solamente aparecerán los almacenes de datos cifrados en la lista desplegable.
6. Seleccione el almacén de datos de destino. El almacén de datos de destino debería estar en el dispositivo externo.
7. Haga clic en **Finalizar**.

   La sección **Eventos recientes** del panel derecho muestra el progreso de la replicación.

   Tras la finalización del proceso de replicación, los datos se replicarán en el almacén de datos temporal. Se puede verificar el tamaño de ambos almacenes de datos en la página **Destinos: servidor de punto de recuperación**.

Supresión del almacén de datos temporal desde la consola de origen

Administrador de origen

Para mantener la integridad de los datos en el dispositivo externo, debe suprimirse el almacén de datos temporal de la consola de UDP antes de eliminar el dispositivo externo.

Nota: La supresión del almacén de datos temporal de la consola de UDP de origen no elimina los archivos del almacén de datos del dispositivo externo.

Siga estos pasos:

1. Haga clic con el botón secundario del ratón en el almacén de datos temporal y haga clic en **Detener**.

   Se detiene el almacén de datos.

2. Haga clic con el botón secundario del ratón en el almacén de datos temporal y haga clic en **Suprimir**.

   Aparecerá un diálogo de confirmación.

3. Haga clic en **Sí**.

   El almacén de datos se suprime.

   Ahora, se puede eliminar el dispositivo externo del equipo.

Envío del dispositivo externo a la ubicación de destino

Administrador de origen

Después de eliminar el dispositivo externo, debe enviarse este a la ubicación de destino.

Recepción del dispositivo externo

Administrador de destino

Debe recibirse el dispositivo externo que incluye los datos de origen. Ahora, debe conectarse este dispositivo externo al servidor de destino.

Importación del almacén de datos temporal desde el dispositivo externo

Administrador de destino

Antes de poder replicar los datos de origen en el almacén de datos de destino, debe importarse el almacén de datos temporal al servidor de puntos de recuperación de destino.

Siga estos pasos:

1. Vaya a la ficha **recursos** y seleccione el servidor de punto de recuperación donde se desea importar el almacén de datos.
2. Haga clic con el botón secundario del ratón en el servidor de punto de recuperación y seleccione **Importar almacén de datos**.

   Se abre el cuadro de diálogo **Importar un almacén de datos**.
3. Seleccione la carpeta de destino de la copia de seguridad del dispositivo externo.
4. Haga clic en **Siguiente**.

   Se muestran los detalles del almacén de datos temporales. Si es necesario, a continuación, cambie la ruta de datos, índice y hash.
5. Haga clic en **Guardar**.

   El almacén de datos se importa y puede verse en la consola de destino.

Creación de un almacén de datos de destino

Administrador de destino

Para replicar datos desde el almacén de datos temporal, primero, debe crearse un almacén de datos de destino. Para obtener más información, consulte Cómo agregar un almacén de datos.

Nota: También se puede utilizar un almacén de datos existente como un almacén de datos de destino.

Replicación de datos desde el almacén de datos temporal en el de destino

Tras crear el almacén de datos de destino, deben replicarse los datos desde el almacén de tatos temporal en el de destino Después de que se repliquen los datos en el almacén de datos de destino, se puede suprimir el almacén de datos temporal.

Siga estos pasos:

1. Haga clic en **Acciones** y, a continuación, haga clic en **Servidor de puntos de recuperación JumpStart**.

   Se abrirá el **Asistente del servidor de punto de recuperación Jumpstart**.

2. Seleccione el servidor de punto de recuperación de origen y el almacén de datos de origen. Qué plan debería seleccionarse aquí.

   Se muestran los nodos.

3. Seleccione los nodos que desee migrar.

4. Haga clic en **Siguiente**.

   Se abre la página **Selección del almacén de datos de destino**. Si se cifra el almacén de datos de origen, solamente aparecerán los almacenes de datos cifrados en la lista desplegable.

5. Seleccione el almacén de datos de destino. El almacén de datos de destino debería estar en el dispositivo externo.

6. Haga clic en **Finalizar**.

   La sección **Eventos recientes** del panel derecho muestra el progreso de la replicación.

   Tras la finalización del proceso de replicación, los datos se replicarán en el almacén de datos temporal. Se puede verificar el tamaño de ambos almacenes de datos en la página **Destinos: servidor de punto de recuperación**.

   Los datos se replican en este almacén de datos de destino.

Verificación de la replicación de los datos

Administrador de destino

Después de que se repliquen los datos, se puede verificar si la replicación se ha realizado correctamente.

Siga estos pasos:

1. En la consola de destino, diríjase al almacén de datos de destino en el servidor de puntos de recuperación.
2. Verifique que el tamaño de los datos replicados coincide con los datos de origen.

   Se habrán replicado correctamente los datos entre dos almacenes de datos gestionados mediante consolas de UDP diferentes.

(Opcional) Establecimiento del número de nodos simultáneos para el servidor de puntos de recuperación JumpStart

Administrador de origen

Cuando se inicia una tarea del servidor de puntos de recuperación JumpStart, el número de nodos simultáneos para el almacén de datos es 4 de manera predeterminada. Para especificar el número de nodos simultáneos, debe crearse una clave y agregar manualmente un DWORD para establecer el número.

Siga estos pasos:

1. Inicie sesión en el servidor de punto de recuperación.
2. Vaya a la ubicación siguiente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
3. Cree una clave en el directorio del motor y denomínela *Servidor de puntos de recuperación JumpStart*.
4. Agregue el DWORD siguiente en la clave Servidor de puntos de recuperación JumpStart:

   JumpStartConCurrencyCount
5. Proporcione un valor para el DWORD.

   Ejemplo: si se desea limitar a 10 nodos por tarea del servidor de puntos de recuperación JumpStart, debe agregarse lo siguiente como DWORD:

   JumpStartConCurrencyCount=10

   Se establece el número de nodos simultáneos para el servidor de puntos de recuperación JumpStart.

Cómo realizar la replicación inversa

Con esta función, se pueden replicar datos (punto de recuperación) desde la nube, MSP o el servidor de puntos de recuperación gestionado de forma remota a un servidor de puntos de recuperación local o a una instancia local de UDP. Para recuperar los datos replicados en la instancia local de UDP o en el servidor local de un servidor de puntos de recuperación que se gestiona desde una Consola de Arcserve UDP diferente como, por ejemplo, la nube, MSP o el servidor de puntos de recuperación gestionado de forma remota, es necesario realizar la replicación inversa. En la replicación inversa, los datos se replican desde un almacén de datos de origen

(en la Consola de origen) hasta un almacenes de datos de destino (en la Consola de destino).

Esta sección incluye los siguientes temas:

Revisión de los requisitos previos

Revise los siguientes requisitos previos antes de replicar volúmenes:

- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Administrador: consola de destino

- Verifique que se ha instalado Arcserve UDP en el servidor de destino.
- Verifique que tiene privilegios completos para crear cuentas de usuario de Windows en el servidor de destino.
- Compruebe que se ha activado la casilla de verificación **Permitir la recuperación de puntos de recuperación** en la Configuración avanzada durante la replicación desde la creación de un plan del servidor de puntos de recuperación gestionado remotamente.

  Nota: Si no activa la casilla de verificación **Permitir la recuperación de puntos de recuperación** e inicia la tarea de replicación inversa para la Consola remota, se le pedirá que active el indicador remoto Permitir recuperación para la replicación inversa.

Administrador: consola de UDP de origen

- Verifique que se ha instalado Arcserve UDP en el servidor de origen.
- Verifique que dispone de al menos una copia de seguridad entera completada en un almacén de datos.

Realización de la replicación ad hoc

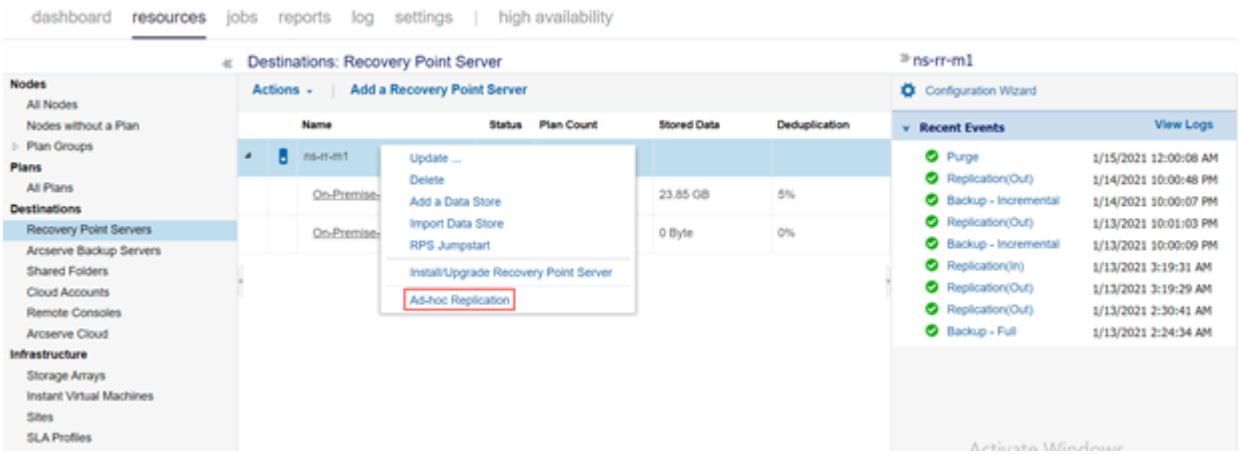
Esta sección explica cómo iniciar la replicación ad hoc.

Nota: Antes de realizar la replicación ad hoc, asegúrese de que la replicación directa se ejecuta correctamente. Para verificar si la replicación directa es correcta, consulte Verificación de los datos replicados.

Siga estos pasos:

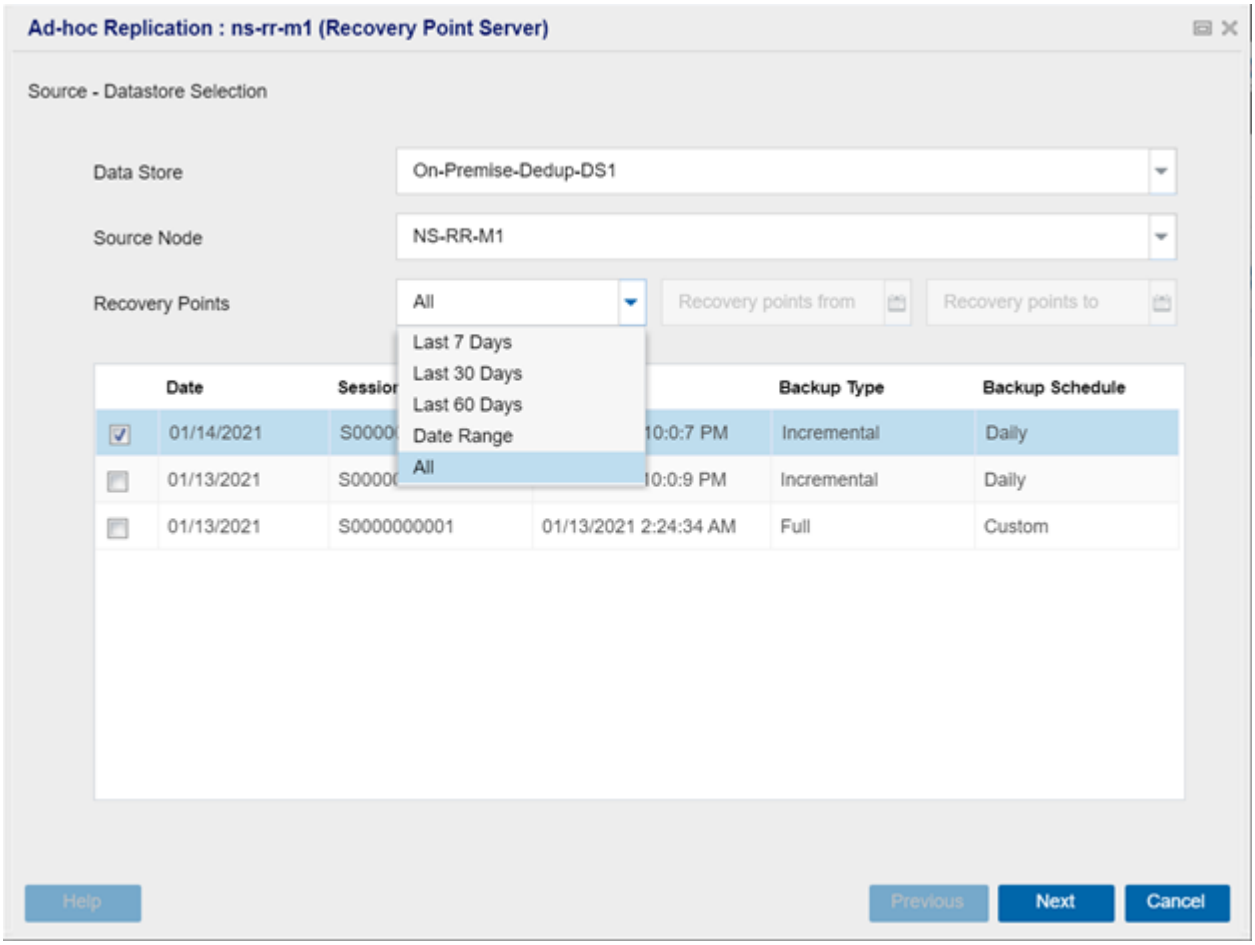
1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** > **Servidores de puntos de recuperación**.

   La lista de servidores de puntos de recuperación aparece en el panel central.
3. Haga clic con el botón secundario del ratón en el servidor de puntos de recuperación y, a continuación, seleccione **Replicación ad hoc**.



   Espere hasta que se conecte al servidor de puntos de recuperación.

   Se abrirá el cuadro de diálogo Replicación ad hoc: xx-xx-xx (servidor de puntos de recuperación).
4. En la página Origen: Selección del almacén de datos, haga lo siguiente:



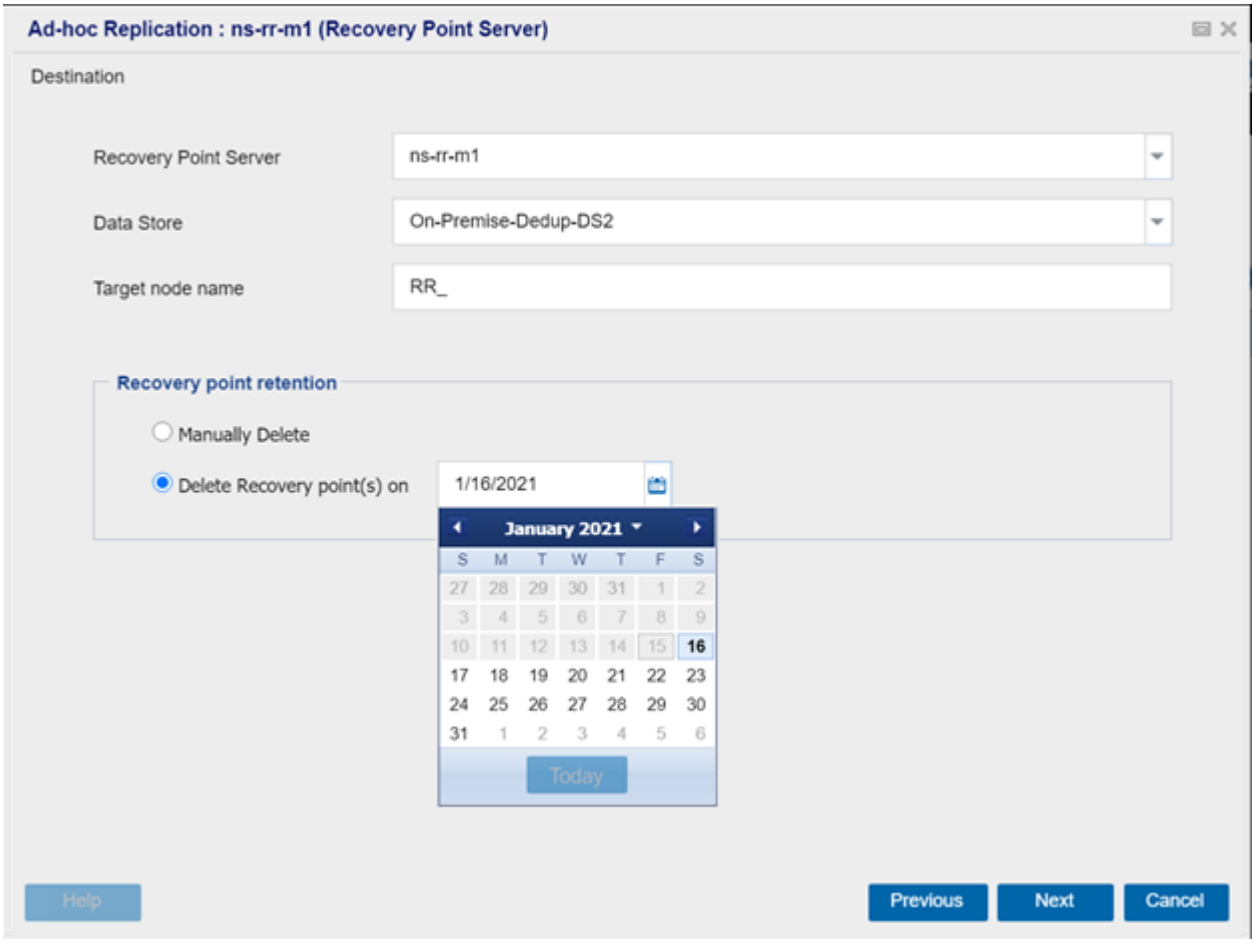
- Almacén de datos: Seleccione el almacén de datos de origen en la lista desplegable.
- Nodo de origen: Seleccione el nodo de origen en la lista desplegable.
- Puntos de recuperación: Realice una de las siguientes acciones:
  - Si desea que se muestren todos los puntos de recuperación de los que se ha realizado la copia de seguridad, seleccione **Todo** en la lista desplegable.
  - Si desea que los puntos de recuperación se muestren durante un período específico, seleccione una de las siguientes opciones en la lista desplegable:
    - Últimos 7 días
    - Últimos 30 días
    - Últimos 60 días
    - Intervalo de fechas

Nota: Si se ha seleccionado **Intervalo de fechas**, establezca la fecha en los campos **Puntos de recuperación desde** y **Puntos de recuperación a**.

Se muestran todos los puntos de recuperación asociados dentro de la duración especificada.

- En la tabla, haga clic en las casillas de verificación para seleccionar uno o más puntos de recuperación.

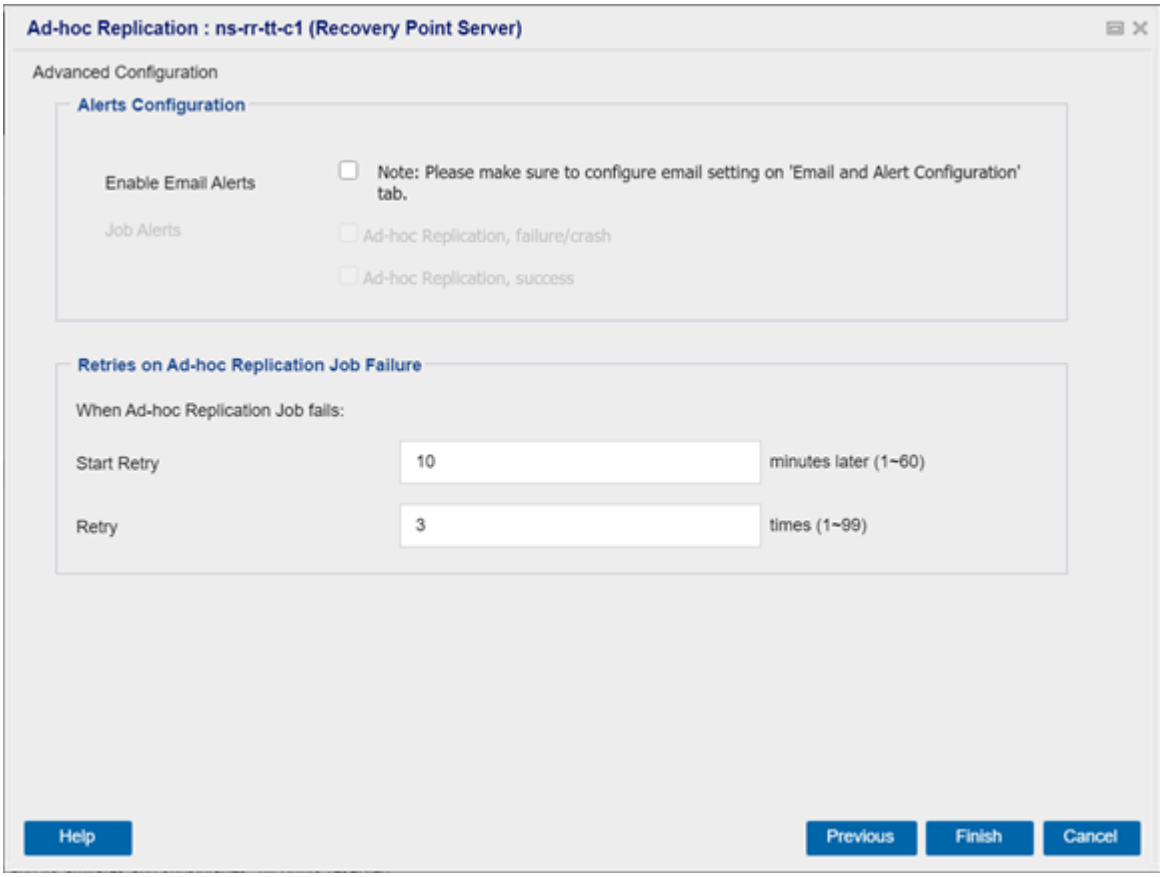
5. Haga clic en **Siguiente**.
6. En la página Destino, haga lo siguiente:



- Servidor de puntos de recuperación: Seleccione el servidor de puntos de recuperación de destino en la lista desplegable.
- Almacén de datos: Seleccione el almacén de datos de destino en la lista desplegable.
- Nombre del nodo de destino: Especifique el nombre de nodo de destino de su elección.

- Retención del punto de recuperación: Suprima los puntos de recuperación de una de las siguientes maneras:
  - Para suprimir los puntos de recuperación manualmente, seleccione la opción **Suprimir manualmente.**
  - Si desea que los puntos de recuperación se supriman automáticamente, seleccione la opción **Suprimir puntos de recuperación en** y, a continuación, especifique la fecha. Todos los puntos de recuperación correspondientes a esa fecha se suprimirán automáticamente.

7. Haga clic en **Siguiente**.
8. En la página Configuración avanzada, haga lo siguiente:



- Para la configuración de alertas

  Activar Alertas de correo electrónico

  Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y especificar los tipos de alertas que se desea recibir en un correo electrónico. Al seleccionar la opción **Nota: Asegúrese de configurar el correo**

electrónico en la ficha Configuración de correo electrónico y alertas., la siguiente opción está activada para su selección:

Alertas de tarea

Le permite seleccionar el tipo de correo electrónico de alerta de las tareas que se desea recibir.

- Si desea recibir alertas de correo electrónico para los errores o bloqueos de la replicación ad hoc, seleccione la casilla de verificación **Replicación ad hoc, error/bloqueo**.

  Nota: Esta alerta de correo electrónico se envía con importancia alta. Las alertas de correo electrónico que tienen una configuración de alta importancia muestran un indicador visual con un signo de admiración en la bandeja de entrada.

- Si desea recibir alertas de correo electrónico sobre la realización correcta de la replicación ad hoc, seleccione la casilla de verificación **Replicación ad hoc, correcta**.

- Para Reintentos en caso de error de la tarea de replicación ad hoc

  Cuando se produce un error en la tarea de replicación ad hoc, haga lo siguiente:

  Iniciar reintento

  Le permite especificar el tiempo (en minutos) restante para reiniciar la tarea de replicación después de que se produzca un error en la tarea. Por ejemplo, si se especifican 10 minutos, la tarea de replicación se reinicia después de que pasen 10 minutos del error.

  Límite: 1 a 60

  Reintentar

  Permite especificar el número de reintentos que se desea realizar si la tarea de replicación produce un error. La tarea de replicación se ejecuta hasta que la tarea sea correcta o hasta que se alcance el límite. Tras superar el número de reintentos, la tarea de replicación se ejecutará solamente en el siguiente período programado.

  Límite: 1 a 99

9. Haga clic en **Finalizar**.

Nota: Si desea cambiar la configuración de las pantallas anteriores, haga clic en **Atrás** y, a continuación, cambie la configuración según sea necesario.

Aparece el cuadro de diálogo Información, que muestra el mensaje *La tarea de replicación ad hoc se ha enviado.*.

10. Haga clic en **Aceptar** para cerrar el cuadro de diálogo de información.

    La replicación ad hoc se ha realizado correctamente.

Control del estado de la replicación ad hoc

Administrador de origen

Después de que la replicación ad hoc sea correcta, se puede controlar el estado de la tarea de replicación ad hoc.

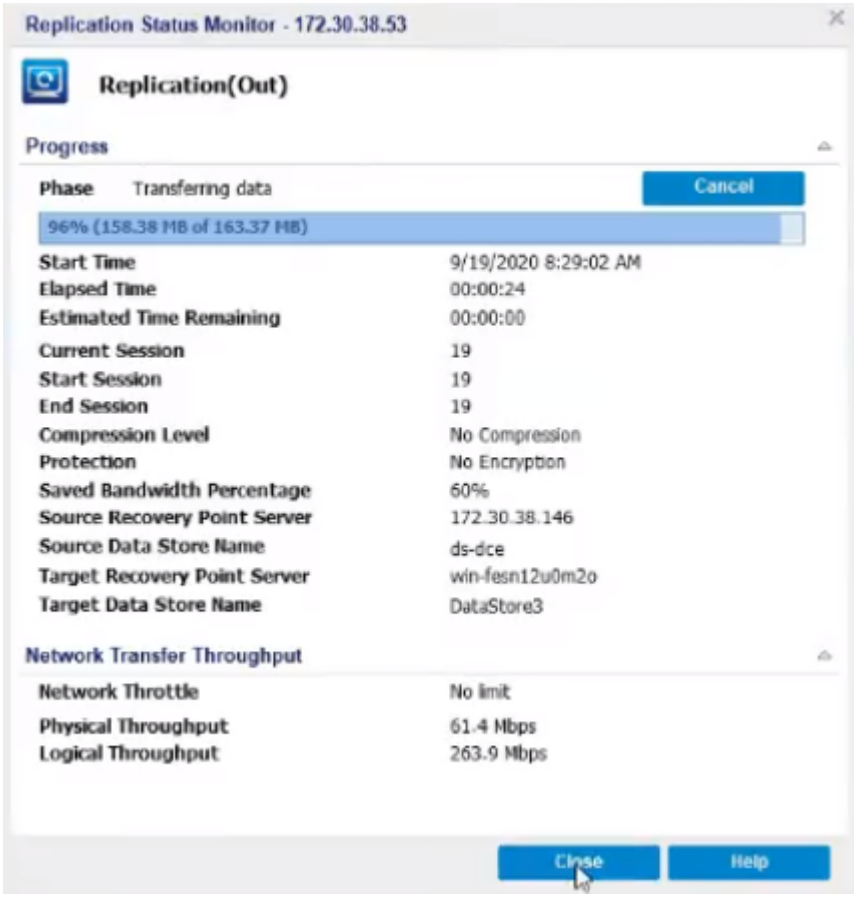
Siga estos pasos:

1. Vaya a **tareas** > **Tareas en ejecución**.

   Las tareas de replicación (saliente) y de replicación (entrante) que están en curso aparecen en el panel central.

2. Para controlar el estado de una tarea específica, haga clic en **Detalles** junto a la barra de progreso correspondiente a esa tarea.

   Aparecerá el cuadro de diálogo Controlador del estado de la replicación: xx.-xx.xx.xx



3. Espere hasta que la transferencia de datos sea del 100 % y, a continuación, haga clic en **Cerrar**.

Se ha controlado correctamente el estado de la replicación ad hoc.

Verificación de si la replicación ad hoc es correcta

Administrador de origen

Después de que se repliquen los datos, se puede verificar si la replicación ad hoc se ha realizado correctamente.

Siga estos pasos:

1. En la consola de origen, vaya a **tareas** > **Tareas finalizadas correctamente**.

   Aparecerá una lista de las tareas completadas en el panel central.

2. Haga clic en la tarea de replicación inversa finalizada. Se actualiza el panel derecho.
3. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
4. Compruebe que la replicación de datos sea correcta.

Se ha verificado correctamente la replicación ad hoc.

Realización de la replicación inversa desde la Consola remota al servidor del servidor de puntos de recuperación local

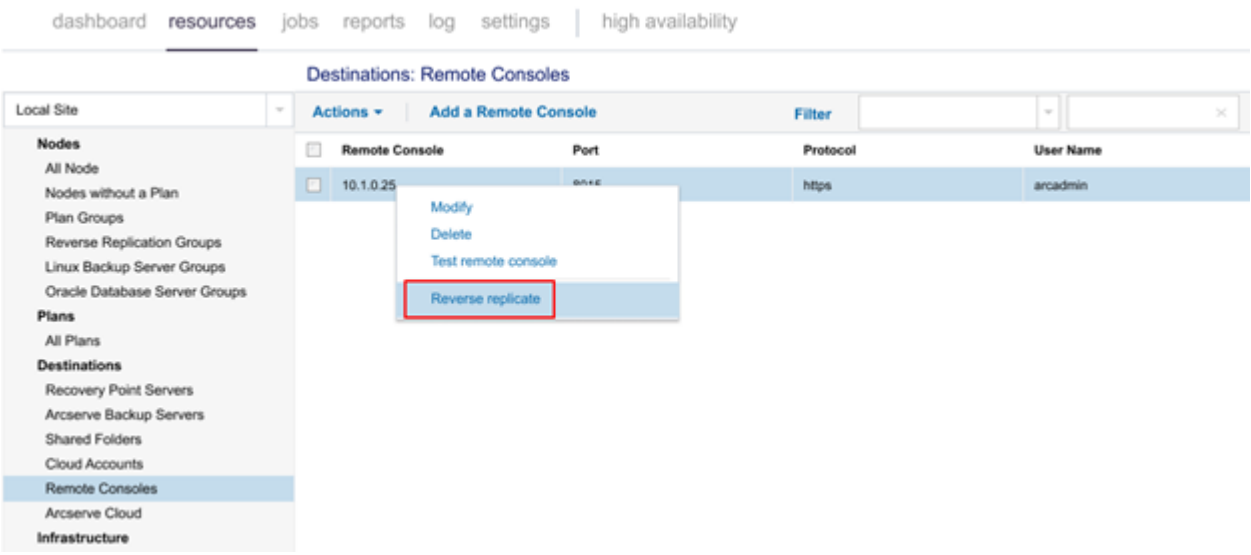
Esta sección explica cómo realizar la replicación inversa desde la Consola remota a la instancia local de UDP o al servidor de puntos de recuperación local.

Nota: Antes de realizar la replicación inversa, asegúrese de que la replicación directa se ejecuta correctamente. Para verificar si la replicación directa es correcta, consulte Verificación de los datos replicados.

Siga estos pasos:

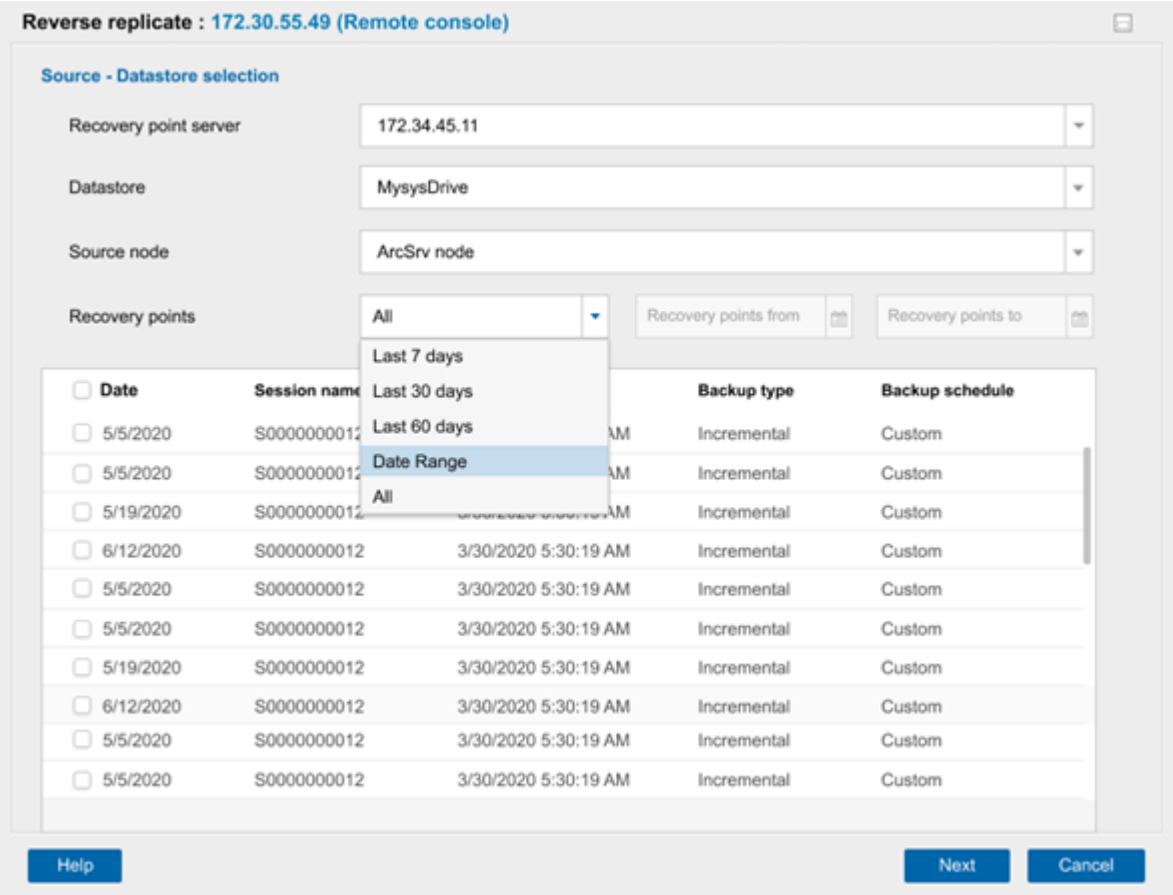
1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** > **Consolas remotas**.

   La lista de consolas remotas aparece en el panel central.
3. Haga clic con el botón secundario del ratón en la consola remota y, a continuación, seleccione **Replicación inversa**.



   Espere hasta que se conecte a la consola remota.

   Se abre el cuadro de diálogo Replicación inversa: xxx.xx.xx.xxx (Consola remota).
4. En la página Origen: Selección del almacén de datos, haga lo siguiente:



- Servidor de puntos de recuperación: Seleccione el servidor de puntos de recuperación de origen en la lista desplegable.
- Almacén de datos: Seleccione el almacén de datos de origen en la lista desplegable.
- Nodo de origen: Seleccione el nodo de origen en la lista desplegable.
- Puntos de recuperación: Realice una de las siguientes acciones:
  - Si desea que se muestren todos los puntos de recuperación de los que se ha realizado la copia de seguridad, seleccione **Todo** en la lista desplegable.
  - Si desea que los puntos de recuperación se muestren durante un período específico, seleccione una de las siguientes opciones en la lista desplegable:
    - Últimos 7 días
    - Últimos 30 días

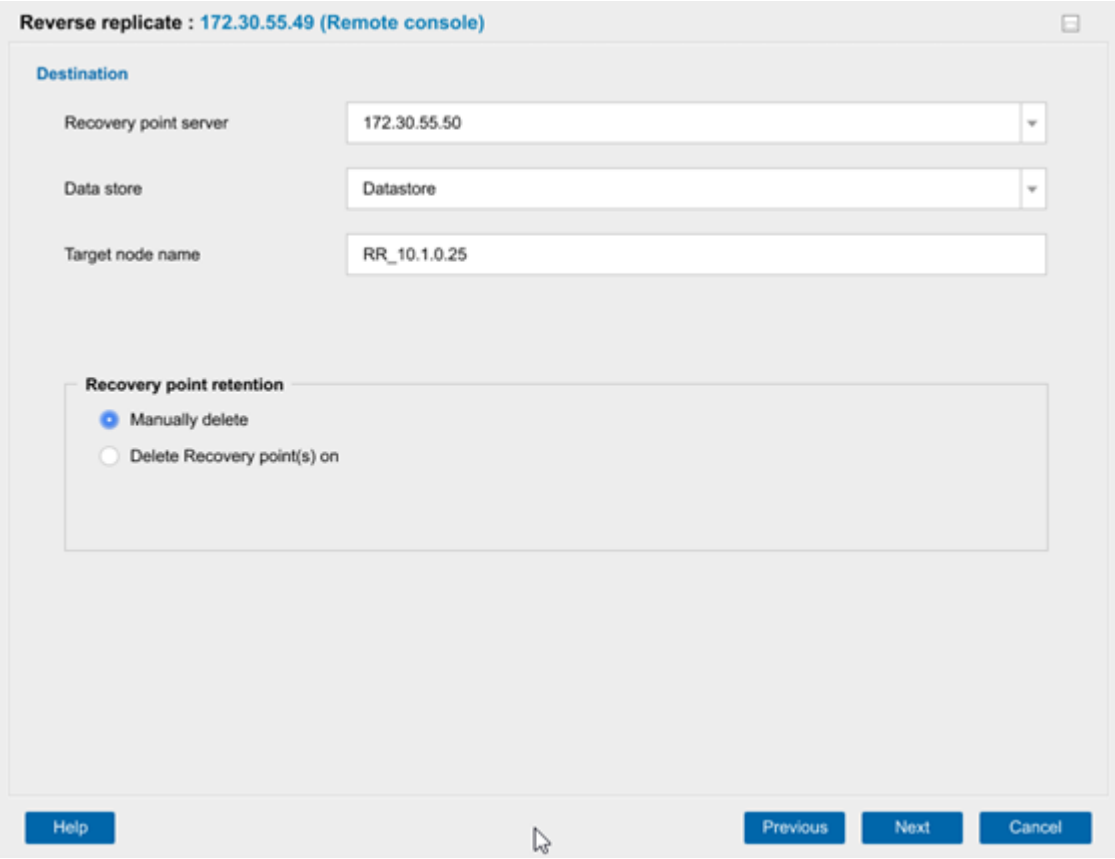
- Últimos 60 días
- Intervalo de fechas

Nota: Si se ha seleccionado **Intervalo de fechas**, establezca la fecha en los campos **Puntos de recuperación desde** y **Puntos de recuperación a**.

Se muestran todos los puntos de recuperación asociados dentro de la duración especificada.

- En la tabla, haga clic en las casillas de verificación para seleccionar uno o más puntos de recuperación.

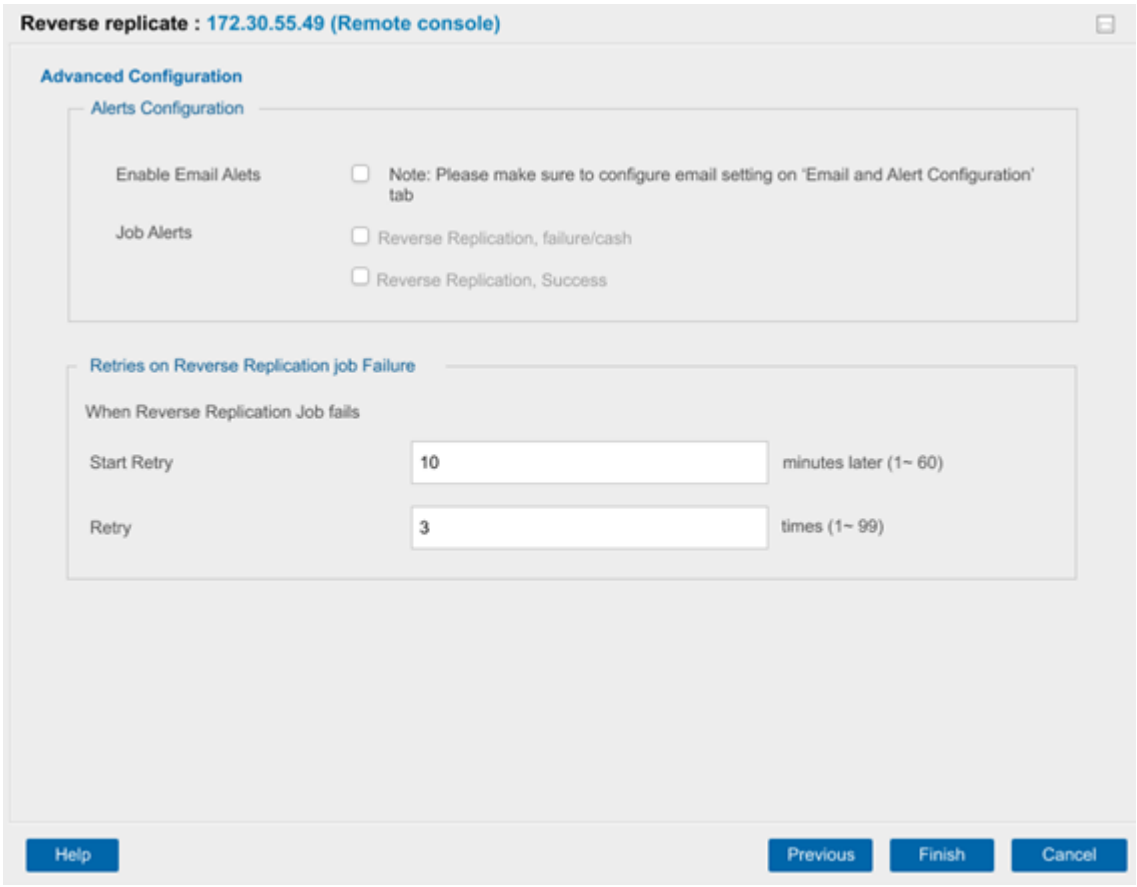
5. Haga clic en **Siguiente**.
6. En la página Destino, haga lo siguiente:



- Servidor de puntos de recuperación: Seleccione el servidor de puntos de recuperación de destino en la lista desplegable.
- Almacén de datos: Seleccione el almacén de datos de destino en la lista desplegable.
- Nombre del nodo de destino: Especifique el nombre de nodo de destino de su elección.

- Retención del punto de recuperación: Suprima los puntos de recuperación de una de las siguientes maneras:
  - Para suprimir los puntos de recuperación manualmente, seleccione la opción **Suprimir manualmente.**
  - Si desea que los puntos de recuperación se supriman automáticamente, seleccione la opción **Suprimir puntos de recuperación en** y, a continuación, especifique la fecha. Todos los puntos de recuperación correspondientes a esa fecha se suprimirán automáticamente.

7. Haga clic en **Siguiente**.
8. En la página Configuración avanzada, haga lo siguiente:



- Para la configuración de alertas

  Activar Alertas de correo electrónico

  Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y especificar los tipos de alertas que se desea recibir en un correo electrónico. Al seleccionar la opción **Nota: Asegúrese de configurar el correo**

electrónico en la ficha Configuración de correo electrónico y alertas., la siguiente opción está activada para su selección:

Alertas de tarea

Le permite seleccionar el tipo de correo electrónico de alerta de las tareas que se desea recibir.

- Si desea recibir alertas de correo electrónico para los errores o bloqueos de la replicación inversa, seleccione la casilla de verificación **Replicación inversa, error/bloqueo**.

  Nota: Esta alerta de correo electrónico se envía con importancia alta. Las alertas de correo electrónico que tienen una configuración de alta importancia muestran un indicador visual con un signo de admiración en la bandeja de entrada.

- Si desea recibir alertas de correo electrónico sobre la realización correcta de la replicación inversa, seleccione la casilla de verificación **Replicación inversa, correcta**.

- Para reintentos en caso de error de la tarea de replicación inversa

  Cuando se produce un error en la tarea de replicación inversa, haga lo siguiente:

  Iniciar reintento

  Le permite especificar el tiempo (en minutos) restante para reiniciar la tarea de replicación después de que se produzca un error en la tarea. Por ejemplo, si se especifican 10 minutos, la tarea de replicación se reinicia después de que pasen 10 minutos del error.

  Límite: 1 a 60

  Reintentar

  Permite especificar el número de reintentos que se desea realizar si la tarea de replicación produce un error. La tarea de replicación se ejecuta hasta que la tarea sea correcta o hasta que se alcance el límite. Tras superar el número de reintentos, la tarea de replicación se ejecutará solamente en el siguiente período programado.

  Límite: 1 a 99

9. Haga clic en **Finalizar**.

Nota: Si desea cambiar la configuración de las pantallas anteriores, haga clic en **Atrás** y, a continuación, cambie la configuración según sea necesario.

Aparece el cuadro de diálogo Información, que muestra el mensaje *La tarea de replicación inversa se ha enviado.*.

10. Haga clic en **Aceptar** para cerrar el cuadro de diálogo de información.

    La replicación inversa se completa correctamente desde la Consola remota a la instancia local de UDP o al servidor de puntos de recuperación local.

Control del estado de la replicación inversa

Administrador de origen

Después de que la replicación inversa sea correcta, se puede controlar el estado de la tarea de replicación inversa.

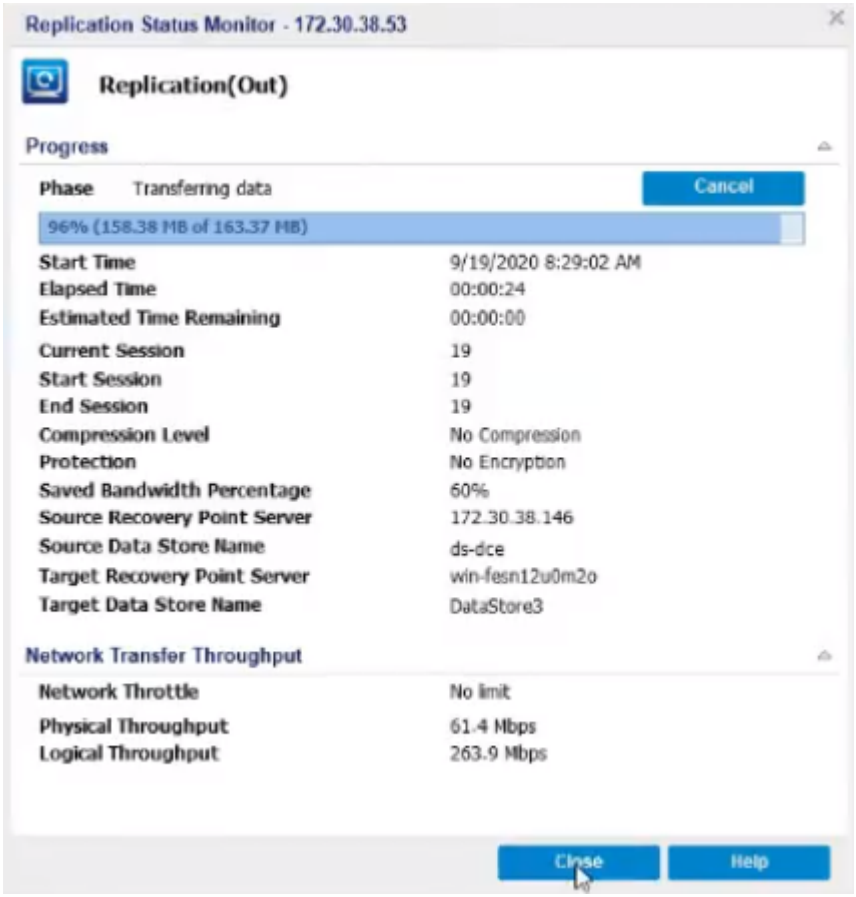
Siga estos pasos:

1. Vaya a **tareas** > **Tareas en ejecución**.

   Las tareas de replicación (saliente) y de replicación (entrante) que están en curso aparecen en el panel central.

2. Para controlar el estado de una tarea específica, haga clic en **Detalles** junto a la barra de progreso correspondiente a esa tarea.

   Aparecerá el cuadro de diálogo Controlador del estado de la replicación: xx.-xx.xx.xx



3. Espere hasta que la transferencia de datos sea del 100 % y, a continuación, haga clic en **Cerrar**.

Se ha controlado correctamente el estado de la replicación inversa.

Verificación de si la replicación inversa es correcta

Administrador de origen

Después de que se repliquen los datos, se puede verificar si la replicación inversa se ha realizado correctamente.

Siga estos pasos:

1. En la consola de origen, vaya a **tareas** > **Tareas finalizadas correctamente**.

   Aparecerá una lista de las tareas completadas en el panel central.
2. Haga clic en la tarea de replicación inversa finalizada. Se actualiza el panel derecho.
3. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
4. Compruebe que la replicación de datos sea correcta.

Se ha verificado correctamente la replicación inversa de los datos desde la Consola remota a la instancia local de UDP o al servidor de puntos de recuperación local.

Cómo crear un plan de copia de puntos de recuperación

Mediante Arcserve Unified Data Protection se pueden copiar los puntos de recuperación en la nube, en una carpeta compartida o en un volumen local para proteger los puntos de recuperación. Este proceso garantiza que se tiene una copia adicional de los puntos de recuperación si los puntos de recuperación originales se suprimen accidentalmente. La tarea de copia de puntos de recuperación copia los puntos de recuperación del destino de la copia de seguridad a la nube, a una carpeta compartida o a un volumen local solamente. No se puede copiar el punto de recuperación a un servidor de punto de recuperación.

Se puede agregar solamente una tarea de copia de puntos de recuperación a un plan.

Notas:

- En la versión actual, las tareas de copia del punto de recuperación no se admiten si la **Copia de seguridad: Linux, basada en el agente** se ha creado como Tarea1.
- Las tareas de copia del punto de recuperación siempre se ejecutan en el Agente, incluso si la copia de seguridad está configurada en el servidor de puntos de recuperación.

  Para la copia de seguridad de la máquina virtual sin agente, el servidor proxy del Agente de UDP utilizado en Tarea1 procesa la tarea de copia del punto de recuperación.

Solución de problemas: Congestión del ancho de banda con las tareas de copia de punto de recuperación de copia a la nube

¿Qué hacer a continuación?

- Revisión de las consideraciones y los requisitos previos
- Creación de un plan con una tarea de copia de seguridad
- Adición de una tarea de copia de puntos de recuperación al plan
- Verificación del plan

Revisión de las consideraciones y requisitos previos

Verifique si se han completado los requisitos previos siguientes:

- Inicie sesión en la Consola.
- Se ha instalado el componente del servidor y se han creado almacenes de datos si se desea almacenar los datos de la copia de seguridad en servidores de punto de recuperación.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Creación de un plan con una tarea de copia de seguridad

Un plan incluye tipos diferentes de tareas que se desea realizar. Para crear una tarea de copia de puntos de recuperación, se debe tener primero un punto de recuperación válido. Para obtener un punto de recuperación válido, tiene que crear una tarea de copia de seguridad.

La tarea de copia de seguridad realiza una copia de seguridad de los nodos de origen y almacena los datos en el destino especificado. La copia de puntos de recuperación es compatible tanto con la copia de seguridad sin agente basada en el host como con la copia de seguridad de Windows basada en el agente. El procedimiento siguiente explica los pasos para crear la tarea de copia de seguridad de Windows basada en el agente. No se puede realizar la copia del punto de recuperación para los planes de copia de seguridad basados en el Agente de Linux.

Nota: Para obtener más información sobre la copia de seguridad sin agente basada en el host, consulte Cómo crear un plan de copia de seguridad de máquina virtual basada en el host.

Para obtener más información sobre la copia de seguridad de la ruta UNC, consulte Cómo crear un plan de copia de seguridad de la ruta UNC.

Para obtener más información sobre la copia de seguridad de Exchange Online, consulte Cómo crear un plan de copia de seguridad de Exchange Online.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Detener plan** para detener el plan.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un

nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.

6. En la lista desplegable **Tipo de tarea** seleccione **Copia de Seguridad, Windows basado en el agente**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

La página Origen le permite especificar los nodos de origen que se desean proteger. Se pueden seleccionar más de un nodo del plan. Si no se ha agregado ningún nodo a la consola, se podrán agregar nodos al crear o modificar un plan en la página Origen. Se puede guardar un plan sin agregar ningún nodo de origen. El plan se implementa solamente después de agregar nodos de origen.

Siga estos pasos:

1. En la ficha Origen, haga clic en **Agregar**.
2. Seleccione una de las opciones siguientes:

   Seleccionar los nodos para proteger en Arcserve UDP

   Abre el cuadro de diálogo Seleccionar los nodos para proteger en Arcserve UDP. Seleccione los nodos de la lista que se muestra. Seleccione esta opción si ya se han agregado los nodos a la consola.

   Agregar nodo de Windows

   Se abre el cuadro de diálogo Agregar nodos a un plan. Seleccione esta opción si no se han agregado los nodos y desea agregarlos manualmente para la protección.

   Detectar nodos desde Active Directory

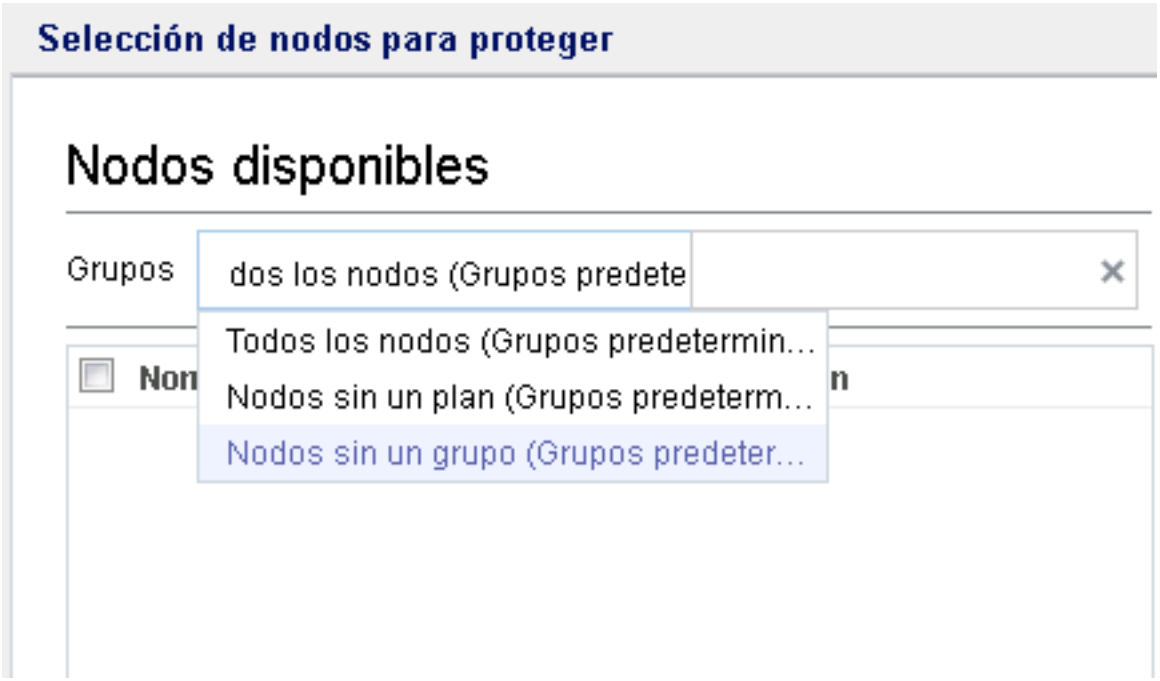
   Se abre el cuadro de diálogo Agregar nodos a la Consola de Arcserve UDP. Seleccione esta opción si desea detectar y agregar nodos en Active Directory.
3. Si ha seleccionado la opción **Seleccionar nodos para proteger en Arcserve UDP**, haga lo siguiente en el cuadro de diálogo Seleccionar nodos para proteger:
   a. (Opcional) Seleccione un filtro en la lista desplegable Grupos para filtrar nodos. Se pueden especificar palabras clave para filtrar más detalladamente los nodos.

      Los nodos se muestran en la columna Nodos disponibles.

   b. Seleccione los nodos en la columna Nodos disponibles y, a continuación, haga clic en la flecha simple hacia la derecha (>) o en la flecha doble hacia la derecha (>>) para mover los nodos seleccionados o todos los nodos respectivamente a la columna Nodos seleccionados.

      Los nodos se muestran en la columna Nodos seleccionados.

   c. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.



4. Para elegir el Tipo de El Protección, seleccione una de las opciones siguientes:

   Realizar copia de seguridad de todos los volúmenes

   Prepara una instantánea de copia de seguridad de todos los volúmenes.

   Realizar copia de seguridad de los volúmenes seleccionados

   Prepara una instantánea de copia de seguridad del volumen seleccionado.

   Se especifica el origen.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Seleccione uno de los siguientes **Tipos de destino**:

   Disco local o carpeta compartida

   Especifica que el destino de la copia de seguridad es un destino local o una carpeta compartida. Si se selecciona esta opción, se pueden guardar datos como puntos de recuperación o como conjuntos de recuperación. Las opciones Puntos de recuperación y Conjuntos de recuperación están disponibles en la ficha **Programación**.

   Servidor de puntos de recuperación de Arcserve UDP

   Especifica que el destino de la copia de seguridad es un servidor de puntos de recuperación. Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.

2. Si se ha seleccionado **Servidor de puntos de recuperación de Arcserve UDP**, se deben proporcionar los detalles siguientes:
   a. Seleccione un servidor de puntos de recuperación.
   b. Seleccione un almacén de datos. La lista muestra todos los almacenes de datos que se han creado en el servidor de punto de recuperación especificado.
   c. Proporcione una contraseña de la sesión.
   d. Confirme la contraseña de la sesión.

3. Si ha seleccionado **Disco local o carpeta compartida**, a continuación proporcione los detalles siguientes:
   a. Proporcione la ruta completa del destino local o de red. Para el destino de la red, especifique las credenciales con acceso de escritura.
   b. Seleccione el algoritmo de cifrado. Para obtener más información, consulte Configuración de cifrado.
   c. Opcionalmente, proporcione una contraseña de cifrado.
   d. Confirme la contraseña de cifrado.

e. Seleccione un tipo de compresión. Para obtener más información, consulte Tipo de compresión.

Notas:

- La copia del punto de recuperación (CRP) no admite copias de seguridad personalizadas incluso cuando se agrega la programación de la CRP. Además, la tarea de copia del punto de recuperación no es compatible con la programación de copia de seguridad personalizada.
- La tarea de copia del punto de recuperación a la nube solo admite desde una consola. No es compatible con un agente independiente.
- Tanto las *carpetas de disco local o recursos compartidos* como las *copias de seguridad almacenadas en el servidor de puntos de recuperación* admiten las tareas de copia del punto de recuperación.

Se especifica el destino.

Especificación de la programación

La página Programación permite programar una copia de seguridad. La Copia de puntos de recuperación es compatible con las copias de seguridad diarias, semanales y mensuales desde la consola. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar programaciones diarias, semanales y mensuales, así como también se puede proporcionar la configuración de la retención.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

Siga estos pasos:

1. (Opcional) Seleccione la opción para gestionar puntos de recuperación. Esta opción solo está visible si se ha seleccionado la carpeta local o compartida como destino de la copia de seguridad.

   Retener por puntos de recuperación

   Los datos de la copia de seguridad se almacenan como puntos de recuperación.

   Retener por conjuntos de recuperación

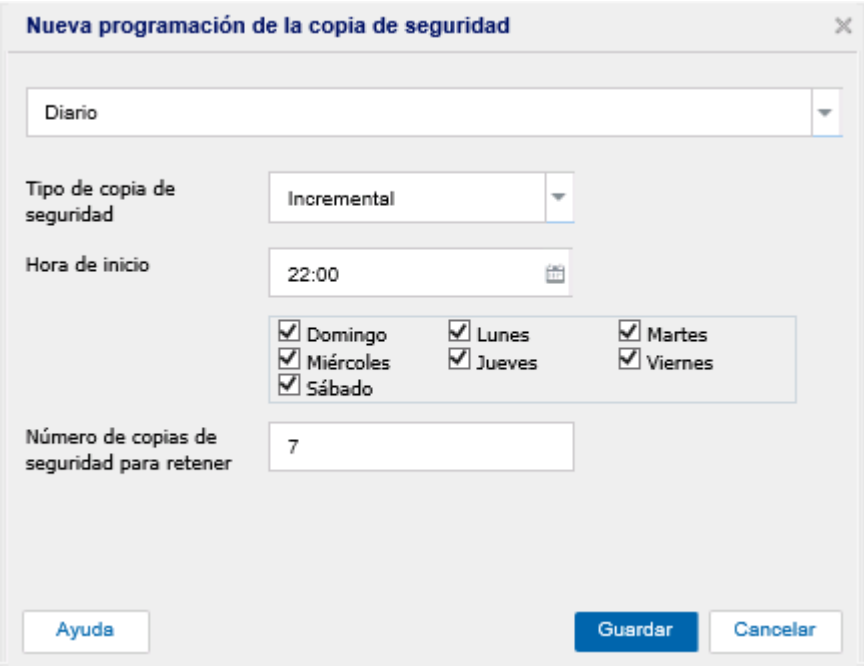
   Los datos de la copia de seguridad se almacenan como conjuntos de recuperación.

   Nota: No se admite Retener por conjuntos de recuperación para la Copia de puntos de recuperación.

2. Agregue la programación de la copia de seguridad.

   a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

      Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

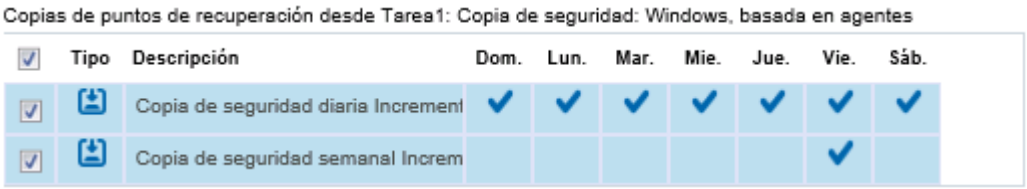
Tal y como se ha programado, Arcserve UDP hará una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

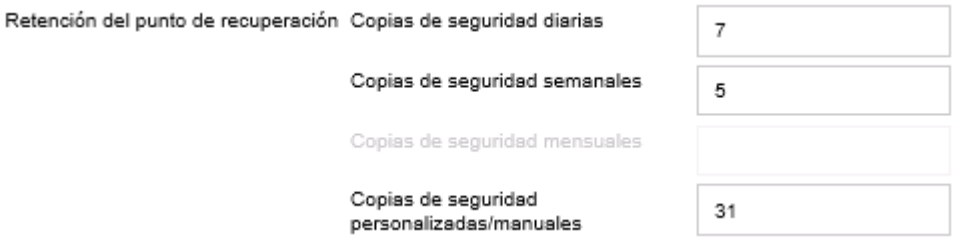
e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



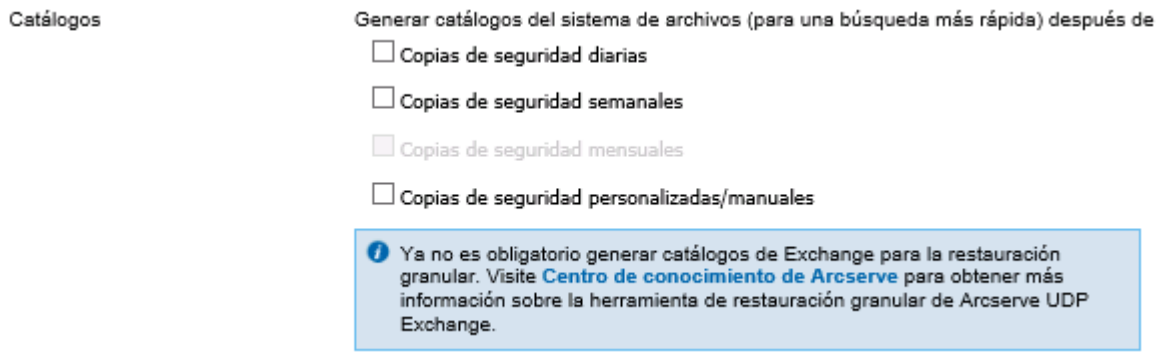
3. Especifique la hora de inicio para la copia de seguridad programada.



4. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Diaria, Semanal y Mensual.

   Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo Programación de la copia de seguridad.

5. Especifique los detalles del catálogo.



Los catálogos permiten generar el catálogo del sistema de archivos. El catálogo del sistema de archivos se requiere para realizar la mejor búsqueda de la forma más rápida. Si se seleccionan las casillas de verificación del catálogo, los catálogos se activan en función del tipo de copia de seguridad especificada. Desactive la casilla de verificación para desactivar la generación del catálogo.

Se especifica la programación.

Funcionamiento de la programación avanzada y de la retención

La opción de programación le permite especificar una programación personalizada, una programación diaria/semanal/mensual o ambas. En la programación personalizada, se puede configurar la programación de la copia de seguridad durante cada día de la semana y se pueden agregar hasta cuatro programaciones de copia de seguridad cada día. Se puede seleccionar un día específico de una semana y crear un período de tiempo para definir cuando se desea ejecutar la copia de seguridad y con qué frecuencia.

Programación	Tarea compatible	Comentarios
Copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para ejecutar las tareas de copia de seguridad.
Regulación de la copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para controlar la velocidad de la copia de seguridad.
Combinar	Tarea de combinación	Defina cuando se deben ejecutar las tareas de combinación.
Programación diaria	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad diarias.
Programación semanal	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad semanales.
Programación mensual	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad mensuales.

Se pueden especificar también los valores de configuración de retención para los puntos de recuperación.

Nota: Establezca la configuración de la retención en cada plan para controlar cómo se retienen los datos para los nodos asignados a ese plan en el almacén de datos de destino.

Las programaciones para las copias de seguridad diarias/semanales/mensuales son independientes de la programación personalizada y de las unas a las otras. Se puede configurar solamente ejecutar una copia de seguridad diaria, una copia de seguridad semanal o una copia de seguridad mensual sin configurar la programación personalizada.

Programación de la tarea de copia de seguridad

Se pueden agregar cuatro períodos de tiempo por día en la programación de la copia de seguridad. Un período de tiempo válido es desde las 12:00 horas hasta las 23:59 horas. No se puede especificar un período de tiempo como, por

ejemplo, de las 18:00 horas a las 06:00 horas. En tales casos, se debe especificar manualmente dos períodos de tiempo diferentes.

Para cada período de tiempo, la hora de inicio está incluida y, en cambio, no se incluye la hora de finalización. Por ejemplo, se ha configurado ejecutar una copia de seguridad incremental ejecutada todas las horas entre las 06:00 horas y las 09:00 horas y la copia de seguridad se iniciará a las 06:00 horas. Esto significa que la copia de seguridad se ejecuta a las 06:00 horas, a las 07:00 horas y a las 08:00 horas, pero NO a las 09:00 horas.

Nota: Si desea ejecutar la tarea de copia de seguridad reiteradamente hasta el final del día, configure la programación hasta las 12:00 horas. Por ejemplo, para ejecutar la tarea de copia de seguridad cada 15 minutos durante todo el día, configure la programación de las 12:00 a las 12:00, cada 15 minutos.

Programación del regulador de la copia de seguridad

La programación del regulador de la copia de seguridad le permite controlar la velocidad del rendimiento de la copia de seguridad, que a su vez controla el uso de recursos (E/S del disco, CPU, ancho de banda de la red) del servidor del que se está realizando la copia de seguridad. Esto es útil si no se desea afectar al rendimiento del servidor durante el horario comercial. Se pueden agregar cuatro períodos de tiempo por día en la programación del regulador de la copia de seguridad. Para cada período de tiempo, se puede especificar un valor en MB por minuto. Este valor se utiliza para controlar el rendimiento de la copia de seguridad. Los valores válidos van desde 1 MB/minuto a 99999 MB/minuto.

Si una tarea de copia de seguridad excede el tiempo especificado, el límite del regulador se ajusta según el período de tiempo especificado. Por ejemplo, se ha definido el límite del regulador de la copia de seguridad en 500 MB/minuto desde las 08:00 horas a las 20:00 horas y en 2500 MB/minuto de las 20:00 horas a las 22:00 horas. Si una tarea de copia de seguridad se inicia a las 19:00 horas y se ejecuta durante tres horas, el límite del regulador es de 500 MB/minuto de las 19:00 horas a las 20:00 horas y de 2500 MB/minuto de las 20:00 horas a las 22:00 horas.

Si no se define ninguna programación de la copia de seguridad ni ninguna programación del rendimiento de la copia de seguridad, la copia de seguridad se ejecuta tan deprisa como pueda.

Programación de la combinación

Le permite combinar puntos de recuperación basándose en la programación proporcionada.

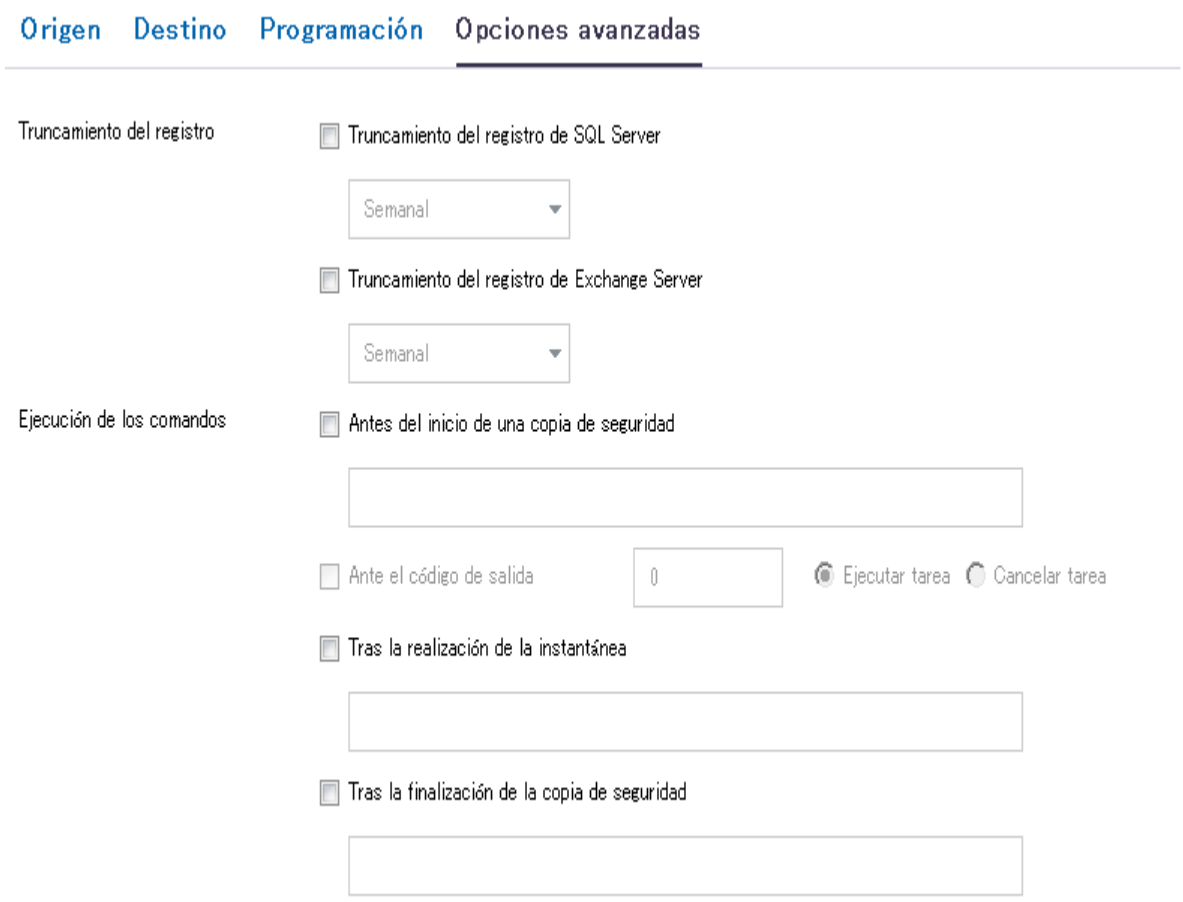
Tenga en cuenta los puntos siguientes para la tarea de combinación:

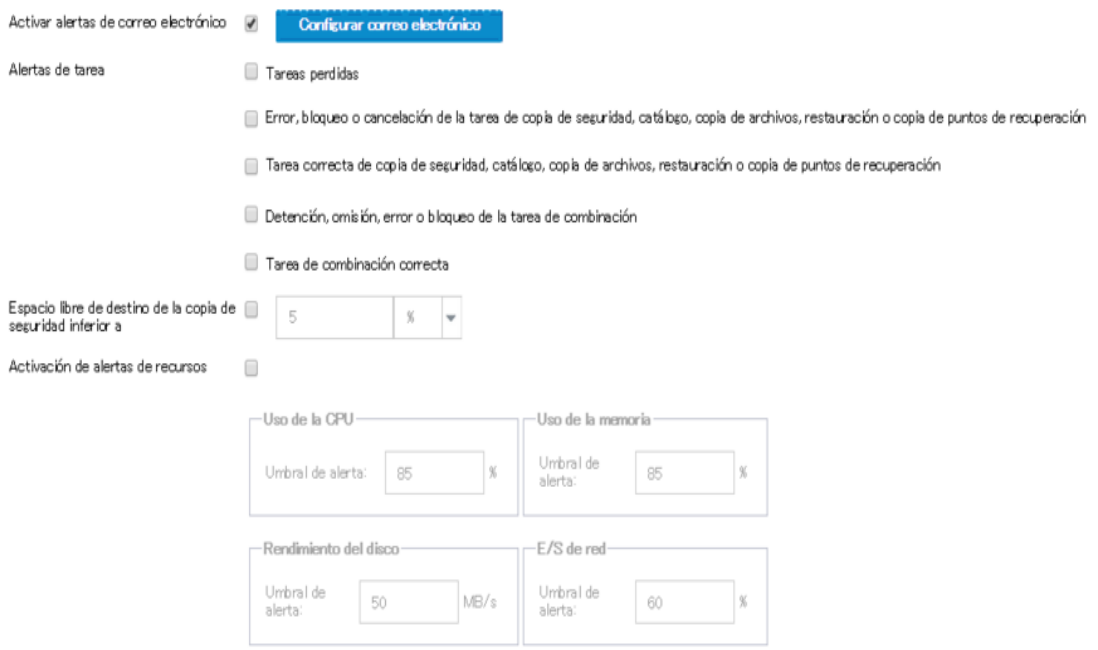
- Solamente una tarea de combinación puede ejecutarse para un nodo en cualquier momento proporcionado.
- Si se inicia una tarea de combinación, se tiene que completar antes de que la siguiente tarea de combinación se pueda iniciar. Esto no significa que, si uno o más conjuntos de puntos de recuperación se combinan, no se pueda agregar un punto de recuperación nuevo a este proceso de combinación hasta que el proceso de combinación del conjunto actual de puntos de recuperación se complete.
- Si una tarea de combinación está procesando más de un conjunto de puntos de recuperación (por ejemplo, el conjunto [1~4], el conjunto [5~11] y el conjunto [12~14] son tres conjuntos), el servidor de puntos de recuperación procesará estos conjuntos uno a uno.
- Si una tarea de combinación se reanuda después de una pausa, la tarea detecta en qué punto se ha pausado y reanuda la combinación a partir del punto de pausa.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye la configuración de registros de truncamiento, proporcionar la ubicación de los scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha Avanzada:





Siga estos pasos:

1. Especifique los siguientes detalles:

Cómo truncar un registro

Le permite especificar la programación para truncar los registros de SQL Server y Exchange Server. Se puede especificar la programación como **Diaria**, **Semanal** o **Mensual**.

Nombre de usuario

Le permite especificar el usuario que se autoriza para ejecutar un script.

Contraseña

Le permite especificar la contraseña del usuario autorizado para ejecutar el script.

Ejecutar un comando antes de empezar una copia de seguridad

Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde el script está almacenado. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de seguridad continuará cuando el script devuelva el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detendrá cuando el script devuelva el código de salida.

Ejecutar un comando después de realizar una instantánea

Le permite ejecutar un script después de realizar la instantánea de la copia de seguridad. Especifique la ruta donde el script está almacenado.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta donde el script está almacenado.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y se pueden especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de tareas que se desea recibir.

Cómo activar las alertas de recurso

Le permite especificar un umbral para el Uso de CPU, Uso de memoria, Rendimiento del disco y E/S de la red. Se puede proporcionar el valor en porcentaje. Se recibirá un correo electrónico cuando se exceda el valor de Umbral de alerta.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en Guardar.

Los cambios se guardan y se muestra una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **Recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar.

El plan de copia de seguridad se crea y se implementa automáticamente en el nodo de origen. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

Adición de una tarea de copia de puntos de recuperación al plan

La tarea de copia de puntos de recuperación copia los puntos de recuperación desde el destino de la copia de seguridad a la nube, a una carpeta compartida o a un volumen local.

Nota: Si una tarea de copia de seguridad está en curso y se pausa el plan, la tarea de copia de seguridad se detendrá y la tarea de copia de puntos de recuperación no se iniciará. Cuando se vuelva a reanudar el plan, la tarea de copia de puntos de recuperación no se reanuda automáticamente. Se debe ejecutar manualmente otra tarea de copia de seguridad para iniciar la tarea de copia de puntos de recuperación.

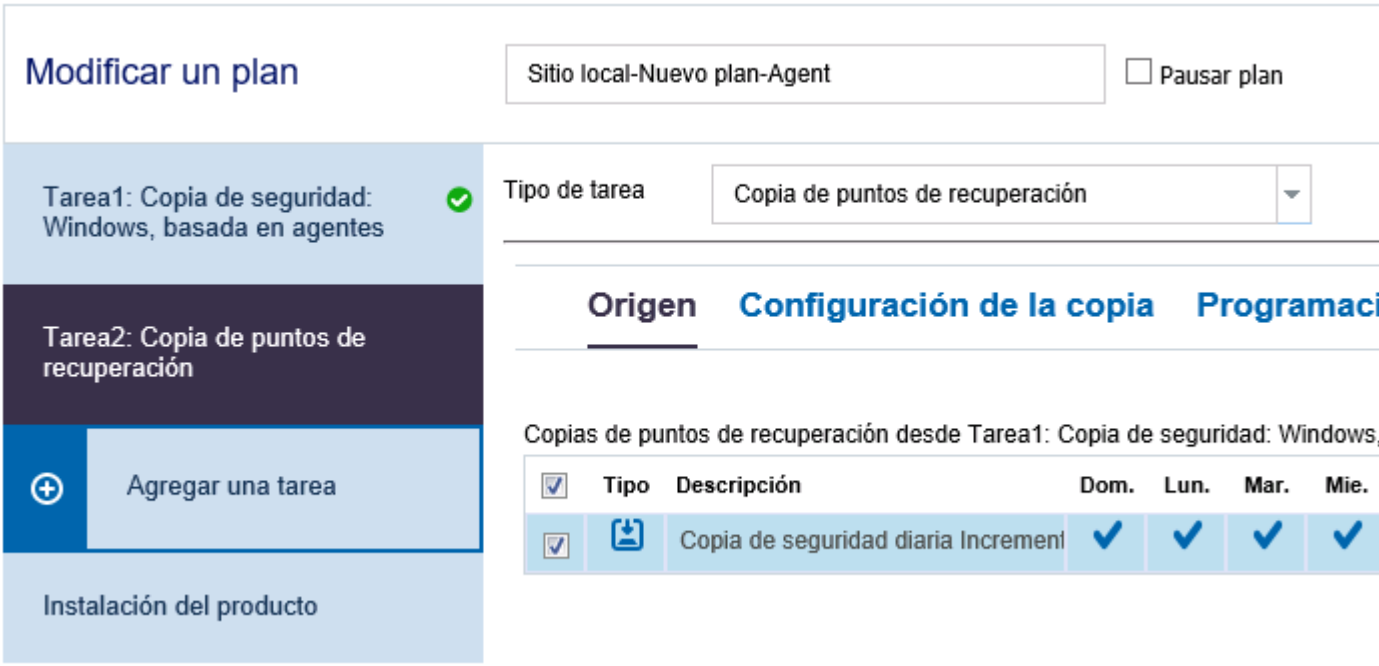
Siga estos pasos:

1. En el panel izquierdo, haga clic en **Agregar una tarea**.

   Una tarea nueva se agrega al panel izquierdo.

2. En la lista desplegable **Tipo de tarea**, seleccione **Copia de puntos de recuperación**.

   La tarea de copia de puntos de recuperación se ha agregado. No es necesario configurar la ficha **Origen** en la tarea de copia del punto de recuperación (CRP). Además, se puede ver el destino de la copia de seguridad en la tarea de copia de seguridad.



Nota: Se puede configurar una ubicación personalizada como ruta de la copia de puntos de recuperación mediante la siguiente clave de registro.

Ruta: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession*

Nombre de la clave: *LocalTempPath*

Tipo de clave: *REG_SZ (cadena)*

Valor de la clave: *"Ruta_disco_local"*

3. En la ficha Origen, seleccione una programación.
4. En la ficha Configuración de copia, proporcione los siguientes detalles:

Tipo de destino

Especifica el tipo de destino. Se puede seleccionar una de las opciones como almacenamiento en la nube, disco local o carpeta compartida. No se puede optar por Servidor de puntos de recuperación como el tipo de destino.

Disco local o carpeta compartida

Es necesario introducir los detalles del destino.

Destino

Especifica el destino donde se desea guardar la copia de puntos de recuperación.

Nota: Haga clic en la flecha para validar el destino proporcionado. La flecha está visible cuando se introduce el destino.

Almacenamiento en la nube

Se debe seleccionar el servicio de la nube y agregar un almacenamiento en la nube.

Para obtener información detallada sobre la estructura de directorios, consulte la sección Estructura de directorios de los puntos de recuperación en el depósito de la nube de S3.

Servicio de la nube

Permite seleccionar una de las opciones del servicio de almacenamiento múltiple disponible.

Almacenamiento en la nube

Permite seleccionar la cuenta de la nube del servicio de almacenamiento seleccionado. Si la lista desplegable no muestra ninguna cuenta, haga clic en **Agregar** para agregar una cuenta.

Activar bloqueo de objetos

Permite proteger el almacenamiento de la nube utilizando la función Bloqueo de objetos. Cuando se selecciona lo siguiente como servicio de la nube, aparece la casilla de verificación Activar bloqueo de objetos.

- Amazon S3
- Wasabi Hot Cloud Storage
- Nutanix Objects

Cuando se selecciona la casilla de verificación **Activar bloqueo de objetos**, se activa el botón Configuración de bloqueo de objetos. Se debe configurar los valores de Configuración de bloqueo de objetos después de activar la casilla de verificación Bloqueo de objetos. Para obtener más información sobre cómo configurar los valores de configuración de Configuración de bloqueo de objetos, consulte Configuración de los valores de configuración del bloqueo de objetos para un servicio de la nube.

Notas:

- Para Amazon S3 y Wasabi Hot Cloud Storage:
  - Se puede activar la opción Bloqueo de objetos solo para los depósitos nuevos.
  - Al modificar un plan, tenga en cuenta lo siguiente:
    - Si se crea un plan con el bloqueo de objetos activado, se desactiva la casilla de verificación *Activar bloqueo de objetos* y se activa el botón *Configuración de bloqueo de objetos*. Se puede modificar el Modo de retención y el Período de retención utilizando el botón *Configuración de bloqueo de objetos*.
    - Si se crea un plan con el bloqueo de objetos desactivado, se desactivan la casilla de verificación *Activar bloqueo de objetos* y el botón *Configuración de bloqueo de objetos*.
- Para Nutanix Objects:
  - Se puede activar la opción del bloqueo de objetos para los depósitos nuevos y antiguos.
  - Al modificar un plan, tenga en cuenta lo siguiente:

- Si se crea un plan con el bloqueo de objetos activado, no se puede desactivar la casilla de verificación *Activar bloqueo de objetos*. Solo se puede aumentar el Período de retención utilizando el botón *Configuración de bloqueo de objetos*.
- Si se crea un plan con el bloqueo de objetos desactivado, se puede activar la casilla de verificación *Activar bloqueo de objetos* y configurar los valores de la Configuración de bloqueo de objetos.

- Cuando se activa la opción Bloqueo de objetos, la configuración de la retención en la ficha Programación no es aplicable.

Compresión

Especifica seleccionar un nivel de compresión para las copias de punto de recuperación. La compresión se suele aplicar para reducir el uso de espacio en disco, pero también tiene un efecto contrario en la velocidad de la copia de seguridad, dado el incremento del uso de la CPU. A continuación se especifican las opciones disponibles:

Sin compresión: no se realiza ninguna compresión. Los archivos son VHD auténticos. Esta opción utiliza menor cantidad de CPU (velocidad más alta), pero también utiliza más espacio en disco para la imagen de copia de seguridad.

Sin compresión - VHD: no se realiza ninguna compresión. Los archivos se convierten directamente al formato .vhd, sin necesidad de realizar operaciones manuales. Esta opción utiliza menor cantidad de CPU (velocidad más alta), pero también utiliza más espacio en disco para la imagen de copia de seguridad.

Compresión estándar: se realizará algún tipo de compresión. Esta opción proporciona un buen equilibrio entre el uso de la CPU y el uso de espacio en disco. Se trata de la configuración predeterminada.

Compresión máxima: se realizará una compresión máxima. Esta opción utiliza mayor cantidad de CPU (velocidad más baja) pero también utiliza menos espacio en disco para la imagen de copia de seguridad.

Nota: Si la imagen de copia de seguridad contiene datos que no pueden comprimirse (como imágenes JPG, archivos ZIP, entre otros), deberá adjudicarse espacio de almacenamiento adicional para tratar estos datos. Como resultado, si ha seleccionado cualquier opción de compresión y dispone de datos que no pueden comprimirse en la copia de seguridad, se puede producir un incremento del uso de espacio en disco.

Algoritmo de cifrado

Especifica el tipo de algoritmo de cifrado que debe utilizarse para las copias de punto de recuperación. Las opciones de formato disponibles son Sin cifrado, AES-128, AES-192 y AES-256.

Contraseña de cifrado

Especifica proporcionar una contraseña de cifrado que se utilizará para cifrar la sesión de destino. Cuando se restaura desde la copia de puntos de recuperación, se debe proporcionar esta contraseña para confirmar su autenticación.

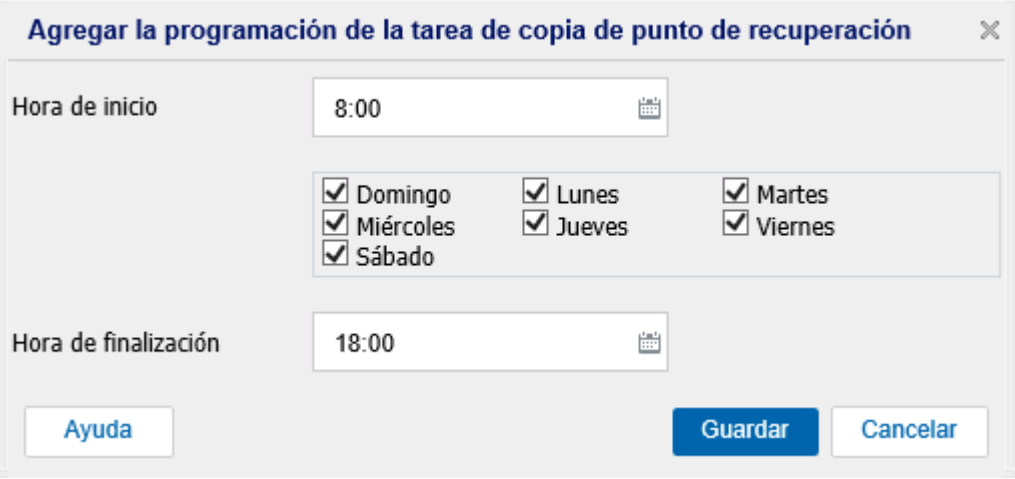
Confirmar contraseña de cifrado

Especifica que se debe volver a introducir la contraseña.

5. Haga clic en la ficha **Programación** para especificar la programación de la tarea.

   Mediante la opción de la programación, se pueden agregar varias programaciones a un punto de recuperación. También se deben tener en cuenta los siguientes detalles:

   - Si no se ha configurado ninguna programación, la tarea de copia de puntos de recuperación se ejecuta inmediatamente después de la finalización de la tarea de copia de seguridad.
   - Ahora, se puede configurar la copia de puntos de recuperación para la hora de inicio y la hora de finalización.



   - La copia de puntos de recuperación siempre intenta comprobar si la sesión está disponible durante las horas especificadas.
   - Si cualquier sesión de copia de seguridad configurada en la ficha Origen está disponible durante el tiempo especificado, la copia de puntos de recuperación copia la sesión al destino correspondiente.

- También se pueden configurar puntos de retención en las opciones Diaria, Semanal y Mensual.

Nota: El número de copias de seguridad correctas se cuenta para cualquier copia de seguridad diaria, semanal o mensual que se haya configurado.

6. Haga clic en **Guardar cambios**.

   Los cambios se guardan y la tarea de copia de puntos de recuperación se implementa automáticamente en el nodo.

   Se ha creado e implementado correctamente el plan de la copia de puntos de recuperación.

Configuración de los valores de configuración del bloqueo de objetos para un servicio de la nube

Esta sección proporciona información sobre cómo configurar los valores de configuración del bloqueo de objetos para un servicio de la nube:

Siga estos pasos:

1. Seleccione la casilla de verificación Activar bloqueo de objetos.

   Se activa el botón Configuración de bloqueo de objetos.

2. Haga clic en el botón Configuración de bloqueo de objetos.

   Aparecerá el cuadro de diálogo Configuración de bloqueo de objetos.

3. En el cuadro de diálogo Configuración de bloqueo de objetos, realice lo siguiente:

   Nota: En el cuadro de diálogo Configuración de bloqueo de objetos, las opciones pueden variar en función del servicio de la nube que se haya seleccionado al crear un plan.

   Amazon S3

   Modo de retención predeterminado

   Permite activar diferentes niveles de protección en las versiones de los objetos. Para activarlos, seleccione una de las siguientes opciones:

   - **Gobierno:** Si tiene permisos de IAM especiales durante el período de retención, puede sobrescribir o suprimir las versiones de objetos protegidos o cambiar la configuración de bloqueo.

- **Conformidad:** No se pueden sobrescribir ni suprimir versiones de objetos protegidos aunque sea un usuario raíz en la cuenta de AWS.

Período de retención predeterminado

Permite especificar una cantidad fija de tiempo para proteger las versiones de objetos. Puede proporcionar un período de retención en días o años.

Wasabi Hot Cloud Storage

Modo de retención predeterminado

Permite activar diferentes niveles de protección en las versiones de los objetos. Para activarlos, seleccione una de las siguientes opciones:

- **Gobierno:** Si tiene permisos de IAM especiales durante el período de retención, puede sobrescribir o suprimir las versiones de objetos protegidos o cambiar la configuración de bloqueo.
- **Conformidad:** No se pueden sobrescribir ni suprimir versiones de objetos protegidos aunque sea un usuario raíz en la cuenta de AWS.

Período de retención predeterminado

Permite especificar una cantidad fija de tiempo para proteger las versiones de objetos. Puede proporcionar un período de retención en días o años.

Nutanix Objects

Período de retención predeterminado

Permite especificar una cantidad fija de tiempo para proteger las versiones de objetos. Puede proporcionar un período de retención en días o años.

Nota: Cuando se activa el bloqueo de objetos mientras se crea un plan para Nutanix Objects, también se activa lo siguiente:

- **Write-Once-Read-Many (WORM):** No se pueden sobrescribir ni suprimir los objetos existentes durante un período de tiempo de retención especificado.
- **Control de versiones:** Se pueden mantener varias versiones de Nutanix Objects en un depósito.

4. Haga clic en **Aceptar**.

Estructura de directorios de los puntos de recuperación en el depósito/contenedor de la nube

Todos los puntos de recuperación de los nodos con un solo plan de CRP y una cuenta de la nube (creada en la Consola de gestión de Arcserve) como destino se almacenan dentro de un depósito de la nube.

La estructura de directorios de los puntos de recuperación en el depósito/contenedor de la nube de es la siguiente:

arcserve-{random-generated-id}-<NombreDepósito>

ca_root_arcserve-recovery-points_<NombreNodo1>

Set0

<AAAA-MM-DD_HH-MM-SS_<TipoProgramación>>

<NombreNodo1>

<AAAA-MM-DD_HH-MM-SS_<TipoProgramación>>

<NombreNodo1>

.....

<AAAA-MM-DD_HH-MM-SS_<TipoProgramación>>

<NombreNodo1>

ca_root_arcserve-recovery-points_<NombreNodo2>

.....

ca_root_arcserve-recovery-points_<NombreNodoN>

Notas:

- Los nuevos cambios en el prefijo arcserve-{ID-generado-aleatorio}- no tienen ningún efecto en los planes existentes.
- El prefijo arcserve-{ID-generado-aleatorio}- se agrega al nombre de depósito configurado en la cuenta de la nube.
- El nombre de nodo es similar al nombre que aparece en el destino de la copia de seguridad.
- AAAA-MM-DD: Formato de fecha (A – año, M – mes, D – día)
- HH:MM:SS: Formato de hora (H – hora, M – minuto, S – segundo)
- <TipoProgramación> es el tipo de programación de la copia de seguridad y hace referencia a una de las opciones siguientes:

- Diaria: Punto de recuperación de la copia de seguridad diaria
- Semanal: Punto de recuperación de la copia de seguridad semanal
- Mensual: Punto de recuperación de la copia de seguridad mensual
- Personalizada: Se ha cargado el punto de recuperación utilizando la opción Cargar punto de recuperación en la nube (punto de recuperación de copia ad hoc)

- Los puntos de recuperación de los nodos que comparten el mismo nombre se almacenan en el mismo directorio si están destinados a la misma cuenta de la nube. Como resultado, se recomienda utilizar cuentas de la nube diferentes para los nodos que comparten el mismo nombre para ayudarles a almacenar en depósitos diferentes.

Verificación del plan

Para verificar la función de la copia de puntos de recuperación, confirme que se ha creado correctamente el plan. Después de verificar que el plan se ha creado correctamente, compruebe si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Después de que la tarea de copia de seguridad se complete correctamente, se ejecutará la tarea de copia de puntos de recuperación. Se puede comprobar el estado de la tarea de copia de seguridad y de la tarea de copia de puntos de recuperación en la ficha **tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga estos pasos para verificar las tareas de copia de puntos de recuperación:

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad y la tarea de copia de puntos de recuperación se han realizado correctamente.

Cómo crear un plan de copia de archivo

Arcserve Unified Data Protection permite copiar o mover los archivos de origen seleccionados a un destino. El destino puede ser un almacenamiento en la nube o una red compartida. El archivo de origen debe ser del mismo volumen del que se ha realizado la copia de seguridad. Por ejemplo, se ha realizado la copia de seguridad de todo el volumen D:\ del nodo de origen. Ahora se desea copiar un archivo específico del volumen D:\ del nodo de origen. Se puede crear una tarea de copia de archivos para realizar esta operación.

Se puede utilizar Copia de archivo para copiar datos críticos a ubicaciones secundarias y se puede utilizar también como una solución de archivado.

Las ventajas de copiar archivos son:

- Mejorar la eficiencia: ayuda a agilizar los procesos de copia de seguridad y recuperación ya que los datos sin cambios se copian y se mueven; de esta forma se reduce la cantidad de datos reales de los cuales se hace copia de seguridad y que se almacenarán en cinta o disco.
- Cumplir las reglamentaciones: facilita la conservación de documentos, correos electrónicos y otros datos críticos importantes, puesto que son necesarios para cumplir con la normativa interna y externa.
- Reducir costes de almacenamiento: facilita la recuperación de la capacidad de almacenamiento mediante la migración de los datos más antiguos o de los datos a los que se ha accedido de manera menos frecuente desde los servidores primarios a ubicaciones de almacenamiento de archivo de archivado más rentables.
- Mantener versiones de varios archivos: facilita la reversión a versiones anteriores de archivos de los que se ha realizado copia de seguridad (si es necesario) o mantener versiones múltiples de los mismos archivos en destinos diferentes.

¿Qué hacer a continuación?

- Revisión de los requisitos previos
- Creación de un plan con una tarea de copia de seguridad
- Adición de una tarea de copia de archivo al plan
- (Opcional) Realización de una copia de archivos manual
- Verificación del plan

Revisión de las consideraciones y requisitos previos

Verifique si se han completado los requisitos previos siguientes:

- Inicie sesión en la Consola.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Consideraciones:

- En la siguiente tabla se indica el límite de longitud del nombre de archivo de una tarea de copia de archivos. Los archivos que superen dichos límites se omitirán.

Destino	Límite
Recurso compartido de red	240
Nube	245

- Si la copia del archivo se está ejecutando desde una sesión replicada y el *origen* de replicación tiene varias sesiones de copia de seguridad, la tarea de copia de archivos se ejecuta para cada sesión por separado. Por ejemplo, si hay **cinco** *sesiones de copia de seguridad* en el destino de la copia de seguridad y agrega una tarea de replicación, esta última replica todas las sesiones en *una única tarea*. Si agrega una tarea de copia de archivos y el origen de esta es el destino de replicación, **se ejecutan cinco** *tareas de copia de archivos* para replicar cada sesión.

Creación de un plan con una tarea de copia de seguridad

Un plan incluye tipos diferentes de tareas que se desea realizar. Para crear una tarea de copia de archivo, se debe tener primero un punto de recuperación válido. Para obtener un punto de recuperación válido, tiene que crear una tarea de copia de seguridad.

La tarea de copia de seguridad realiza una copia de seguridad de los nodos de origen y almacena los datos en el destino especificado. La copia de archivo solo es compatible con la copia de seguridad de Windows basada en el agente. El procedimiento siguiente explica los pasos para crear la tarea de copia de seguridad de Windows basada en el agente.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable **Tipo de tarea** seleccione **Copia de Seguridad, Windows basado en el agente**.



Ahora, especifique el origen, el destino, la programación y las opciones avanzadas.

Especificación del origen

La página Origen le permite especificar los nodos de origen que se desean proteger. Se pueden seleccionar más de un nodo del plan. Si no se ha agregado ningún nodo a la consola, se podrán agregar nodos al crear o modificar un plan en la página Origen. Se puede guardar un plan sin agregar ningún nodo de origen. El plan se implementa solamente después de agregar nodos de origen.

Siga estos pasos:

1. En la ficha Origen, haga clic en **Agregar**.
2. Seleccione una de las opciones siguientes:

   Seleccionar los nodos para proteger en Arcserve UDP

   Abre el cuadro de diálogo Seleccionar los nodos para proteger en Arcserve UDP. Seleccione los nodos de la lista que se muestra. Seleccione esta opción si ya se han agregado los nodos a la consola.

   Agregar nodo de Windows

   Se abre el cuadro de diálogo Agregar nodos a un plan. Seleccione esta opción si no se han agregado los nodos y desea agregarlos manualmente para la protección.

   Detectar nodos desde Active Directory

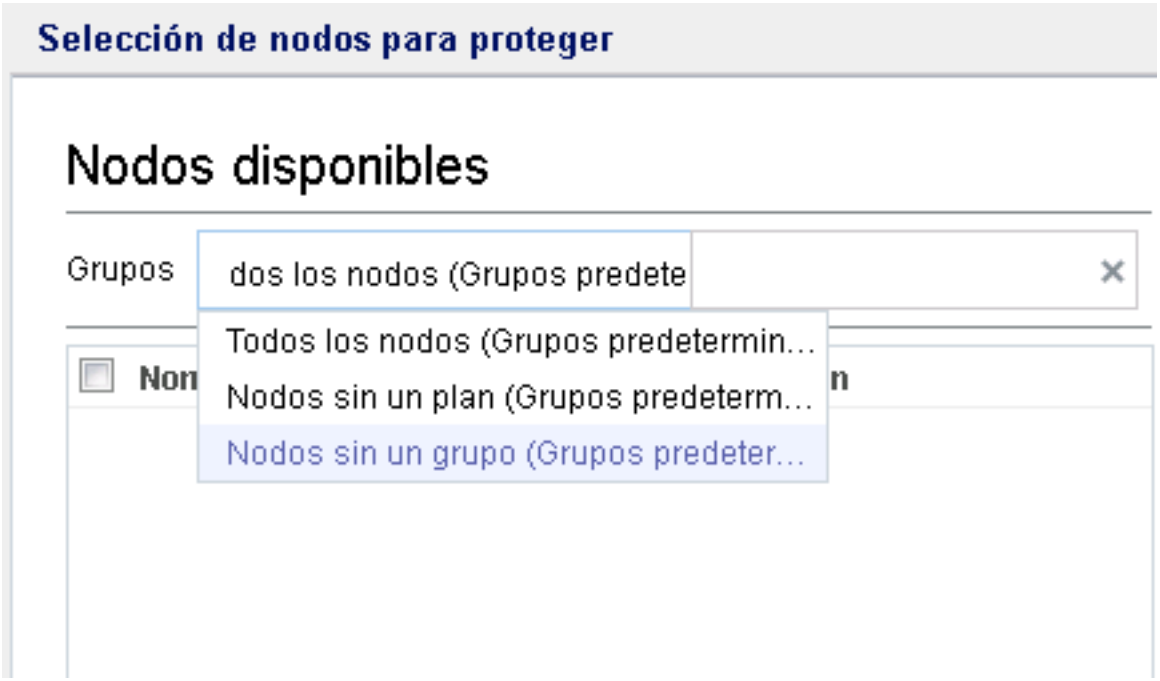
   Se abre el cuadro de diálogo Agregar nodos a la Consola de Arcserve UDP. Seleccione esta opción si desea detectar y agregar nodos en Active Directory.
3. Si ha seleccionado la opción **Seleccionar nodos para proteger en Arcserve UDP**, haga lo siguiente en el cuadro de diálogo Seleccionar nodos para proteger:
   a. (Opcional) Seleccione un filtro en la lista desplegable Grupos para filtrar nodos. Se pueden especificar palabras clave para filtrar más detalladamente los nodos.

      Los nodos se muestran en la columna Nodos disponibles.

   b. Seleccione los nodos en la columna Nodos disponibles y, a continuación, haga clic en la flecha simple hacia la derecha (>) o en la flecha doble hacia la derecha (>>) para mover los nodos seleccionados o todos los nodos respectivamente a la columna Nodos seleccionados.

      Los nodos se muestran en la columna Nodos seleccionados.

   c. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.



4. Para elegir el Tipo de El Protección, seleccione una de las opciones siguientes:

   Realizar copia de seguridad de todos los volúmenes

   Prepara una instantánea de copia de seguridad de todos los volúmenes.

   Realizar copia de seguridad de los volúmenes seleccionados

   Prepara una instantánea de copia de seguridad del volumen seleccionado.

   Se especifica el origen.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Seleccione uno de los siguientes **Tipos de destino**:

   Disco local o carpeta compartida

   Especifica que el destino de la copia de seguridad es un destino local o una carpeta compartida. Si se selecciona esta opción, se pueden guardar datos como puntos de recuperación o como conjuntos de recuperación. Las opciones Puntos de recuperación y Conjuntos de recuperación están disponibles en la ficha **Programación**.

   Servidor de puntos de recuperación de Arcserve UDP

   Especifica que el destino de la copia de seguridad es un servidor de punto de recuperación. Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.

2. Si se ha seleccionado **Servidor de punto de recuperación de Arcserve UDP**, se deben proporcionar los detalles siguientes:
   a. Seleccione un servidor de punto de recuperación.
   b. Seleccione un almacén de datos. La lista muestra todos los almacenes de datos que se han creado en el servidor de punto de recuperación especificado.
   c. Proporcione una contraseña de la sesión.
   d. Confirme la contraseña de la sesión.

3. Si ha seleccionado **Disco local o carpeta compartida**, a continuación proporcione los detalles siguientes:
   a. Proporcione la ruta completa del destino local o de red. Para el destino de la red, especifique las credenciales con acceso de escritura.
   b. Seleccione el algoritmo de cifrado. Para obtener más información, consulte Configuración de cifrado.
   c. Opcionalmente, proporcione una contraseña de cifrado.
   d. Confirme la contraseña de cifrado.

e. Seleccione un tipo de compresión. Para obtener más información, consulte Tipo de compresión.

Nota: Si se almacenan los datos a un disco local o a una carpeta compartida, no se pueden replicar los datos a otro servidor de punto de recuperación. Se es compatible con la replicación solamente si se almacenan los datos en un servidor de punto de recuperación.

Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y se pueden proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

Siga estos pasos:

1. (Opcional) Seleccione la opción para gestionar puntos de recuperación. Esta opción solo está visible si se ha seleccionado la carpeta local o compartida como destino de la copia de seguridad.

   Retener por puntos de recuperación

   Los datos de la copia de seguridad se almacenan como puntos de recuperación.

   Retener por conjuntos de recuperación

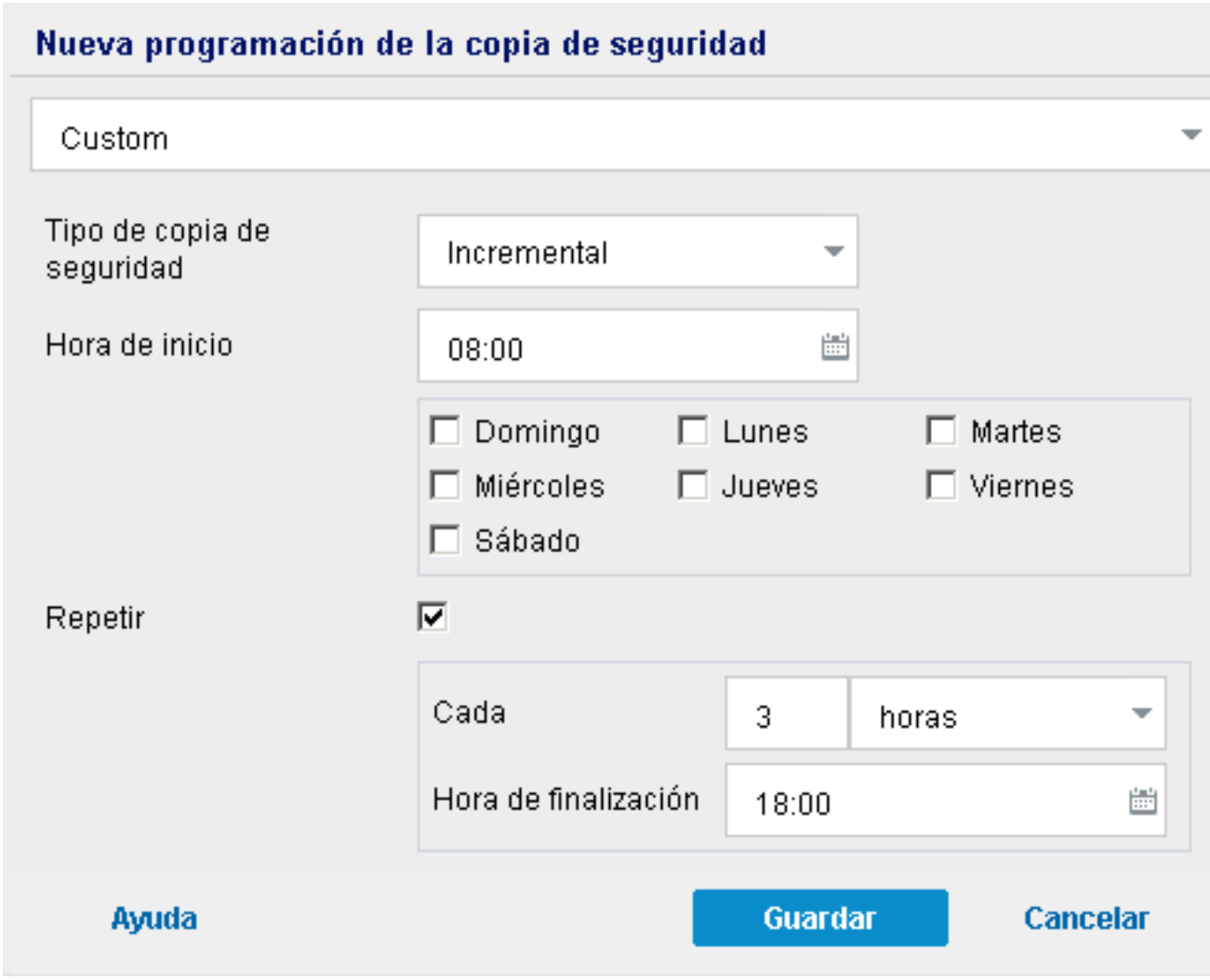
   Los datos de la copia de seguridad se almacenan como conjuntos de recuperación.

2. Agregue las programaciones de la copia de seguridad, de la combinación y del regulador.

   Agregar programación de la copia de seguridad

   a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

      Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Verificar

Especifica la programación de la copia de seguridad para las copias de seguridad de verificación.

Arcserve UDP verifica que los datos protegidos sean válidos y estén completos mediante una comprobación de confianza de la imagen de copia de seguridad almacenada en el origen de la copia de seguridad. Si es necesario, volverá a sincronizar la imagen. Una copia de seguridad de verificación se fijará en la copia de seguridad más reciente de cada bloque individual y comparará el contenido y la información con la de origen. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad de un bloque no coincide con la del origen (posiblemente por cambios en el sistema desde la última copia de seguridad), Arcserve UDP actualiza (resincroniza) la copia de seguridad del bloque que no coincide. Se puede utilizar también una copia de seguridad de verificación (aunque poco frecuentemente) para obtener la garantía de copia de seguridad completa sin utilizar el espacio necesario para una copia de seguridad completa.

Ventajas: produce una pequeña imagen de copia de seguridad si se compara con la copia de seguridad completa porque solamente se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventajas: el tiempo durante el cual se realiza la copia de seguridad es considerable puesto que todos los bloques de origen se comparan con los bloques de la última copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

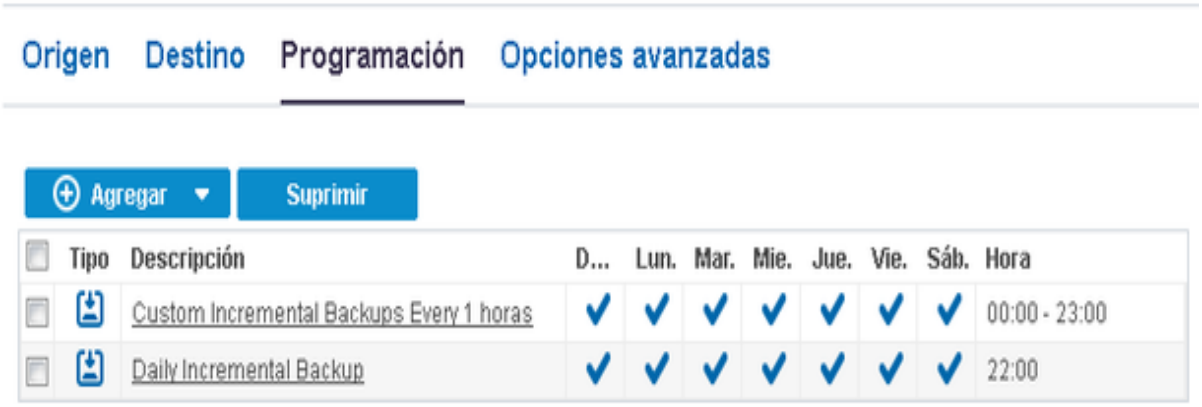
Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en Agregar y seleccione Agregar programación de la combinación.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

b. Especifique la hora de inicio para iniciar la tarea de combinación.

c. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

d. Haga clic en **Guardar**.

La Programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

   Se abre el cuadro de diálogo Agregar nueva programación del limitador.

b. Especifique el límite de rendimiento en MB por minuto.

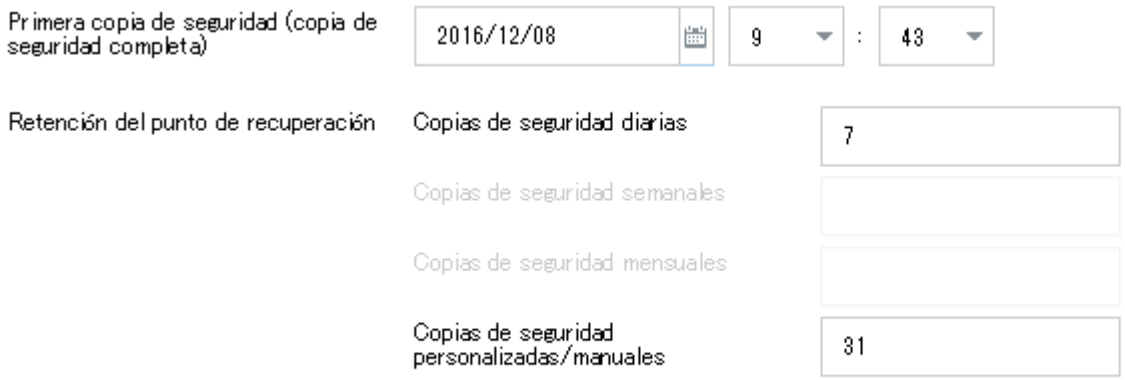
c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

   La programación del limitador se especifica y se muestra en la página **Programación**.

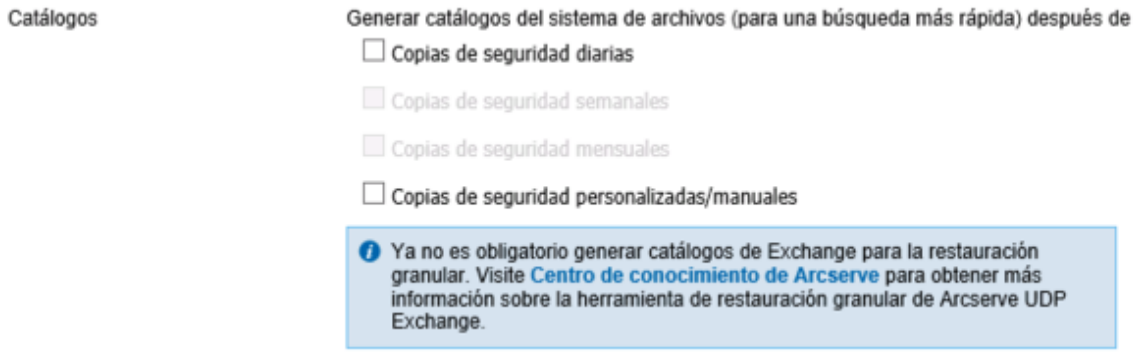
3. Especifique la hora de inicio para la copia de seguridad programada.



4. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

   Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo Programación de la copia de seguridad.

5. Especifique los detalles del catálogo.



Los catálogos permiten generar el catálogo del sistema de archivos. El catálogo del sistema de archivos se requiere para realizar la mejor búsqueda de la forma más rápida. Si se seleccionan las casillas de verificación del catálogo, los catálogos se activan en función del tipo de copia de seguridad especificada. Desactive la casilla de verificación para desactivar la generación del catálogo.

Se especifica la programación.

Funcionamiento de la programación avanzada y de la retención

La opción de programación le permite especificar una programación personalizada, una programación diaria/semanal/mensual o ambas. En la programación personalizada, se puede configurar la programación de la copia de seguridad durante cada día de la semana y se pueden agregar hasta cuatro programaciones de copia de seguridad cada día. Se puede seleccionar un día específico de una semana y crear un período de tiempo para definir cuando se desea ejecutar la copia de seguridad y con qué frecuencia.

Programación	Tarea compatible	Comentarios
Copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para ejecutar las tareas de copia de seguridad.
Regulación de la copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para controlar la velocidad de la copia de seguridad.
Combinar	Tarea de combinación	Defina cuando se deben ejecutar las tareas de combinación.
Programación diaria	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad diarias.
Programación semanal	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad semanales.
Programación mensual	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad mensuales.

Se pueden especificar también los valores de configuración de retención para los puntos de recuperación.

Nota: Establezca la configuración de la retención en cada plan para controlar cómo se retienen los datos para los nodos asignados a ese plan en el almacén de datos de destino.

Las programaciones para las copias de seguridad diarias/semanales/mensuales son independientes de la programación personalizada y de las unas a las otras. Se puede configurar solamente ejecutar una copia de seguridad diaria, una copia de seguridad semanal o una copia de seguridad mensual sin configurar la programación personalizada.

Programación de la tarea de copia de seguridad

Se pueden agregar cuatro períodos de tiempo por día en la programación de la copia de seguridad. Un período de tiempo válido es desde las 12:00 horas hasta las 23:59 horas. No se puede especificar un período de tiempo como, por

ejemplo, de las 18:00 horas a las 06:00 horas. En tales casos, se debe especificar manualmente dos períodos de tiempo diferentes.

Para cada período de tiempo, la hora de inicio está incluida y, en cambio, no se incluye la hora de finalización. Por ejemplo, se ha configurado ejecutar una copia de seguridad incremental ejecutada todas las horas entre las 06:00 horas y las 09:00 horas y la copia de seguridad se iniciará a las 06:00 horas. Esto significa que la copia de seguridad se ejecuta a las 06:00 horas, a las 07:00 horas y a las 08:00 horas, pero NO a las 09:00 horas.

Nota: Si desea ejecutar la tarea de copia de seguridad reiteradamente hasta el final del día, configure la programación hasta las 12:00 horas. Por ejemplo, para ejecutar la tarea de copia de seguridad cada 15 minutos durante todo el día, configure la programación de las 12:00 a las 12:00, cada 15 minutos.

Programación del regulador de la copia de seguridad

La programación del regulador de la copia de seguridad le permite controlar la velocidad del rendimiento de la copia de seguridad, que a su vez controla el uso de recursos (E/S del disco, CPU, ancho de banda de la red) del servidor del que se está realizando la copia de seguridad. Esto es útil si no se desea afectar al rendimiento del servidor durante el horario comercial. Se pueden agregar cuatro períodos de tiempo por día en la programación del regulador de la copia de seguridad. Para cada período de tiempo, se puede especificar un valor en MB por minuto. Este valor se utiliza para controlar el rendimiento de la copia de seguridad. Los valores válidos van desde 1 MB/minuto a 99999 MB/minuto.

Si una tarea de copia de seguridad excede el tiempo especificado, el límite del regulador se ajusta según el período de tiempo especificado. Por ejemplo, se ha definido el límite del regulador de la copia de seguridad en 500 MB/minuto desde las 08:00 horas a las 20:00 horas y en 2500 MB/minuto de las 20:00 horas a las 22:00 horas. Si una tarea de copia de seguridad se inicia a las 19:00 horas y se ejecuta durante tres horas, el límite del regulador es de 500 MB/minuto de las 19:00 horas a las 20:00 horas y de 2500 MB/minuto de las 20:00 horas a las 22:00 horas.

Si no se define ninguna programación de la copia de seguridad ni ninguna programación del rendimiento de la copia de seguridad, la copia de seguridad se ejecuta tan deprisa como pueda.

Programación de la combinación

Le permite combinar puntos de recuperación basándose en la programación proporcionada.

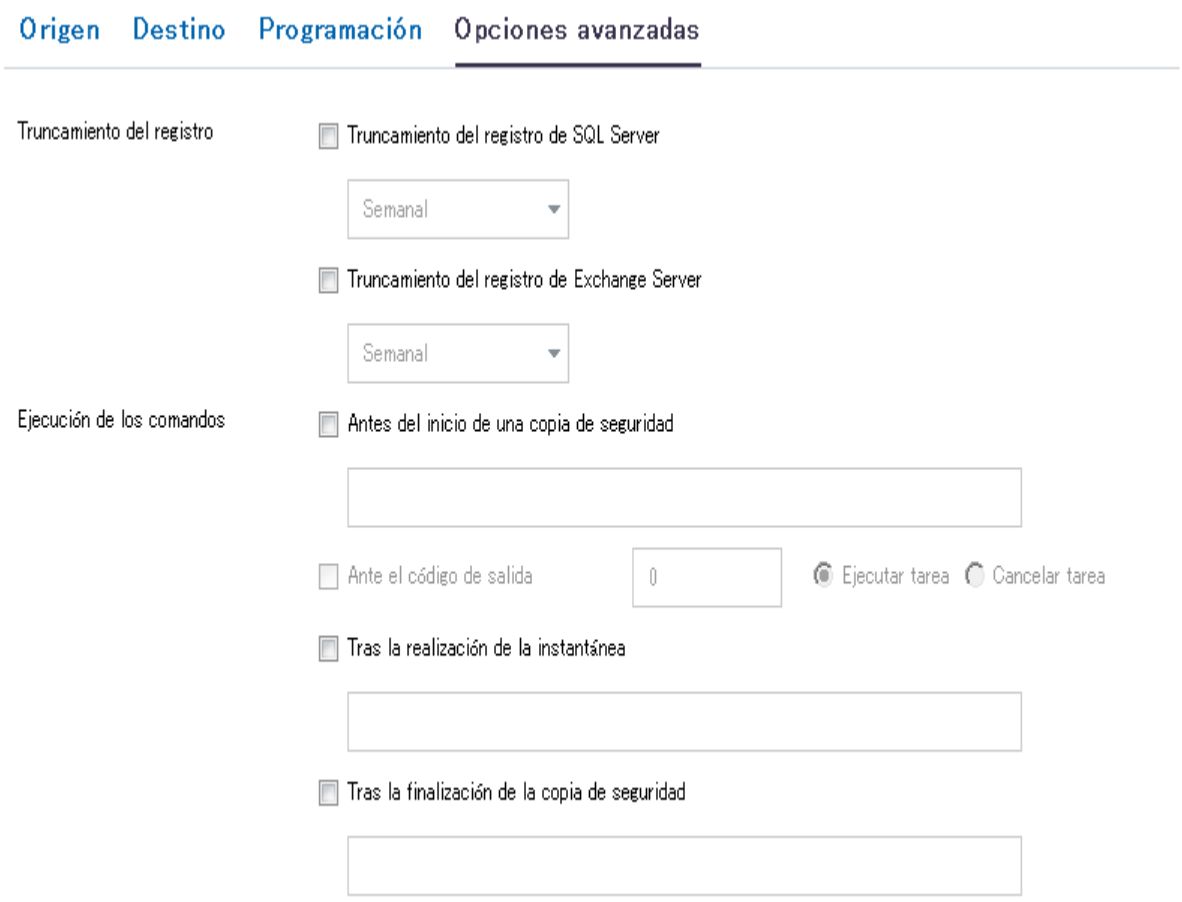
Tenga en cuenta los puntos siguientes para la tarea de combinación:

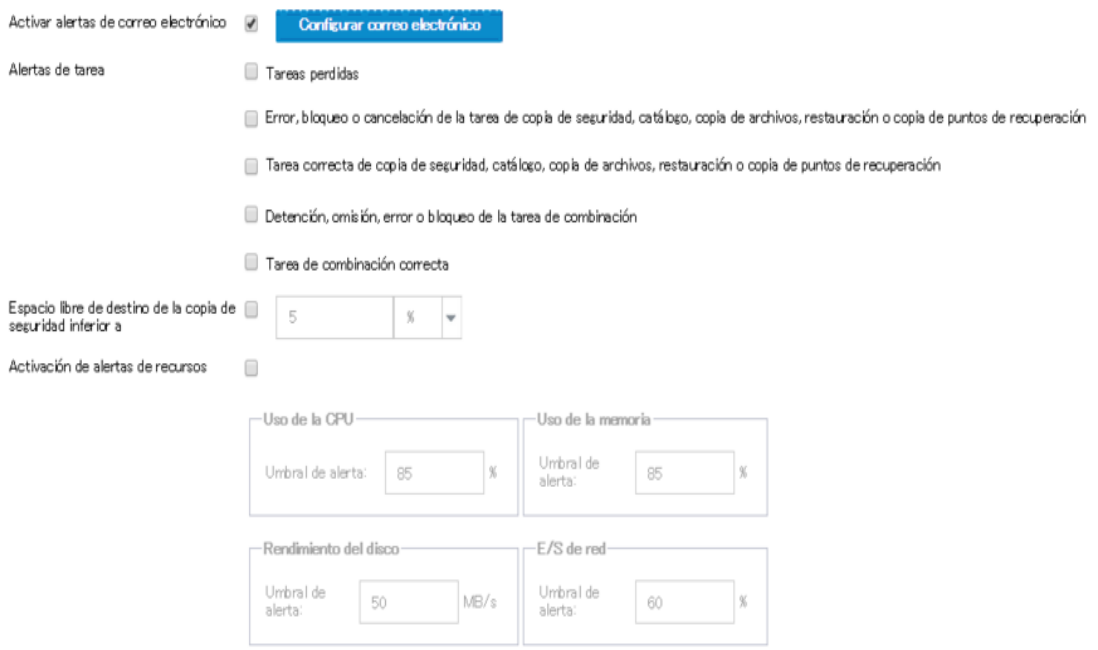
- Solamente una tarea de combinación puede ejecutarse para un nodo en cualquier momento proporcionado.
- Si se inicia una tarea de combinación, se tiene que completar antes de que la siguiente tarea de combinación se pueda iniciar. Esto no significa que, si uno o más conjuntos de puntos de recuperación se combinan, no se pueda agregar un punto de recuperación nuevo a este proceso de combinación hasta que el proceso de combinación del conjunto actual de puntos de recuperación se complete.
- Si una tarea de combinación está procesando más de un conjunto de puntos de recuperación (por ejemplo, el conjunto [1~4], el conjunto [5~11] y el conjunto [12~14] son tres conjuntos), el servidor de puntos de recuperación procesará estos conjuntos uno a uno.
- Si una tarea de combinación se reanuda después de una pausa, la tarea detecta en qué punto se ha pausado y reanuda la combinación a partir del punto de pausa.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye la configuración de registros de truncamiento, proporcionar la ubicación de los scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha Avanzada:





Siga estos pasos:

1. Especifique los siguientes detalles:

Cómo truncar un registro

Le permite especificar la programación para truncar los registros de SQL Server y Exchange Server. Se puede especificar la programación como **Diaria**, **Semanal** o **Mensual**.

Nombre de usuario

Le permite especificar el usuario que se autoriza para ejecutar un script.

Contraseña

Le permite especificar la contraseña del usuario autorizado para ejecutar el script.

Ejecutar un comando antes de empezar una copia de seguridad

Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde el script está almacenado. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de seguridad continuará cuando el script devuelva el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detendrá cuando el script devuelva el código de salida.

Ejecutar un comando después de realizar una instantánea

Le permite ejecutar un script después de realizar la instantánea de la copia de seguridad. Especifique la ruta donde el script está almacenado.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta donde el script está almacenado.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y se pueden especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de tareas que se desea recibir.

Cómo activar las alertas de recurso

Le permite especificar un umbral para el Uso de CPU, Uso de memoria, Rendimiento del disco y E/S de la red. Se puede proporcionar el valor en porcentaje. Se recibirá un correo electrónico cuando se exceda el valor de Umbral de alerta.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en Guardar.

Los cambios se guardan y se muestra una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **Recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar.

El plan de copia de seguridad se crea y se implementa automáticamente en el nodo de origen. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

Adición de una tarea de copia de archivo al plan

La tarea de copia de archivo le permite copiar archivos individuales al destino especificado. La copia original se conserva después de copiar los archivos en el destino especificado. La copia de archivos no depende de las tareas de catálogo. Si el destino de la copia de seguridad es un almacén de datos de deduplicación o de no deduplicación, la carpeta del catálogo se mueve a dicho destino. La tarea de catálogo forma parte de la tarea de copia de archivos. La tarea de copia de archivos se ejecuta en el servidor de puntos de recuperación y, al hacerlo, Arcserve UDP descarga la tarea de los agentes.

Arcserve UDP admite la copia de archivos desde un almacén de datos de replicación. ;

Comprobación previa para los nodos de copia de archivos: También es posible efectuar una comprobación previa de la copia de archivos. Solo los nodos que se agreguen para la copia de archivos son aptos para la comprobación previa. Para realizar una comprobación previa de la copia de archivos, haga clic con el botón secundario del ratón en el nodo desde Todos los nodos y seleccione Comprobación previa de copia de archivos.

Nota: Si una tarea de copia de seguridad está en curso y se pausa el plan, la tarea de copia de seguridad se detendrá y la tarea de copia de archivo no se iniciará. Cuando se vuelva a reanudar el plan, la tarea de copia de archivo no se reanuda automáticamente. Se tiene que ejecutar manualmente otra tarea de copia de seguridad para iniciar la tarea de copia de archivo.

Siga estos pasos:

1. Haga clic en **Agregar una tarea** en el panel izquierdo.

   Una tarea nueva se agrega al panel izquierdo.

2. En el menú desplegable **Tipo de tarea**, seleccione **Copia de archivo**.

   Se agrega la tarea de copia de archivo.

3. Haga clic en la ficha **Origen** e introduzca los detalles.

   Origen de puntos de recuperación para la copia de archivos

   Permite seleccionar el origen de los puntos de recuperación. Si solo hay un origen, este se muestra automáticamente. Si hay más de un origen, se tendrá que seleccionar el pertinente en la lista desplegable.

   Tipos de puntos de recuperación

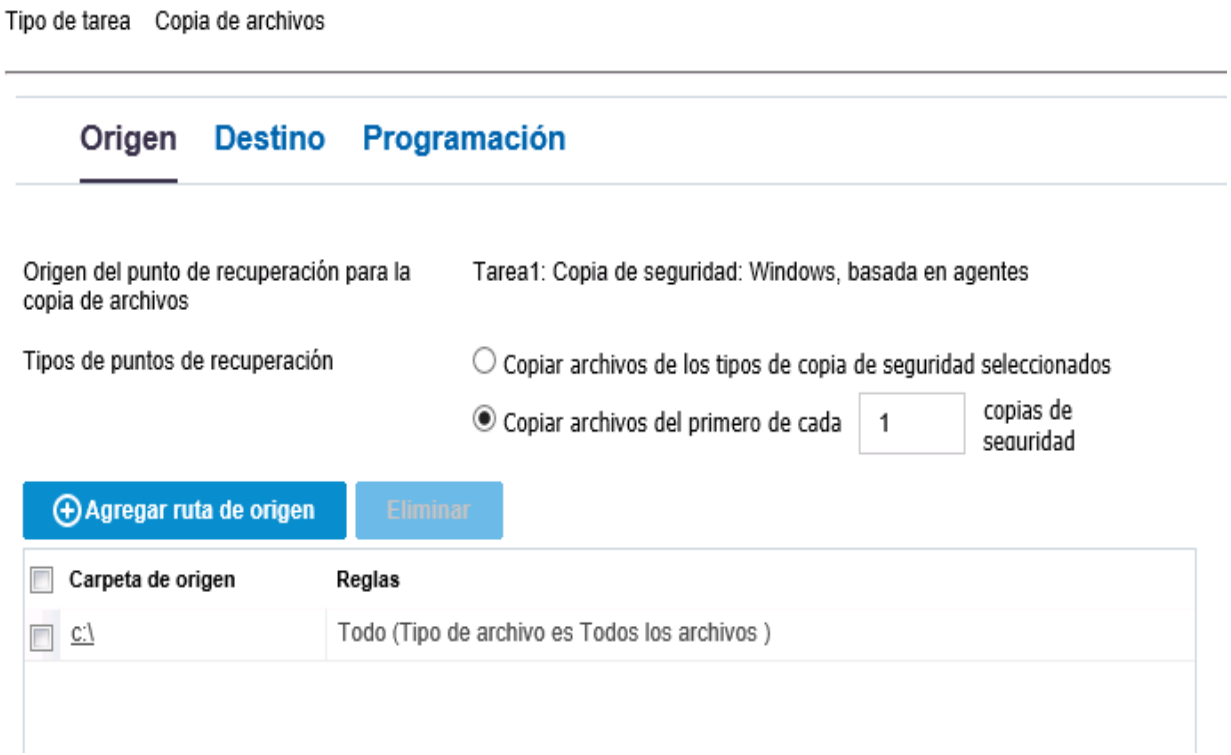
   Permite seleccionar los puntos de recuperación para la copia de archivos. Puede seleccionar una de las dos siguientes opciones:

Copy files from selected backup types(s) (Copiar archivos de los tipos de copia de seguridad seleccionados)

Se puede seleccionar **Copias de seguridad diarias**, **Copias de seguridad semanales** o **Copias de seguridad mensuales**. Las opciones diarias, semanales o mensuales están disponibles en función de la programación de la copia de seguridad de origen. Por ejemplo, si la copia de seguridad de origen solo tiene programadas copias de seguridad mensuales, la opción **Copy files from selected backup types(s)** (Copiar archivos de los tipos de copia de seguridad seleccionados) solo presentará **Copias de seguridad mensuales**.

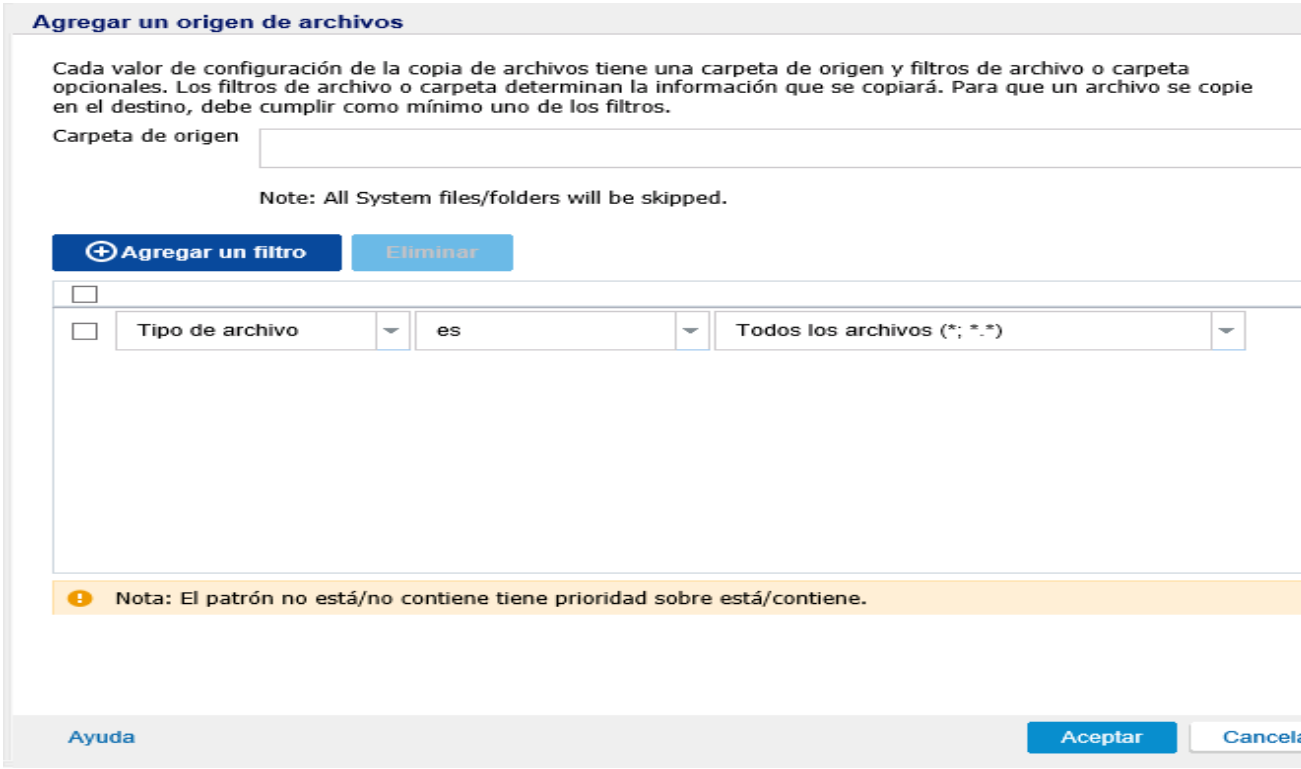
Copy file from the first of every backup(s) (Copiar archivos de la primera de todas las copias de seguridad)

Es posible especificar el número de la copia de seguridad que desea copiar. Por ejemplo, si especifica 3, se copiará la tercera copia de seguridad. La copia de archivos admite hasta 700 puntos de recuperación desde los que copiar.



4. Haga clic en **Agregar ruta de origen**.

   Se abre el cuadro de diálogo **Agregar un origen de archivos**.



Se puede evitar la omisión de los directorios del sistema de Windows (C:\Windows) y de los archivos de programa (C:\Archivos de programa, C:\Archivos de programa (x86)) mediante la configuración siguiente:

Agregue la siguiente etiqueta XML (si no aparece) o actualícela en el archivo FileCopyDebugSetting.xml incluido en la carpeta $UDPHome\Engine\Configuration:

<SkipWindowsFolders>0</SkipWindowsFolders>

El archivo XML aparece como se muestra a continuación:

<?xml version="1.0" encoding="UTF-8"?>

<HKLM>

<AFArchiveDLL>

.....

<SkipWindowsFolders>0</SkipWindowsFolders>

</AFArchiveDLL>

</HKLM>

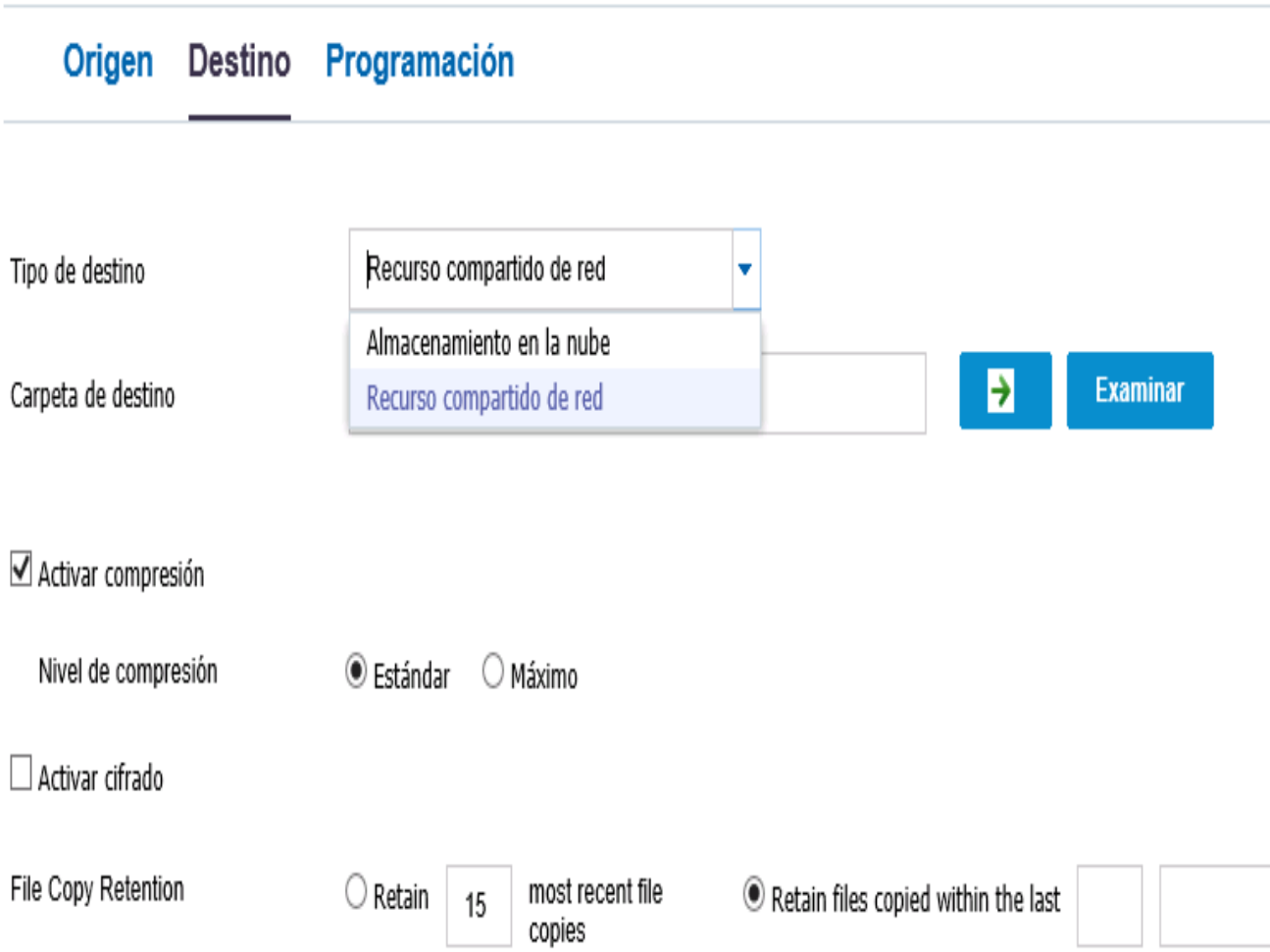
5. Especifique la ruta de la carpeta de origen que desee copiar.
6. Haga clic en **Agregar un filtro**.

El filtro se agrega debajo del botón **Agregar un filtro.** Es posible agregar varios filtros y también eliminarlos. Para obtener más información, consulte Adición de filtros de copia de archivos.

7. Seleccione el filtro en la lista y haga clic en **Aceptar**.

   Se cerrará el cuadro de diálogo **Agregar un origen de archivos**.

8. Haga clic en la ficha **Destino** y especifique los detalles del destino.



Tipo de destino

Especifica si el tipo de destino es un recurso compartido de red o un almacenamiento en la nube. Independientemente de la opción de destino seleccionada, si la conexión al destino especificado se pierde o se interrumpe, Arcserve UDP realiza varios intentos para continuar con la tarea de copia de archivos. Si estos reintentos no son correctos, se realizará una tarea de nueva copia de seguridad a partir del punto en que se produjo el error. Además, el registro de actividades se actualizará con un mensaje de error correspondiente y se enviará una notificación de correo electrónico (si se configura).

Recurso compartido de red

Especifica que el destino es una carpeta compartida. Cuando se selecciona, permite especificar la ruta completa de la ubicación en la que desee desplazar o copiar los archivos/carpetas de origen.

Carpeta de destino

Especifica el destino donde se almacenan los archivos copiados. El destino puede ser cualquier volumen local o carpeta o un recurso compartido de archivo a los cuales puede acceder cualquier ruta de convención de denominación uniforme (UNC). Este campo está disponible cuando se selecciona Recurso compartido de red como tipo de destino. También se puede explorar la carpeta de destino.

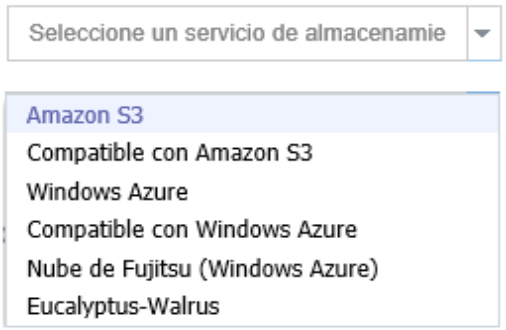
Almacenamiento en la nube

Especifica que los archivos copiados se almacenan en un entorno de nube. Arcserve UDP admite actualmente la copia de archivos a varios distribuidores de la nube como, por ejemplo, Amazon S3 (Simple Storage Service), compatible con Amazon S3, Windows Azure, compatible con Windows Azure, Eucalyptus-Walrus y FUJITSU Hybrid IT Service FJcloud-O. Estos distribuidores de la nube son servicios web disponibles públicamente que permiten almacenar y recuperar cualquier cantidad de datos, en cualquier momento y desde cualquier sitio de la Web en un entorno seguro

Nota: Para eliminar cualquier error potencial de sesgo de reloj al intentar conectarse a la nube, compruebe que el equipo tiene establecida la zona horaria correcta y que el reloj esté en sincronización con la hora global. Es recomendable comprobar siempre la hora del equipo con la hora GMT. Si la hora del equipo no se sincroniza con la hora de reloj global correcta (entre 5 y 10 minutos), puede que la conexión de la nube no funcione. Si es necesario, restablezca la hora correcta del equipo y vuelva a ejecutar la tarea de copia.

Dispositivo de almacenamiento

Seleccione el tipo de dispositivo en la lista desplegable.



Almacenamiento en la nube

Seleccione la ruta de almacenamiento en la nube en la lista desplegable. La lista desplegable está disponible si ha especificado los detalles de almacenamiento en la nube. Si se especifica la cuenta de almacenamiento en la nube por primera vez, haga clic en Agregar para agregar la cuenta de la nube. A partir de la siguiente vez que se selecciona Almacenamiento en la nube, la cuenta aparecerá en la lista desplegable de Almacenamiento en la nube.

Nota: Para obtener más información sobre cómo agregar una cuenta de la nube, consulte Agregar una cuenta de la nube.

Compresión

Especifica el tipo de compresión que debe utilizarse para las tareas de copia de archivo.

La compresión se realiza para reducir el espacio de almacenamiento en el destino Copia de archivo, pero también tiene un impacto inverso en la velocidad de copia de archivo a causa del uso en aumento de la CPU.

Nota: Para una tarea de copia de archivo comprimida, el registro de actividades mostrará solamente el tamaño no comprimido.

A continuación se especifican las opciones disponibles:

Compresión estándar

Se realiza algún tipo de compresión. Esta opción proporciona un buen equilibrio entre el uso de la CPU y el requisito de espacio de almacenamiento. Se trata de la configuración predeterminada.

Compresión máxima

Se realiza la compresión máxima. Esta opción proporciona el uso de la CPU más elevado (velocidad más baja) pero también dispone del requisito de espacio de almacenamiento más bajo para la copia de archivo.

Activación del cifrado

Especifica el uso del cifrado para la copia de archivo.

El cifrado de datos es la traducción de los datos a una forma que resulte ininteligible sin un mecanismo de descifrado. La protección de datos de Arcserve UDP utiliza algoritmos de cifrado seguros AES-256 (Estándar de cifrado avanzado) para obtener la máxima seguridad y privacidad de los datos especificados. Cuando se selecciona un cifrado, se debe proporcionar (y confirmar) una contraseña de cifrado.

Nota: Al modificar una tarea de copia de archivos, no es posible cambiar la configuración de cifrado ni compresión.

Retención de archivos

Conserva los archivos en el destino de copia de archivo si se cumplen los criterios especificados.

Archivo creado en los últimos

Especifica la cantidad de tiempo (años, meses, días) durante el cual se conservan los datos almacenados en la ubicación de destino. Al final del período de tiempo de retención especificado, se borrarán definitivamente los datos almacenados del destino.

Importante: Al final del tiempo de retención especificado, cuando los datos se borran definitivamente desde el destino, todos estos datos borrados definitivamente ya no se almacenan ni se guardan.

Nota: El proceso de borrado definitivo del tiempo de retención se activa sólo cuando se activa la opción Programación de copia de archivo.

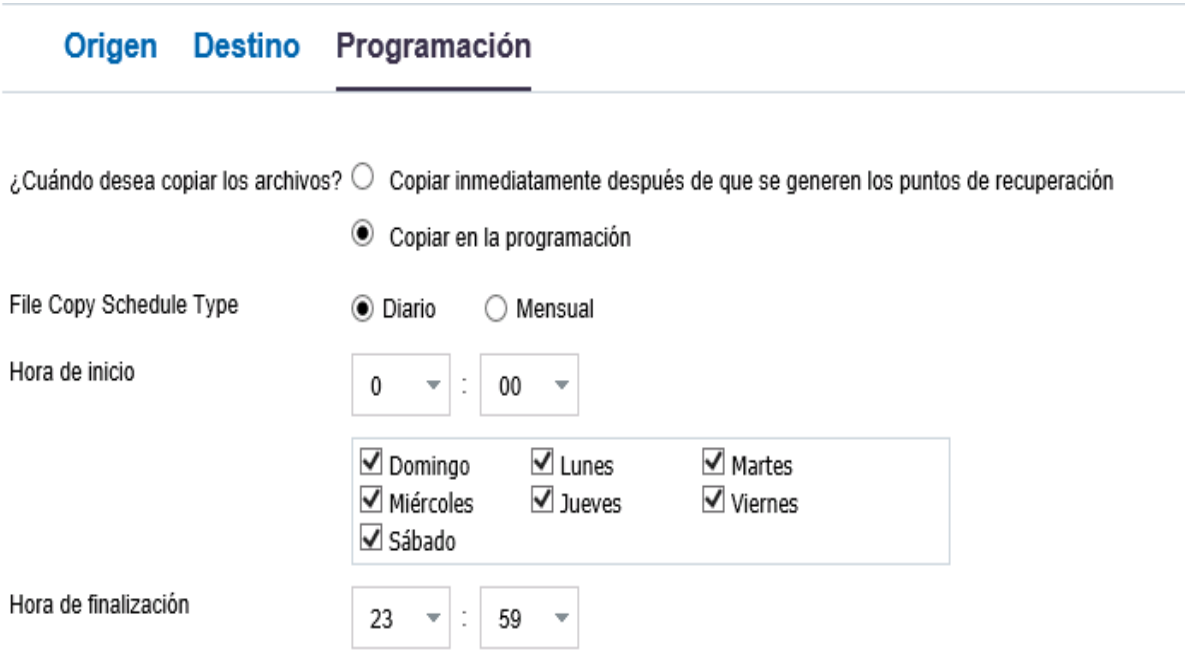
Versión del archivo menor de

Especifica el número de copias conservadas y almacenadas en la ubicación de destino. Si se excede este número, la primera versión (la más antigua) se eliminará. Este ciclo de eliminación de la versión almacenada más antigua se repetirá a medida que se agreguen versiones más nuevas al destino, de modo que permite mantener siempre el número especificado de versiones almacenadas.

Por ejemplo, si el recuento de retenciones de versiones de archivo especificado se establece en 5 y se realizan cinco copias de archivo a las t1, t2, t3, t4, y t5, se convierten en las cinco versiones de copia de archivo conservadas y disponibles para la recuperación. Después de realizar la sexta copia de archivos (la nueva versión se guarda), Arcserve UDP elimina la copia t1. Las cinco versiones disponibles que restan para la recuperación son ahora t2, t3, t4, t5 y t6.

De forma predeterminada, el número de copias conservadas en la ubicación de destino antes de la eliminación es 15.

9. Haga clic en la ficha **Programación** para especificar la programación de la copia de archivo.



Si se ejecuta una tarea de copia de archivo más allá de la hora de finalización, la tarea seguirá ejecutándose hasta que se complete. La siguiente tarea de copia de archivo no se ejecutará hasta que se complete la tarea de copia de archivo anterior, incluso si una tarea programada se superpone a la tarea en ejecución.

La tarea de copia de archivo se ejecuta como se indica en la programación.

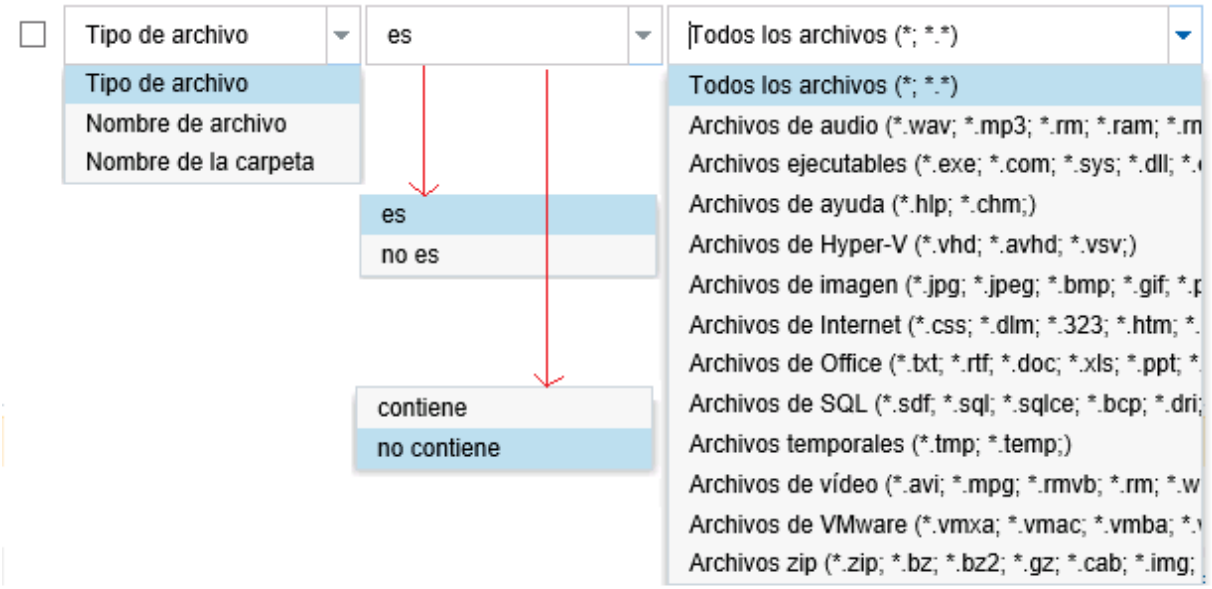
10. Haga clic en **Guardar**.

    Los cambios se guardan y la tarea de copia de archivo se implementa automáticamente en el nodo.

Adición de filtros de copia de archivos

Agregar un filtro

Permite agregar un filtro. Los filtros permiten limitar los objetos de los cuales ciertos tipos y valores especificados realizarán copia de archivo.



Categoría de filtros

Existen tres categorías de filtros disponibles: **Tipo de archivo**, **Nombre de archivo** y **Nombre de la carpeta**. Los campos Variable de filtro y Valor de filtro cambian en función de la categoría de filtro.

Variable de filtro

Si la categoría de filtro es **Tipo de archivo**, las opciones de Variable de filtro son **es** y **no es**. Si la categoría de filtro es **Nombre de archivo o Nombre de la carpeta**, las opciones de Variable de filtro son **contiene** o **no contiene**.

Se pueden especificar varios filtros dentro de la misma solicitud de copia de archivos. Puede especificar la misma categoría filtro, pero distintas variables de filtro.

Nota: Cuando las variables de filtro entran en conflicto dentro de la misma categoría de filtro, las variables **no** o **no contiene** siempre tienen más prioridad y se aplican.

Valor de filtro

El valor de filtro permite limitar la información de la cual se realiza copia de archivo seleccionando solamente la información del parámetro que se especifique, como los archivos .txt.

Arcserve UDP admite el uso de caracteres comodín para poder seleccionar a la vez varios objetos para copiar sus archivos en una única solicitud. Un carácter comodín es un carácter especial que se puede utilizar como sustituto para representar bien un carácter solo o una cadena de texto.

El asterisco y el signo de interrogación de los caracteres comodines se admiten en el campo Valor. Si no sabe el valor de patrón de la carpeta/archivo completo, se pueden simplificar los resultados del filtro. Para ello, especifique un carácter comodín.

"*": utilice el asterisco para sustituir cero o más caracteres en el valor.

"?" "?": utilice el signo de interrogación para sustituir un único carácter en el valor.

Por ejemplo, se puede introducir *.txt para excluir todos los archivos con una extensión de .txt si no se sabe el nombre específico del archivo. Se puede proporcionar la cantidad del nombre de archivo que sepa. A continuación, utilice caracteres comodines para rellenar los espacios en blanco.

Nota: Si se selecciona **Tipo de archivo** como el tipo de filtro, hay disponible una lista desplegable de filtros predeterminados para muchos archivos utilizados comúnmente (archivos de Microsoft Office, archivos de imagen, archivos ejecutables, archivos temporales, etc.). Después de elegir cualquiera de los filtros predeterminados, se pueden añadir o modificar todavía los valores correspondientes.

Protección de las carpetas del sistema contra la omisión

La tarea de copia de archivos omite las carpetas del sistema de forma predeterminada cuando se realiza la tarea en los volúmenes que contienen carpetas del sistema. Para proteger esas carpetas y copiarlas en el destino, se puede cambiar el texto predeterminado agregando una entrada de configuración.

Agregue la siguiente entrada de la etiqueta XML en el archivo FileCopyDebugSetting.xml que se encuentra en el directorio $UDPHome\Engine\Configuration:

Nombre de archivo: FileCopyDebugSetting.xml

Nombre de etiqueta: SkipWindowsFolders

Valor predeterminado: 1

Para proteger cambie el valor a: 0

Nota: Esta opción está limitada a la tarea de copia de archivos solamente. El archivado de archivos omite todas las carpetas del sistema sin tener en cuenta el valor de la etiqueta configurado.

(Opcional) Realización de una copia de archivos manual

Normalmente, las copias de archivos se realizan de forma automática y están controladas por la configuración de programación de copias de archivos. Además de la copia de archivos programada, una copia de archivos manual ofrece la posibilidad de copiar los archivos importantes según resulte necesario.

Cuando se ejecuta una copia de archivos manual, la tarea de copia de archivos se ejecuta solo para la primera sesión de copia de seguridad, apta para una copia de archivos. (Las sesiones de copias de seguridad son aptas para la copia de archivos según la programación de copias de seguridad y si las sesiones están en una cola. Por ejemplo, si se especifica la ejecución de una copia de archivos por cada segunda copia de seguridad, todas las segundas copias de seguridad son aptas para la copia de archivos, pero no así todas las copias de seguridad). Una vez finalizada la copia de archivos, se elimina la primera sesión y la segunda sesión en línea se convierte en la primera. Por ejemplo, si hay tres sesiones de copia de seguridad (S1, S2, S3 respectivamente) y se ejecuta una copia de archivos manual, a continuación, se ejecuta la tarea de copia de archivos solo para S1. No se ejecutará la tarea de copia de archivos para S2 y S3. Cuando se vuelve a ejecutar la tarea de copia de archivos manual, se copia S2.

La copia de archivos se puede ejecutar manualmente desde las vistas Nodos y Planes haciendo clic en el menú contextual o el menú **Acciones**.

Se deben seguir estos pasos para ejecutar la copia de archivos manualmente desde la vista de Nodos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Se muestran los nodos en el panel central.
3. Seleccione los nodos para una tarea de copia de archivos. Los nodos deben tener un plan de copia de archivos asignado.
4. En el panel central, haga clic en **Acciones**, **Copia de archivos ahora**.

   Aparecerá el cuadro de diálogo **Run File copy now (Ejecutar una copia de archivos ahora)**.
5. Haga clic en **Aceptar**.

   Se ejecutará la tarea de copia de archivos.

   La copia de archivos manual se realizará correctamente.

Verificación del plan

Para verificar el plan de la copia de archivo, confirme que se ha creado correctamente el plan. Después de verificar que el plan se ha creado correctamente, compruebe si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Después de que la tarea de copia de seguridad se complete correctamente, se ejecutará la tarea de copia de archivos tal y como estaba programada. Se puede comprobar el estado de la tarea de copia de seguridad y de la tarea de copia de archivo en la ficha **tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga estos pasos para verificar las tareas de copia de archivo:

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas finalizadas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad y la tarea de copia de archivo se han realizado correctamente.

Cómo crear un plan de archivado de archivos

Mediante Arcserve Unified Data Protection, se podrán archivar archivos de origen seleccionados en un destino. El destino puede ser una cuenta en la nube o una red compartida. El archivo de origen debe ser del mismo volumen del que se ha realizado la copia de seguridad. Por ejemplo, se ha realizado la copia de seguridad de todo el volumen D:\ del nodo de origen. A continuación, se desea copiar un tipo específico de archivo (por ejemplo, .htm) del volumen D del nodo de origen. Después de copiar el archivo, se desea suprimir ese archivo del nodo de origen. Se puede crear un plan de archivado de archivos para realizar esta operación.

El archivado de archivos permite suprimir de forma segura los datos de origen una vez que estos se hayan copiado en un repositorio de almacenamiento secundario o sin conexión.

Las ventajas de archivar archivos son:

- Mejorar la eficiencia: ayuda a agilizar los procesos de copia de seguridad y recuperación, ya que los datos sin cambios se archivan; de esta forma, se reduce la cantidad de datos reales de los cuales se hace copia de seguridad y que se almacenarán en cinta o disco.
- Cumplir las reglamentaciones: facilita la conservación de documentos, correos electrónicos y otros datos críticos importantes, puesto que son necesarios para cumplir con la normativa interna y externa.
- Reducir costes de almacenamiento: facilita la recuperación de la capacidad de almacenamiento mediante la migración de los datos más antiguos o de los datos a los que se ha accedido de manera menos frecuente desde los servidores primarios a ubicaciones de almacenamiento de archivo de archivado más rentables.
- Mantener versiones de varios archivos: facilita la reversión a versiones anteriores de archivos de los que se ha realizado copia de seguridad (si es necesario) o mantener versiones múltiples de los mismos archivos en destinos diferentes.

¿Qué hacer a continuación?

Revisión de las consideraciones y requisitos previos

Verifique si se han completado los requisitos previos siguientes:

- Inicie sesión en la Consola.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Tenga en cuenta las consideraciones siguientes:

- La tarea de archivado de archivos se ejecuta desde la última sesión copia de seguridad disponible.
- La tarea de archivado de archivos solo se ejecuta una vez al día según la programación.
- La tarea de eliminación del archivado de archivos se ejecuta como una nueva tarea para suprimir los archivos de origen.
- En la siguiente tabla se indica el límite de longitud del nombre de archivo de una tarea de archivado de archivos. Los archivos que superen dichos límites se omitirán.

Destino	Límite
Recurso compartido de red	240
Nube	245

Creación de un plan con una tarea de copia de seguridad

Un plan incluye tipos diferentes de tareas que se desea realizar. Para crear una tarea de archivado de archivos, se debe tener primero un punto de recuperación válido. Para obtener un punto de recuperación válido, tiene que crear una tarea de copia de seguridad.

La tarea de copia de seguridad realiza una copia de seguridad de los nodos de origen y almacena los datos en el destino especificado. El archivado de archivos solo es compatible con la copia de seguridad de Windows basada en el Agente. El procedimiento siguiente explica los pasos para crear la tarea de copia de seguridad de Windows basada en el agente.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable **Tipo de tarea** seleccione **Copia de Seguridad, Windows**

basado en el agente.



Ahora, especifique el origen, el destino, la programación y las opciones avanzadas.

Especificación del origen

La página Origen le permite especificar los nodos de origen que se desean proteger. Se pueden seleccionar más de un nodo del plan. Si no se ha agregado ningún nodo a la consola, se podrán agregar nodos al crear o modificar un plan en la página Origen. Se puede guardar un plan sin agregar ningún nodo de origen. El plan se implementa solamente después de agregar nodos de origen.

Siga estos pasos:

1. En la ficha Origen, haga clic en **Agregar**.
2. Seleccione una de las opciones siguientes:

   Seleccionar los nodos para proteger en Arcserve UDP

   Abre el cuadro de diálogo Seleccionar los nodos para proteger en Arcserve UDP. Seleccione los nodos de la lista que se muestra. Seleccione esta opción si ya se han agregado los nodos a la consola.

   Agregar nodo de Windows

   Se abre el cuadro de diálogo Agregar nodos a un plan. Seleccione esta opción si no se han agregado los nodos y desea agregarlos manualmente para la protección.

   Detectar nodos desde Active Directory

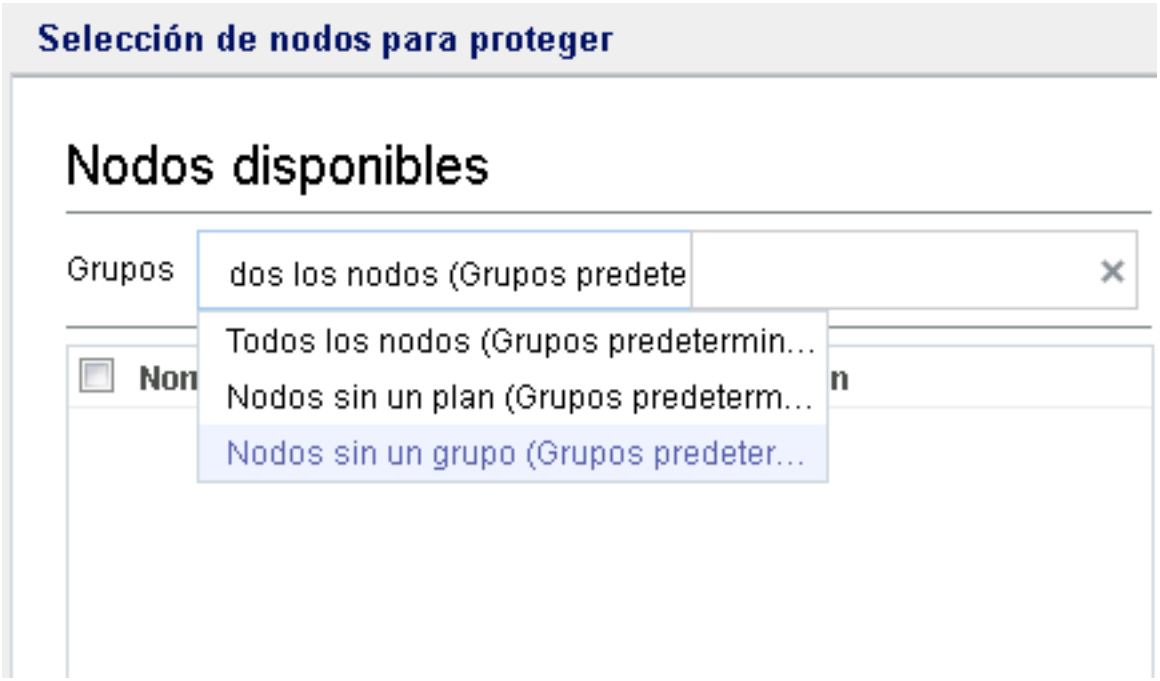
   Se abre el cuadro de diálogo Agregar nodos a la Consola de Arcserve UDP. Seleccione esta opción si desea detectar y agregar nodos en Active Directory.
3. Si ha seleccionado la opción **Seleccionar nodos para proteger en Arcserve UDP**, haga lo siguiente en el cuadro de diálogo Seleccionar nodos para proteger:
   a. (Opcional) Seleccione un filtro en la lista desplegable Grupos para filtrar nodos. Se pueden especificar palabras clave para filtrar más detalladamente los nodos.

      Los nodos se muestran en la columna Nodos disponibles.

   b. Seleccione los nodos en la columna Nodos disponibles y, a continuación, haga clic en la flecha simple hacia la derecha (>) o en la flecha doble hacia la derecha (>>) para mover los nodos seleccionados o todos los nodos respectivamente a la columna Nodos seleccionados.

      Los nodos se muestran en la columna Nodos seleccionados.

   c. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.



4. Para elegir el Tipo de El Protección, seleccione una de las opciones siguientes:

   Realizar copia de seguridad de todos los volúmenes

   Prepara una instantánea de copia de seguridad de todos los volúmenes.

   Realizar copia de seguridad de los volúmenes seleccionados

   Prepara una instantánea de copia de seguridad del volumen seleccionado.

   Se especifica el origen.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Seleccione uno de los siguientes **Tipos de destino**:

   Disco local o carpeta compartida

   Especifica que el destino de la copia de seguridad es un destino local o una carpeta compartida. Si se selecciona esta opción, se pueden guardar datos como puntos de recuperación o como conjuntos de recuperación. Las opciones Puntos de recuperación y Conjuntos de recuperación están disponibles en la ficha **Programación**.

   Servidor de puntos de recuperación de Arcserve UDP

   Especifica que el destino de la copia de seguridad es un servidor de punto de recuperación. Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.

2. Si se ha seleccionado **Servidor de punto de recuperación de Arcserve UDP**, se deben proporcionar los detalles siguientes:
   a. Seleccione un servidor de punto de recuperación.
   b. Seleccione un almacén de datos. La lista muestra todos los almacenes de datos que se han creado en el servidor de punto de recuperación especificado.
   c. Proporcione una contraseña de la sesión.
   d. Confirme la contraseña de la sesión.

3. Si ha seleccionado **Disco local o carpeta compartida**, a continuación proporcione los detalles siguientes:
   a. Proporcione la ruta completa del destino local o de red. Para el destino de la red, especifique las credenciales con acceso de escritura.
   b. Seleccione el algoritmo de cifrado. Para obtener más información, consulte Configuración de cifrado.
   c. Opcionalmente, proporcione una contraseña de cifrado.
   d. Confirme la contraseña de cifrado.

e. Seleccione un tipo de compresión. Para obtener más información, consulte Tipo de compresión.

Nota: Si se almacenan los datos a un disco local o a una carpeta compartida, no se pueden replicar los datos a otro servidor de punto de recuperación. Se es compatible con la replicación solamente si se almacenan los datos en un servidor de punto de recuperación.

Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y se pueden proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

Siga estos pasos:

1. (Opcional) Seleccione la opción para gestionar puntos de recuperación. Esta opción solo está visible si se ha seleccionado la carpeta local o compartida como destino de la copia de seguridad.

   Retener por puntos de recuperación

   Los datos de la copia de seguridad se almacenan como puntos de recuperación.

   Retener por conjuntos de recuperación

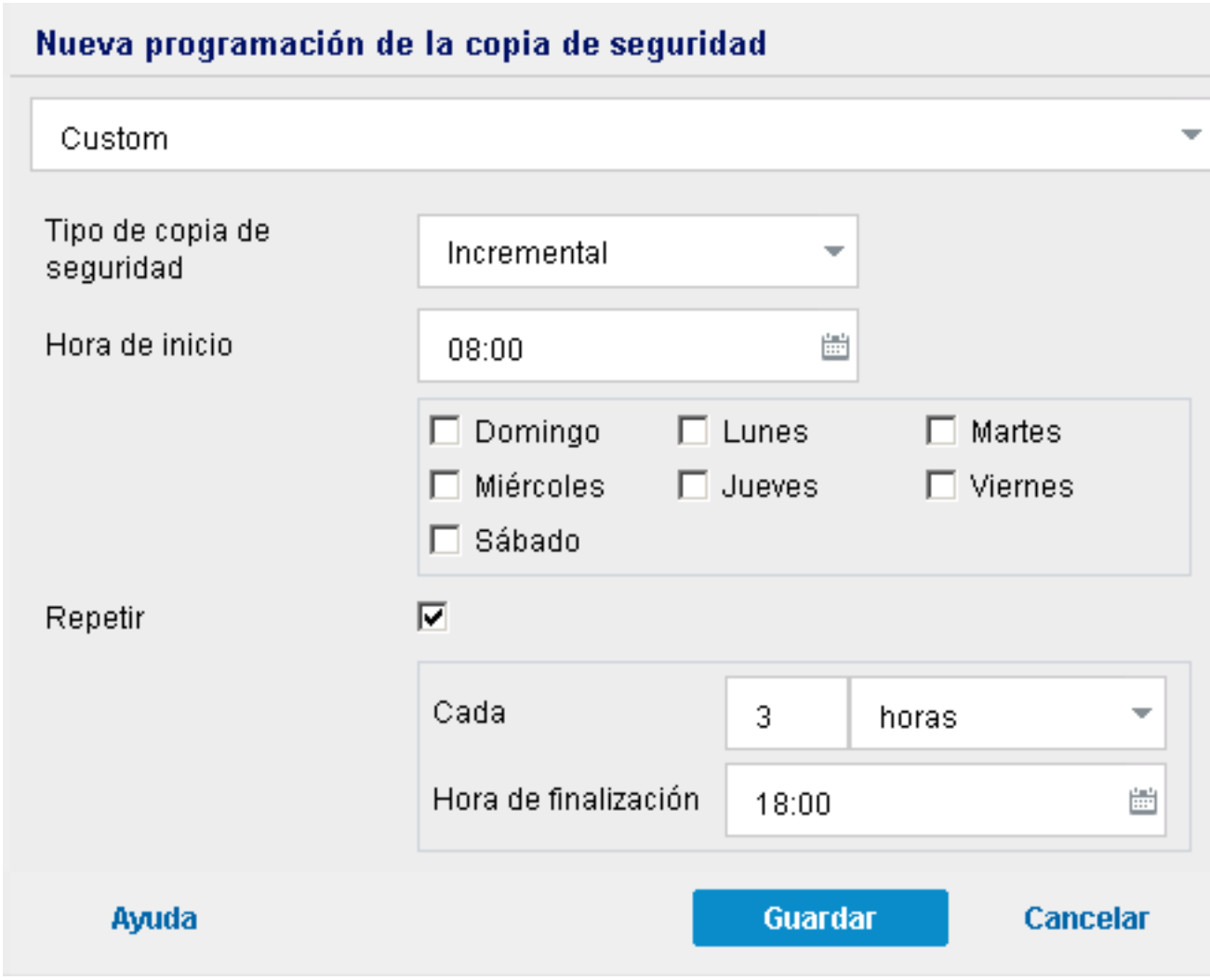
   Los datos de la copia de seguridad se almacenan como conjuntos de recuperación.

2. Agregue las programaciones de la copia de seguridad, de la combinación y del regulador.

   Agregar programación de la copia de seguridad

   a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

      Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Verificar

Especifica la programación de la copia de seguridad para las copias de seguridad de verificación.

Arcserve UDP verifica que los datos protegidos sean válidos y estén completos mediante una comprobación de confianza de la imagen de copia de seguridad almacenada en el origen de la copia de seguridad. Si es necesario, volverá a sincronizar la imagen. Una copia de seguridad de verificación se fijará en la copia de seguridad más reciente de cada bloque individual y comparará el contenido y la información con la de origen. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad de un bloque no coincide con la del origen (posiblemente por cambios en el sistema desde la última copia de seguridad), Arcserve UDP actualiza (resincroniza) la copia de seguridad del bloque que no coincide. Se puede utilizar también una copia de seguridad de verificación (aunque poco frecuentemente) para obtener la garantía de copia de seguridad completa sin utilizar el espacio necesario para una copia de seguridad completa.

Ventajas: produce una pequeña imagen de copia de seguridad si se compara con la copia de seguridad completa porque solamente se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventajas: el tiempo durante el cual se realiza la copia de seguridad es considerable puesto que todos los bloques de origen se comparan con los bloques de la última copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

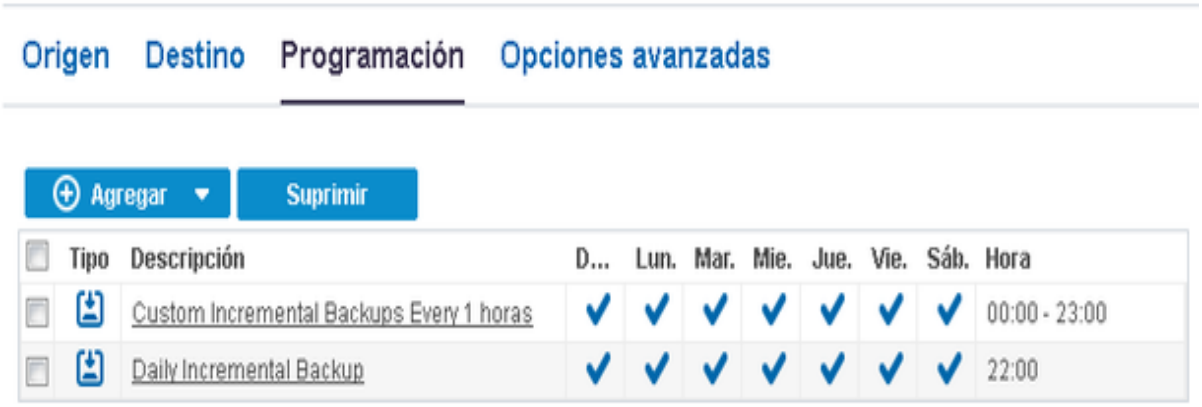
Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en Agregar y seleccione Agregar programación de la combinación.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

b. Especifique la hora de inicio para iniciar la tarea de combinación.

c. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

d. Haga clic en **Guardar**.

La Programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

   Se abre el cuadro de diálogo Agregar nueva programación del limitador.

b. Especifique el límite de rendimiento en MB por minuto.

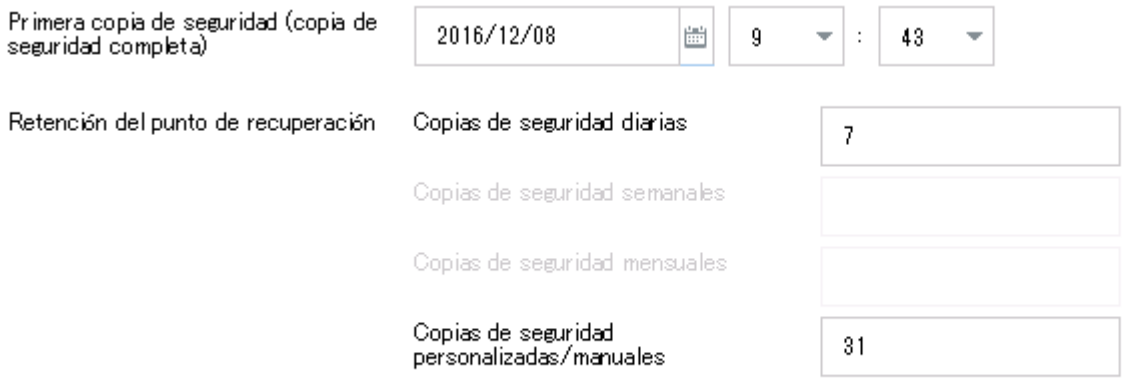
c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

   La programación del limitador se especifica y se muestra en la página **Programación**.

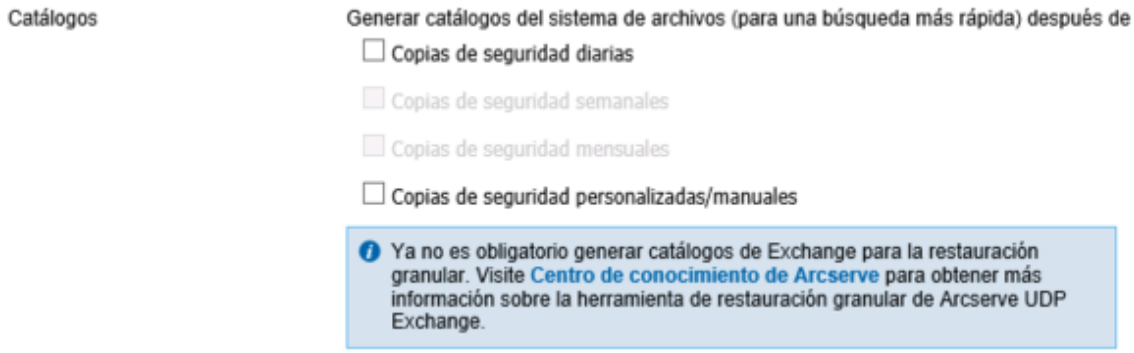
3. Especifique la hora de inicio para la copia de seguridad programada.



4. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

   Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo Programación de la copia de seguridad.

5. Especifique los detalles del catálogo.



Los catálogos permiten generar el catálogo del sistema de archivos. El catálogo del sistema de archivos se requiere para realizar la mejor búsqueda de la forma más rápida. Si se seleccionan las casillas de verificación del catálogo, los catálogos se activan en función del tipo de copia de seguridad especificada. Desactive la casilla de verificación para desactivar la generación del catálogo.

Se especifica la programación.

Funcionamiento de la programación avanzada y de la retención

La opción de programación le permite especificar una programación personalizada, una programación diaria/semanal/mensual o ambas. En la programación personalizada, se puede configurar la programación de la copia de seguridad durante cada día de la semana y se pueden agregar hasta cuatro programaciones de copia de seguridad cada día. Se puede seleccionar un día específico de una semana y crear un período de tiempo para definir cuando se desea ejecutar la copia de seguridad y con qué frecuencia.

Programación	Tarea compatible	Comentarios
Copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para ejecutar las tareas de copia de seguridad.
Regulación de la copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para controlar la velocidad de la copia de seguridad.
Combinar	Tarea de combinación	Defina cuando se deben ejecutar las tareas de combinación.
Programación diaria	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad diarias.
Programación semanal	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad semanales.
Programación mensual	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad mensuales.

Se pueden especificar también los valores de configuración de retención para los puntos de recuperación.

Nota: Establezca la configuración de la retención en cada plan para controlar cómo se retienen los datos para los nodos asignados a ese plan en el almacén de datos de destino.

Las programaciones para las copias de seguridad diarias/semanales/mensuales son independientes de la programación personalizada y de las unas a las otras. Se puede configurar solamente ejecutar una copia de seguridad diaria, una copia de seguridad semanal o una copia de seguridad mensual sin configurar la programación personalizada.

Programación de la tarea de copia de seguridad

Se pueden agregar cuatro períodos de tiempo por día en la programación de la copia de seguridad. Un período de tiempo válido es desde las 12:00 horas hasta las 23:59 horas. No se puede especificar un período de tiempo como, por

ejemplo, de las 18:00 horas a las 06:00 horas. En tales casos, se debe especificar manualmente dos períodos de tiempo diferentes.

Para cada período de tiempo, la hora de inicio está incluida y, en cambio, no se incluye la hora de finalización. Por ejemplo, se ha configurado ejecutar una copia de seguridad incremental ejecutada todas las horas entre las 06:00 horas y las 09:00 horas y la copia de seguridad se iniciará a las 06:00 horas. Esto significa que la copia de seguridad se ejecuta a las 06:00 horas, a las 07:00 horas y a las 08:00 horas, pero NO a las 09:00 horas.

Nota: Si desea ejecutar la tarea de copia de seguridad reiteradamente hasta el final del día, configure la programación hasta las 12:00 horas. Por ejemplo, para ejecutar la tarea de copia de seguridad cada 15 minutos durante todo el día, configure la programación de las 12:00 a las 12:00, cada 15 minutos.

Programación del regulador de la copia de seguridad

La programación del regulador de la copia de seguridad le permite controlar la velocidad del rendimiento de la copia de seguridad, que a su vez controla el uso de recursos (E/S del disco, CPU, ancho de banda de la red) del servidor del que se está realizando la copia de seguridad. Esto es útil si no se desea afectar al rendimiento del servidor durante el horario comercial. Se pueden agregar cuatro períodos de tiempo por día en la programación del regulador de la copia de seguridad. Para cada período de tiempo, se puede especificar un valor en MB por minuto. Este valor se utiliza para controlar el rendimiento de la copia de seguridad. Los valores válidos van desde 1 MB/minuto a 99999 MB/minuto.

Si una tarea de copia de seguridad excede el tiempo especificado, el límite del regulador se ajusta según el período de tiempo especificado. Por ejemplo, se ha definido el límite del regulador de la copia de seguridad en 500 MB/minuto desde las 08:00 horas a las 20:00 horas y en 2500 MB/minuto de las 20:00 horas a las 22:00 horas. Si una tarea de copia de seguridad se inicia a las 19:00 horas y se ejecuta durante tres horas, el límite del regulador es de 500 MB/minuto de las 19:00 horas a las 20:00 horas y de 2500 MB/minuto de las 20:00 horas a las 22:00 horas.

Si no se define ninguna programación de la copia de seguridad ni ninguna programación del rendimiento de la copia de seguridad, la copia de seguridad se ejecuta tan deprisa como pueda.

Programación de la combinación

Le permite combinar puntos de recuperación basándose en la programación proporcionada.

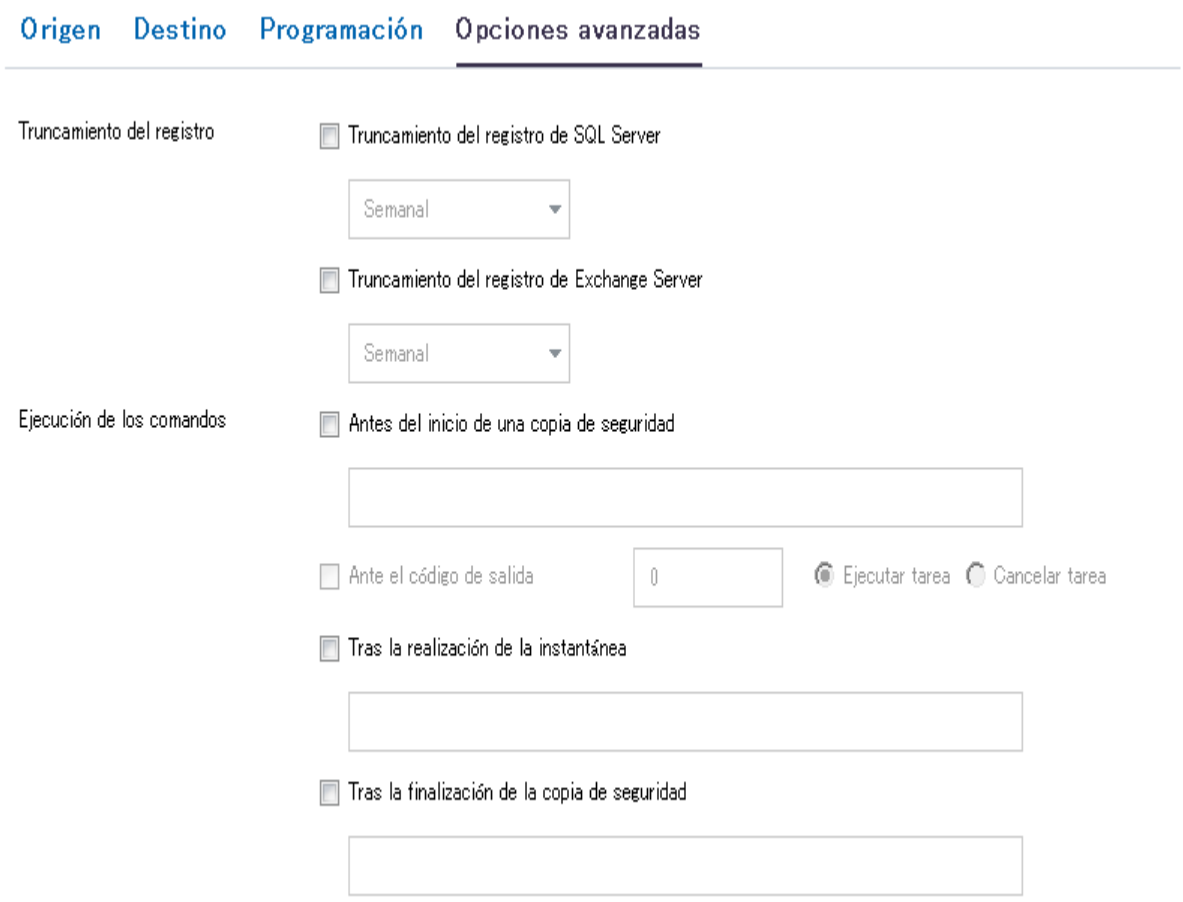
Tenga en cuenta los puntos siguientes para la tarea de combinación:

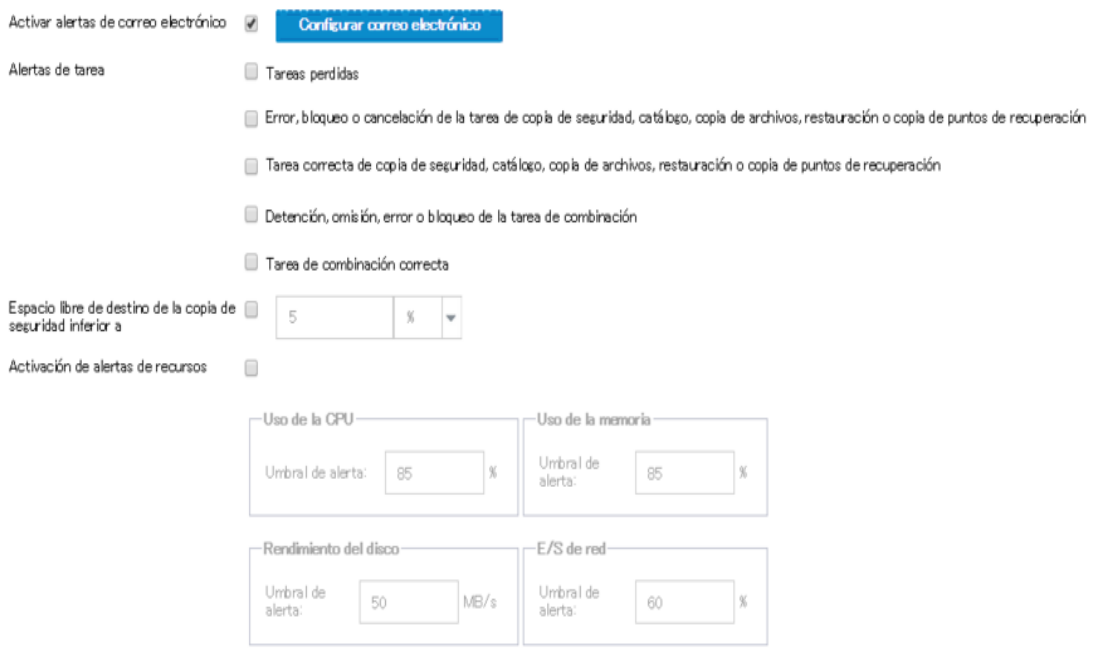
- Solamente una tarea de combinación puede ejecutarse para un nodo en cualquier momento proporcionado.
- Si se inicia una tarea de combinación, se tiene que completar antes de que la siguiente tarea de combinación se pueda iniciar. Esto no significa que, si uno o más conjuntos de puntos de recuperación se combinan, no se pueda agregar un punto de recuperación nuevo a este proceso de combinación hasta que el proceso de combinación del conjunto actual de puntos de recuperación se complete.
- Si una tarea de combinación está procesando más de un conjunto de puntos de recuperación (por ejemplo, el conjunto [1~4], el conjunto [5~11] y el conjunto [12~14] son tres conjuntos), el servidor de puntos de recuperación procesará estos conjuntos uno a uno.
- Si una tarea de combinación se reanuda después de una pausa, la tarea detecta en qué punto se ha pausado y reanuda la combinación a partir del punto de pausa.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye la configuración de registros de truncamiento, proporcionar la ubicación de los scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha Avanzada:





Siga estos pasos:

1. Especifique los siguientes detalles:

Cómo truncar un registro

Le permite especificar la programación para truncar los registros de SQL Server y Exchange Server. Se puede especificar la programación como **Diaria**, **Semanal** o **Mensual**.

Nombre de usuario

Le permite especificar el usuario que se autoriza para ejecutar un script.

Contraseña

Le permite especificar la contraseña del usuario autorizado para ejecutar el script.

Ejecutar un comando antes de empezar una copia de seguridad

Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde el script está almacenado. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de seguridad continuará cuando el script devuelva el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detendrá cuando el script devuelva el código de salida.

Ejecutar un comando después de realizar una instantánea

Le permite ejecutar un script después de realizar la instantánea de la copia de seguridad. Especifique la ruta donde el script está almacenado.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta donde el script está almacenado.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y se pueden especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de tareas que se desea recibir.

Cómo activar las alertas de recurso

Le permite especificar un umbral para el Uso de CPU, Uso de memoria, Rendimiento del disco y E/S de la red. Se puede proporcionar el valor en porcentaje. Se recibirá un correo electrónico cuando se exceda el valor de Umbral de alerta.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en Guardar.

Los cambios se guardan y se muestra una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **Recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar.

El plan de copia de seguridad se crea y se implementa automáticamente en el nodo de origen. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

Adición de una tarea de archivado de archivos al plan

La tarea de archivado de archivos permite archivar archivos individuales en el destino especificado. Los archivos originales se suprimen del origen después de que se hayan copiado los archivos en el destino especificado. Gracias a esta operación, se libera más espacio disponible en el origen. La tarea de archivado de archivos no depende de una tarea del catálogo.

Nota: Si una tarea de copia de seguridad está en curso y se pausa el plan, la tarea de copia de seguridad se detiene y la tarea de copia de archivos no se inicia. Cuando se reanuda el plan, la tarea de copia de archivos no se reanuda automáticamente. Se debe ejecutar manualmente otra tarea de copia de seguridad para iniciar la tarea de copia de archivos.

Para los archivos copiados mediante la opción Archivado de archivos, Arcserve UDP deja en blanco un archivo de código auxiliar con la extensión "UDP.txt". Para obtener más información sobre cómo actualizar el archivo de código auxiliar, consulte Actualización de archivos de código auxiliar.

Siga estos pasos:

1. Haga clic en **Agregar una tarea** en el panel izquierdo.

   Una tarea nueva se agrega al panel izquierdo.

2. En el menú desplegable **Tipo de tarea**, seleccione **Archivado de archivos**.

   Se agrega la tarea de archivado de archivos.

3. Haga clic en la ficha **Origen** e introduzca los detalles.

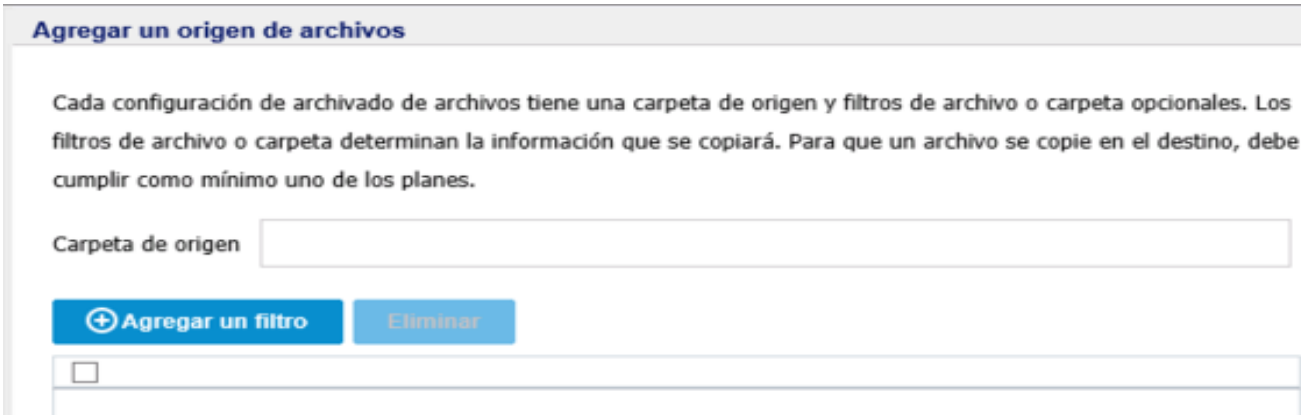
   Ubicación del punto de recuperación

   Especifica la ubicación de los puntos de recuperación que se archivarán. Este campo está preseleccionado.



4. Haga clic en **Agregar un origen**.

   Se abre el cuadro de diálogo **Agregar un origen de archivos**.

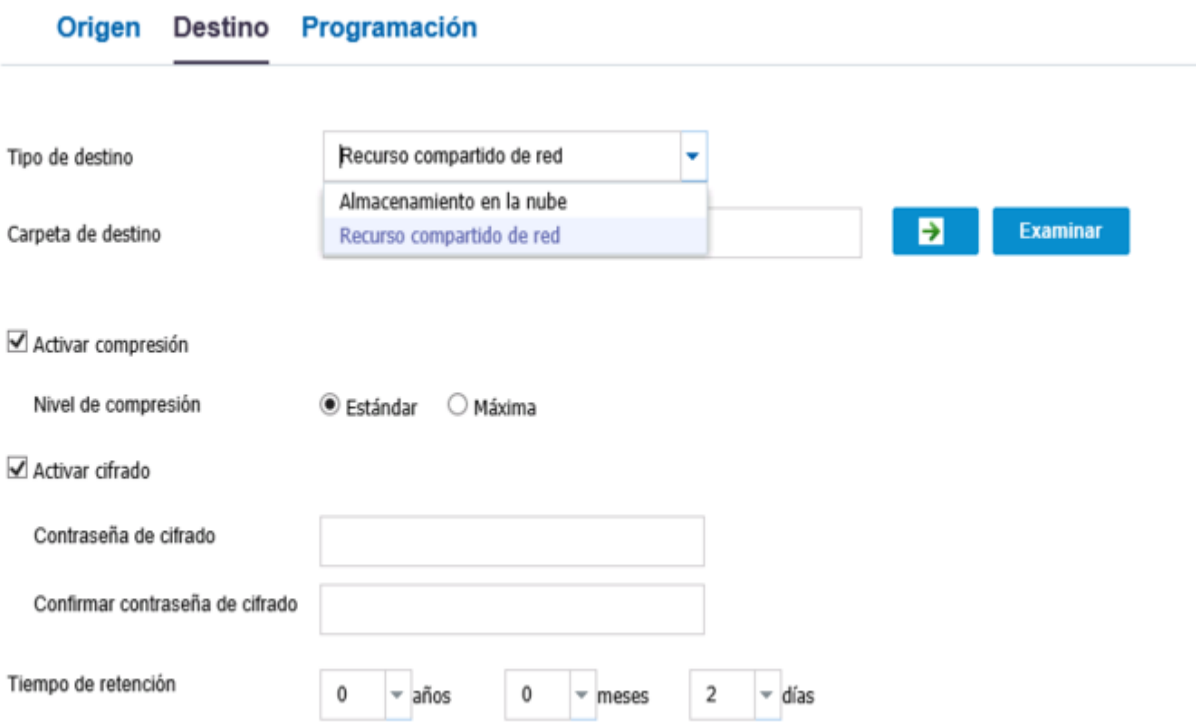


5. Especifique la ruta de archivo de la ruta de origen que desee copiar.
6. Especifique un valor para el **Filtro de tamaño de archivo** y otro para **Filtro de antigüedad de archivo**.



7. Haga clic en **Agregar un filtro**.
8. Seleccione el filtro de la lista y haga clic en **Aplicar**.
9. Haga clic en **Aceptar**.

   Se cerrará el cuadro de diálogo **Agregar un origen de archivos**.
10. Haga clic en la ficha **Destinos** y especifique los detalles del destino.



Tipo de destino

Especifica si el tipo de destino es un recurso compartido de red o un almacenamiento en la nube. Para cualquiera de estas opciones de destino, si la conexión al destino especificado se pierde o se interrumpe, Arcserve UDP realiza varios intentos para continuar con la tarea de copia de archivos. Si estos reintentos no son correctos, se realizará una tarea de nueva copia de seguridad a partir del punto en que se produjo el error. Además, el registro de actividades se actualizará con un mensaje de error correspondiente y se enviará una notificación de correo electrónico (si se configura).

Recurso compartido de red

Especifica que el destino es una carpeta compartida. Cuando se selecciona, permite especificar la ruta completa de la ubicación a la que desee desplazar los archivos/carpetas de origen.

Carpeta de destino

Especifica el destino donde se almacenan los archivos archivados. El destino puede ser cualquier volumen local o carpeta o un recurso compartido de archivo a los cuales puede acceder cualquier ruta de convención de denominación uniforme (UNC). Este campo está disponible cuando se selecciona Recurso compartido de red o Volumen en el nodo protegido como tipo de destino. También se puede explorar la carpeta de destino.

Almacenamiento en la nube

Especifica que los archivos copiados se almacenan en un entorno de nube. Arcserve UDP admite actualmente la copia de archivos a varios distribuidores de la nube como, por ejemplo, Amazon S3 (Simple Storage Service), compatible con Amazon S3, Windows Azure, compatible con Windows Azure, Eucalyptus-Walrus y FUJITSU Hybrid IT Service FJcloud-O. Estos distribuidores de la nube son servicios web disponibles públicamente que permiten almacenar y recuperar cualquier cantidad de datos, en cualquier momento y desde cualquier sitio de la Web en un entorno seguro

Nota: Para eliminar cualquier error potencial de sesgo de reloj al intentar conectarse a la nube, compruebe que el equipo tiene establecida la zona horaria correcta y que el reloj esté en sincronización con la hora global. Es recomendable comprobar siempre la hora del equipo con la hora GMT. Si la hora del equipo no se sincroniza con la hora de reloj global correcta (entre 5 y 10 minutos), puede que la conexión de la nube no funcione. Si es necesario, restablezca la hora correcta del equipo y vuelva a ejecutar la tarea de copia.

Dispositivo de almacenamiento

Seleccione el tipo de dispositivo en la lista desplegable.

Almacenamiento en la nube

Seleccione la ruta de almacenamiento en la nube en la lista desplegable. La lista desplegable está disponible si ha especificado los detalles de almacenamiento en la nube. Si se especifica la cuenta de almacenamiento en la nube por primera vez, haga clic en Agregar para agregar la cuenta de la nube. A partir de la siguiente vez que se selecciona Almacenamiento en la nube, la cuenta aparecerá en la lista desplegable de Almacenamiento en la nube.

Nota: Para obtener más información sobre cómo agregar una cuenta de la nube, consulte Agregar una cuenta de la nube.

Compresión

Especifica el tipo de compresión que debe utilizarse para las tareas de archivado de archivos.

La compresión se realiza para reducir el espacio de almacenamiento en el destino Copia de archivo, pero también tiene un impacto inverso en la velocidad de copia de archivo a causa del aumento del uso de la CPU.

Nota: Para una tarea de archivado de archivos comprimidos, el registro de actividades mostrará solamente el tamaño no comprimido.

A continuación se especifican las opciones disponibles:

Compresión estándar

Se realiza algún tipo de compresión. Esta opción proporciona un buen equilibrio entre el uso de la CPU y el requisito de espacio de almacenamiento. Se trata de la configuración predeterminada.

Compresión máxima

Se realiza la compresión máxima. Esta opción proporciona el uso de la CPU más elevado (velocidad más baja) pero también dispone del requisito de espacio de almacenamiento más bajo para la copia de archivo.

Activación del cifrado

Especifica el uso del cifrado para el archivado de archivos.

El cifrado de datos es la traducción de los datos a una forma que resulte ininteligible sin un mecanismo de descifrado. La protección de datos de Arcserve UDP utiliza algoritmos de cifrado seguros AES-256 (Estándar de cifrado avanzado) para obtener la máxima seguridad y privacidad de los datos especificados. Cuando se selecciona un cifrado, se debe proporcionar (y confirmar) una contraseña de cifrado.

Tiempo de retención

Especifica la cantidad de tiempo (años, meses, días) durante el cual se conservan los datos almacenados en la ubicación de destino. Al final del período de

tiempo de retención especificado, se borrarán definitivamente los datos almacenados del destino.

Los cálculos del tiempo de retención están basados en un mes que es de 30 días y un año que es 365 días. Por ejemplo: Si especifica un tiempo de retención de 2 años, 2 meses y 5 días, el tiempo de retención total para sus datos copiados del archivo es de 795 días (365 + 365 + 30 + 30 + 5).

Importante: Al final del tiempo de retención especificado cuando los datos se borran definitivamente desde el destino, todos estos datos movidos no se almacenan ni se guardan.

Nota: El proceso de borrado definitivo del tiempo de retención se activa sólo cuando se activa la opción Programación de copia de archivo.

Versión del archivo menor de

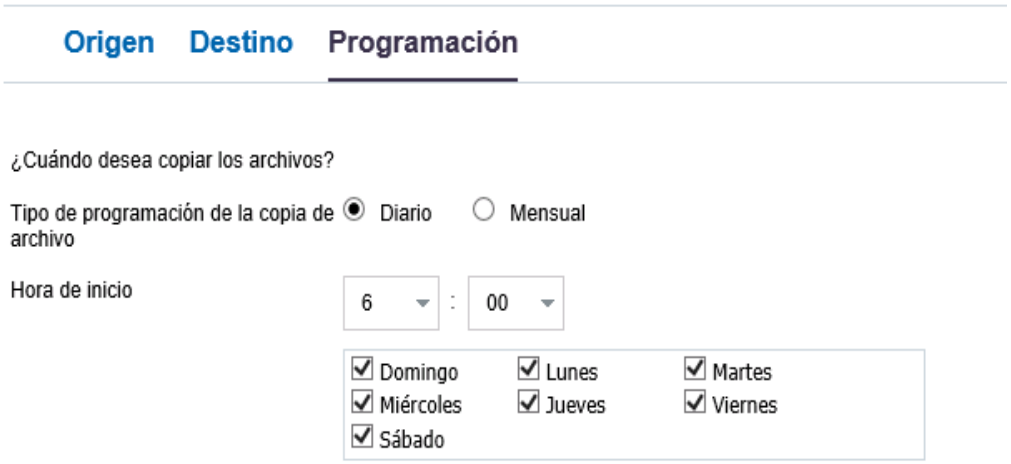
Esta configuración solamente se aplica a los datos copiados que se conservan (los datos no copiados se mueven).

Especifica el número de copias conservadas y almacenadas en la ubicación de destino (nube o disco). Si se excede este número, la primera versión (la más antigua) se eliminará. Este ciclo de eliminación de la versión almacenada más antigua se repetirá a medida que se agreguen versiones más nuevas al destino, de modo que permite mantener siempre el número especificado de versiones almacenadas.

Por ejemplo, si el recuento de retenciones de versiones de archivo especificado se establece en 5 y se realizan cinco copias de archivo a las t1, t2, t3, t4, y t5, se convierten en las cinco versiones de copia de archivo conservadas y disponibles para la recuperación. Después de realizar la sexta copia de archivos (la nueva versión se guarda), Arcserve UDP elimina la copia t1. Las cinco versiones disponibles que restan para la recuperación son ahora t2, t3, t4, t5 y t6.

De forma predeterminada, el número de copias conservadas en la ubicación de destino antes de la eliminación es 15.

11. Haga clic en la ficha **Programación** y especifique la hora a la que se deba ejecutar la tarea de archivado de archivos.



12. Haga clic en **Guardar**.

    Los cambios se guardan y la tarea de archivado de archivos se implementa automáticamente en el nodo.

Agregación de filtros de archivado de archivos

Agregar un filtro

Permite agregar un filtro. Los filtros permiten limitar los objetos de los cuales ciertos tipos y valores especificados realizarán copia de archivo.



Tipo de filtro

Existen dos tipos de filtros: Incluir y Excluir.

Un filtro Incluir copiará solamente los objetos del origen de copia de archivo que coincidan con los valores especificados.

Un filtro Excluir copia todos los objetos del origen de copia de archivo excepto los que coincidan con los valores especificados.

Se pueden especificar varios filtros dentro de la misma solicitud de copia de archivo mediante la separación de cada valor de filtro con una coma.

- Si se especifican varios filtros Incluir, los datos se incluirán en la copia de archivo si coincide uno de los filtros Incluir.
- Si se especifican varios filtros Excluir, los datos se excluirán de la copia de archivo si coincide uno de los filtros Excluir.

- Se pueden mezclar tanto los filtros Incluir como Excluir en la misma solicitud de copia de archivo.

  Nota: En el caso de que los parámetros especificados de los filtros Excluir e Incluir se contradigan, el filtro Excluir siempre tendrá una prioridad más alta y se impondrá. Un filtro Incluir nunca puede realizar copia de archivo de un objeto que también haya sido Excluido.

Variable de filtro (Patrón)

Existen dos tipos de filtros de patrón de variables: Patrón de archivo y Patrón de carpeta.

Se puede utilizar un filtro Patrón de archivo o Patrón de carpeta para incluir o excluir ciertos objetos de la copia de archivo.

Valor de filtro

El valor de filtro permite limitar la información de la cual se realiza copia de archivo seleccionando solamente la información del parámetro que se especifique, como los archivos .txt.

Arcserve UDP admite el uso de caracteres comodín para poder seleccionar a la vez varios objetos cuyos archivos se deban copiar en una única solicitud. Un carácter comodín es un carácter especial que se puede utilizar como sustituto para representar bien un carácter solo o una cadena de texto.

El asterisco y el signo de interrogación de los caracteres comodines se admiten en el campo Valor. Si no sabe el valor de patrón de la carpeta/archivo completo, se pueden simplificar los resultados del filtro. Para ello, especifique un carácter comodín.

"*": utilice el asterisco para sustituir cero o más caracteres en el valor.

"?" "?": utilice el signo de interrogación para sustituir un único carácter en el valor.

Por ejemplo, se puede introducir *.txt para excluir todos los archivos con una extensión de .txt si no se sabe el nombre específico del archivo. Se puede proporcionar la cantidad del nombre de archivo que sepa. A continuación, utilice caracteres comodines para rellenar los espacios en blanco.

Nota: Si se selecciona Patrón de archivo como tipo de filtro, hay disponible una lista desplegable de filtros predeterminados para muchos archivos utilizados comúnmente (archivos de MS-Office, archivos de imagen, archivos ejecutables, archivos temporales, etc.). Después de elegir cualquiera de los

filtros predeterminados, se pueden añadir o modificar todavía los valores correspondientes.

Filtro de tamaño del archivo

Los filtros de tamaño de archivo permiten limitar los objetos de origen de los cuales se debe realizar una copia de archivo en función del tamaño del archivo. Cuando se activa el filtro Tamaño de archivo, los parámetros que se especifican se convertirán en el filtro para los objetos que se incluyan o que no se incluyan en la copia de archivo. Se puede seleccionar el intervalo (Igual a o Mayor que, Igual a, Menos de o Entre) e introduzca un valor para el tamaño.

Por ejemplo, si se especifica Igual a o Mayor de 10 MB, Arcserve UDP solamente archivará objetos de copias de archivos que cumplan estos criterios. El resto de objetos que no cumplan estos criterios de tamaño de archivos no se archivarán.

Filtro de antigüedad de archivo

Los filtros de antigüedad de archivo permiten incluir objetos de origen de los que se puede realizar copia de archivo del archivo en ciertas fechas. Se puede seleccionar un parámetro (Archivos a los que no se ha accedido en, Archivos no modificados en y/o Archivos no creados en) e introducir un valor para el número de días, meses, o años para el filtro de antigüedad de archivo. Se pueden seleccionar varios filtros de antigüedad de archivo para la copia de archivo.

Por ejemplo, si se especifica Archivos sin modificar en 180 días, Arcserve UDP copiará automáticamente todos los archivos que cumplan este criterio (que no se hayan modificado durante los últimos 180 días).

Importante: Si se especifican tanto los filtros Tamaño de archivo como Antigüedad de archivo (o varios filtros de antigüedad de archivo), solamente se copiarán los archivos que cumplan todos los parámetros de filtro especificados. No se copiarán los archivos que no cumplan alguno de estos parámetros especificados.

Actualización de los archivos de código auxiliar

Para los archivos copiados mediante la opción Archivado de archivos, Arcserve UDP deja un archivo de código auxiliar con la extensión UDP.txt. El archivo de código auxiliar contiene información sobre el destino al cual se mueven los archivos e información adicional. Si un archivo se restaura en la ubicación original y a continuación se mueve otra vez al destino especificado, el archivo de código auxiliar se actualizará con esta información de movimiento. En caso necesario, estos archivos de código auxiliar de copia de archivo se pueden desactivar de forma segura o suprimirse sin ningún impacto negativo. (No se suprimirán archivos de código auxiliar existentes cuando la clave de registro se cambie para no crear más archivos de código auxiliar).

La siguiente información está presente en el archivo de código auxiliar de forma predeterminada:

Póngase en contacto con el departamento de TI para restaurar este archivo.

Se puede cambiar el texto predeterminado mediante la adición de una entrada de configuración. Agregue la siguiente entrada de la etiqueta XML en el archivo FileCopyDebugSetting.xml que se encuentra en el directorio $UDPHome\Engine\Configuration:

<ArchiveStubFileText>Se puede agregar texto nuevo aquí para que se muestre en el archivo de código auxiliar

</ArchiveStubFileText>

Ejemplo: El archivo FileCopyDebugSetting.xml sería el siguiente

```
<?xml version="1.0" encoding="UTF-8"?>
<HKLM>
<AFArchiveDLL>
<ArchiveStubFileText>Se puede agregar texto nuevo aquí para que se muestre en el archivo de código auxiliar</ArchiveStubFileText>
</AFArchiveDLL>
</HKLM>
```

Si el archivo FileCopyDebugSetting.xml no está presente en el directorio $UDPHome\Engine\Configuration, cree el archivo XML.

Si se desea desactivar la creación del archivo de código auxiliar, agregue la siguiente entrada de la etiqueta XML en el archivo FileCopyDebugSetting.xml que se encuentra en el directorio $UDPHome\Engine\Configuration:

<CreateStubFile>0</CreateStubFile>

Ejemplo: El archivo FileCopyDebugSetting.xml sería el siguiente

```
<?xml version="1.0" encoding="UTF-8"?>
<HKLM>

<AFArchiveDLL>
<CreateStubFile>0</CreateStubFile>
</AFArchiveDLL>
</HKLM>
```

Nota: Si se desactivan o suprimen los archivos de código auxiliar de copia de archivo, ya no se podrá realizar el seguimiento del estado y la ubicación de los archivos movidos.

(Opcional) Realización de un archivado de archivos manual

Normalmente, los archivados de archivos se realizan de forma automática y están controlados por la configuración de programación de archivados de archivos. Además del archivado de archivos programado, un archivado de archivos manual ofrece la posibilidad de copiar los archivos importantes según resulte necesario. Cuando se ejecuta un archivado de archivos manual, la tarea archiva todas las sesiones del origen de archivado de archivos.

El archivado de archivos se puede ejecutar manualmente desde las vistas Nodos y Planes haciendo clic en el menú contextual o el menú **Acciones**.

Se deben seguir estos pasos para ejecutar el archivado de archivos manualmente desde la vista de Nodos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Se muestran los nodos en el panel central.
3. Seleccione los nodos para una tarea de archivado de archivos. Los nodos deben tener un plan de archivado de archivos asignado.
4. En el panel central, haga clic en **Acciones**, **Archivar archivos ahora**.

   Aparecerá el cuadro de diálogo **Run File archive now (Ejecutar archivado de archivos ahora)**.
5. Haga clic en **Aceptar**.

   Se ejecutará la tarea de archivado de archivos.

   El archivado de archivos manual se realizará correctamente.

Verificación del plan

Para verificar el plan de la copia de archivo, confirme que se ha creado correctamente el plan. Después de verificar que el plan se ha creado correctamente, compruebe si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Después de que la tarea de copia de seguridad se complete correctamente, se ejecutará la tarea de copia de archivos tal y como estaba programada. Se puede comprobar el estado de la tarea de copia de seguridad y de la tarea de copia de archivo en la ficha **tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga estos pasos para verificar las tareas de copia de archivo:

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas finalizadas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad y la tarea de copia de archivo se han realizado correctamente.

Cómo crear un plan de copia en cinta

Arcserve UDP se integra con Arcserve Backup para copiar los datos de la copia de seguridad a un destino de medios de cinta. Se puede crear un plan para realizar una copia de seguridad de los datos de origen y para copiar los datos de la copia de seguridad a la cinta. Se puede crear y gestionar el plan desde la Consola.

Las ventajas de archivar puntos de recuperación en un medio de cinta son las siguientes:

- Cumplir las reglamentaciones: facilita la conservación de documentos, correos electrónicos y otros datos críticos importantes, puesto que son necesarios para cumplir con la normativa interna y externa.
- Reducir costes de almacenamiento: facilita la recuperación de la capacidad de almacenamiento mediante la migración de los datos más antiguos o de los datos a los que se ha accedido de manera menos frecuente desde los servidores primarios a ubicaciones de almacenamiento de archivo de archivado más rentables.
- Mantener versiones de varios archivos: facilita la reversión a versiones anteriores de archivos de los que se ha realizado copia de seguridad (si es necesario) o mantener versiones múltiples de los mismos archivos en destinos diferentes.

Escenarios compatibles

- Si es el destino de la tarea 1 es el **servidor de puntos de recuperación de Arcserve UDP**, instale el agente de cliente en el nodo del servidor de puntos de recuperación.
- Para el plan basado en el agente con un destino como **recurso compartido local o remoto**, instale el agente de cliente en todos los nodos del agente de Arcserve UDP.
- Para el plan sin agente basado en el host, instale el agente de cliente en el nodo del proxy de Arcserve UDP.

¿Qué hacer a continuación?

- Revisión de los requisitos previos
- Creación de un plan con una tarea de copia de seguridad
- Adición de un plan de copia en cinta
- Verificación del plan

Revisión de las consideraciones y requisitos previos

Verifique si se han completado los requisitos previos siguientes:

- Inicie sesión en la Consola.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.
- Se ha agregado el servidor de Arcserve Backup a la consola. Para obtener más información sobre cómo agregar el servidor de Arcserve Backup a la consola, consulte Agregar servidores de Arcserve Backup.
- El servidor de puntos de recuperación que se especifica en la tarea principal de un plan debe tener instalado el Agente del servidor de Arcserve Backup.

Creación de un plan con una tarea de copia de seguridad

Un plan incluye tipos diferentes de tareas que se desea realizar. Por lo general, un plan incluye una tarea primaria seguida de una tarea secundaria. Normalmente, una tarea principal es una tarea de copia de seguridad o de replicación desde una tarea remota de la Consola. El rol de una tarea de copia de seguridad es crear una copia de seguridad de los nodos de origen que se desean proteger. Puede realizar copias de seguridad de máquinas físicas y virtuales de Windows y Linux. A continuación, se pueden guardar los datos de copia de seguridad a otra ubicación, como una medida de precaución adicional.

Para obtener más información, consulte:

- Cómo crear un plan de copia de seguridad en Windows para realizar copias de seguridad de un nodo de Windows.
- Cómo crear un plan de copia de seguridad de máquina virtual basada en el host para realizar copias de seguridad de máquinas virtuales.
- Cómo crear un plan de copia de seguridad en Linux para realizar copias de seguridad de nodos de Linux.
- Cómo replicar datos entre almacenes de datos gestionados desde consolas de UDP diferentes para replicar datos de copia de seguridad en un destino remoto.

Adición de una tarea de copia en cinta al plan

La tarea Copia en cinta permite copiar los datos a una cinta. El medio de cinta se identifica en el servidor de Arcserve Backup agregado.

Siga estos pasos:

1. Haga clic en **Agregar una tarea** en el panel izquierdo.

   Una tarea nueva se agrega al panel izquierdo.

2. En el menú desplegable **Tipo de tarea**, seleccione **Copia en cinta**.

   La tarea Copia en cinta se ha agregado.

   Nota: Las copias de seguridad personalizadas no activan las tareas de copia en cinta.

   Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

Por lo general, el archivo de origen es un destino de copia de seguridad o un destino de replicación.

Siga estos pasos:

1. Especifique los detalles siguientes en la página **Origen**.

   Origen de la copia en cinta

   Especifica la ubicación de los puntos de recuperación que se copiarán. Si solo tiene un origen, este campo está preseleccionado. Por ejemplo, si su plan tiene solamente una tarea de copia de seguridad y, a continuación, agrega la tarea Copia en cinta, el destino de la tarea de copia de seguridad se convierte en el origen de la copia en cinta. Si dispone de varios orígenes para la copia en cinta, puede agregar una copia en cinta para cada origen. Por ejemplo, si la primera tarea es una tarea de copia de seguridad y la segunda y tercera tareas son tareas de replicación, pueden agregarse tres tareas de copia en cinta al plan.

   Tipos de puntos de recuperación

   Especifica los tipos de puntos de recuperación. Las opciones disponibles son copias de seguridad diarias, semanales y mensuales.

2. Haga clic en la ficha **Destino**.

   Se abre la página **Destino**.

   Se han proporcionado correctamente los detalles del origen.

Especificación del destino

El destino es un grupo de medios de cinta del servidor de Arcserve Backup. Antes de crear esta tarea, se debe agregar el servidor de Arcserve Backup a la Consola.

Siga estos pasos:

1. Especifique los siguientes detalles sobre el origen de la copia de seguridad.

Servidor de Arcserve Backup

Seleccione el servidor de Arcserve Backup en la lista desplegable.

Grupo de medios

Seleccione el grupo de medios en la lista desplegable. El grupo de medios depende del servidor de Arcserve Backup. De forma predeterminada, el dispositivo basado en disco de <ASBU> no aparece en el grupo de medios. Además, el grupo RAID de cintas no figura en el grupo de medios.

Para migrar puntos de recuperación de Arcserve UDP a un dispositivo basado en disco de Arcserve Backup, los puntos de recuperación incremental deben convertirse en puntos de recuperación completa. El método recomendado para migrar puntos de recuperación de Arcserve UDP a un dispositivo basado en disco consiste en llevar a cabo una replicación desde el almacén de datos de Arcserve UDP a otro almacén de datos.

Solo los grupos de cintas pueden configurarse como destino para una tarea de copia en cinta. Se puede modificar una clave de configuración en el archivo ConsoleConfiguration.xml disponible en la ruta de configuración de la gestión de UDP para mostrar el grupo ASBU FSD como el destino de la copia en cinta:

C:\Archivos de programa\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml

<displayASBUFSDGroup>0</displayASBUFSDGroup>

Cuando el valor es 0, no se muestra el grupo ASBU FSD.

<displayASBUFSDGroup>1</displayASBUFSDGroup>

Cuando el valor es 1, se muestra el grupo ASBU FSD.

Una vez modificados los valores de configuración, reinicie el Servicio de gestión de Arcserve UDP para que se apliquen los cambios.

La lista del grupo de medios se consultará desde el servidor de Arcserve Backup. Se corresponde con la lista de grupo de dispositivos del servidor de Arcserve Backup.

Multiplexación

Seleccione la casilla de verificación para activar la multiplexación. Especifique el número máximo de flujos que se pueden escribir en una cinta al mismo tiempo. El número predeterminado de flujos es 4 y el intervalo admitido se encuentra entre 2 y 32.

cifrado

Especifica el uso del cifrado para la copia en cinta.

Si se activa el cifrado, se garantiza que se cifren los datos en las cintas. Cuando se selecciona un cifrado, se debe proporcionar (y confirmar) una contraseña de cifrado.

Compresión

Si se activa la compresión, se garantiza que se compriman los datos en las cintas.

2. Compruebe los detalles del grupo de medios del servidor de Arcserve Backup y del grupo de medios seleccionados.
3. Haga clic en la ficha **Programación**.

   Se abrirá la página Programación.

   De esta forma, se habrá especificado el destino.

Especificación de la programación

Se puede programar el inicio de la tarea de copia en cinta. También se puede decidir el modo de uso de la cinta y la política de retención de medios.

Siga estos pasos:

1. Haga clic en **Agregar**, **Agregar programación de copia en cinta**.

   Se abre cuadro de diálogo **Agregar programación de copia en cinta**.

2. Especifique una programación de cinta.

   Una programación define el intervalo de tiempo para iniciar una tarea de copia en cinta. Si se agrega una programación, la tarea de copia en cinta solo se ejecuta durante la programación de tiempo definida. Si no se especifica ninguna programación, la tarea de copia en cinta se ejecuta dentro de los 30 minutos después de que un punto de recuperación completo esté listo en un almacén de datos.

3. Haga clic en **Guardar**.

   Se cierre el cuadro de diálogo **Agregar programación de copia en cinta**.

4. Seleccione **Nombre de la agrupación de medios** de la lista desplegable.

   El nombre de la agrupación de medios se selecciona de forma predeterminada según el nombre del plan.

   También se puede seleccionar un nombre de agrupación de medios existente de la lista desplegable. En ese caso, se copian en esta tarea la política de retención de medios y el modo de uso de la cinta asociados a esa agrupación de medios. Las cintas se pueden compartir entre varios planes de Arcserve UDP especificando la misma agrupación de medios en todos los planes de Arcserve UDP.

   También se puede especificar un nombre de agrupación diferente. Los nombres de agrupación de medios pueden contener un máximo de 13 caracteres.

5. Especifique una política en **Retención del punto de recuperación**.

   Una política de retención de puntos de recuperación permite retener los puntos de recuperación de forma diaria, semanal o mensual. Se puede especificar un tiempo de retención diferente para los distintos tipos de puntos de recuperación. Por ejemplo, si se selecciona **Copias de seguridad diarias** y **Copias de seguridad semanales** en la ficha **Origen**, se puede especificar un período de retención de puntos de recuperación diferente para cada tipo de copia de seguridad seleccionado.

6. Seleccione una de las opciones de **Uso de la cinta**.

   Adjuntar a cintas existentes

Indica que se copian en la misma cinta todos los puntos de recuperación generados dentro del período de retención especificado. Por ejemplo, si se ha especificado el tiempo de retención para la copia de seguridad diaria en 7, se copian en la misma cinta todos los puntos de recuperación del día 1 al día 7. A continuación, todos los puntos de recuperación desde los próximos 7 días (del día 8 a día 14) se copian en una cinta diferente, y así sucesivamente.

Los puntos de recuperación de la primera semana (del día 1 al día 7) se retienen durante los próximos 7 días (del día 8 al día 14). A partir del 15, los puntos de recuperación se copian de nuevo en la cinta 1, ya que la política de retención de puntos de recuperación para la primera semana ha caducado.

En la lista siguiente, se muestra el tiempo de retención predeterminado para Adjuntar a cintas existentes:

- Diario - 7 días
- Semanal - 5 semanas
- Mensual - 12 meses

Los siete puntos de recuperación diarios se copian en la misma cinta, los cinco puntos de recuperación semanales se copian en la misma cinta y los doce puntos de recuperación mensuales se copian en la misma cinta.

Copiar en cintas independientes

Indica que los puntos de recuperación de cada día se copian en cintas distintas. Por ejemplo, si se ha especificado el tiempo de retención para la copia de seguridad diaria en 7, los puntos de recuperación del día 1 se copian en la cinta 1, los puntos de recuperación del día 2 se copian en la cinta 2, los puntos de recuperación del día 3 se copian en la cinta 3, y así sucesivamente.

Los puntos de recuperación del día 1 se retienen durante siete días. En el día 8, los puntos de recuperación se copian en la cinta 1, ya que la política de retención para los puntos de recuperación del día 1 ha caducado.

En la lista siguiente, se muestra el tiempo de retención predeterminado para Copiar en cintas independientes:

- Diario - 7 días
- Semanal - 5 semanas
- Mensual - 12 meses

Cada uno de los siete puntos de recuperación diarios se copian en cintas distintas, cada uno de los cinco puntos de recuperación semanales se copian en cintas distintas y cada uno de los doce puntos de recuperación mensuales se copian en cintas distintas.

7. Haga clic en la ficha **Opciones avanzadas**.

   Aparecerá la página **Configuración avanzada**.

   Se ha especificado la programación.

Especificación de la configuración avanzada

La configuración avanzada le permite configurar algunos valores de configuración adicionales para la tarea de copia en cinta.

1. Especifique los siguientes detalles:

Expulsión del medio

Especifica que el medio se extrae de la unidad después de finalizar la tarea. De esta manera se evita que cualquier otra tarea sobrescriba información en este medio.

Verificación de copia de seguridad

Especifica que Arcserve Backup verifica la fiabilidad de la copia de seguridad comprobando el encabezado de cada archivo para mejorar la legibilidad. Esta opción no se aplica a las copias de seguridad de multiplexación.

Ejecutar un comando antes de que se inicie una tarea de copia en cinta

Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde el script está almacenado. Haga clic en Ante el código de salida y especifique el código de salida para Ejecutar tarea o Cancelar tarea. Ejecutar tarea indica que la tarea de copia de seguridad continuará cuando el script devuelva el código de salida. Cancelar tarea indica que la tarea de copia de seguridad se detendrá cuando el script devuelva el código de salida.

Ejecutar un comando después de que finalice una tarea de copia en cinta

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta donde el script está almacenado.

Nombre de usuario para comandos

Permite especificar el nombre de usuario para ejecutar el script.

Contraseña para comandos

Permite especificar la contraseña para ejecutar el script.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y se pueden especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de tareas que se desea recibir.

2. Haga clic en **Guardar**.

   Los cambios se guardan y se muestra una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

   Se crea la tarea de copia en cinta y se ejecuta según la programación.

   Nota: Cuándo se ejecuta la tarea de **copia en cinta**, los valores del controlador de tareas en la Consola de Arcserve UDP son diferentes de los que están en Acserve Backup.

   Importante: Después de copiar los puntos de recuperación a una cinta, no se pueden restaurar los datos en cinta desde la Consola de Arcserve UDP. Se tiene que restaurar los datos desde el Gestor de Arcserve Backup. Para obtener más información sobre cómo restaurar los datos en cinta, consulte Copia de seguridad y recuperación de datos de D2D/UDP en la Guía del administrador de Arcserve Backup.

Cómo crear y gestionar una máquina virtual instantánea en Microsoft Azure

La máquina virtual instantánea es compatible con la creación de una máquina virtual en Microsoft Azure instantáneamente. La máquina virtual instantánea en Microsoft Azure tiene las siguientes ventajas:

- Proporciona acceso inmediato a los datos y aplicaciones presentes en las sesiones de copia de seguridad de Arcserve UDP.
- Elimina el tiempo de reposo asociado a una restauración tradicional o conversión de la sesión de copia de seguridad a una máquina virtual.
- Proporciona una alternativa para crear una máquina virtual en la nube, en lugar de crear máquinas virtuales locales.

Se puede crear una máquina virtual instantánea desde las sesiones de copia de seguridad siguientes:

- Copia de seguridad de Linux basada en el agente
- Copia de seguridad sin agente basada en el host para la máquina virtual de Linux

Nota: Para seguir las prácticas recomendadas para una máquina instantánea en Microsoft Azure, consulte.Prácticas recomendadas.

¿Qué hacer a continuación?

- Revisión de los requisitos previos
- Creación de un plan de la máquina virtual instantánea en Microsoft Azure
- Gestión de un plan de la máquina virtual instantánea en Microsoft Azure

Revisión de los requisitos previos para una máquina virtual instantánea en Microsoft Azure

Complete los siguientes requisitos previos antes de crear una máquina virtual instantánea:

- Desde la Matriz de compatibilidad, verifique si la máquina virtual es compatible con Microsoft Azure y UDP.
- Adición de una cuenta de la nube de Microsoft Azure
- Compruebe que se dispone de al menos un servidor de puntos de recuperación en un equipo local, como el destino de la copia de seguridad.
- Compruebe que se dispone de al menos un servidor de puntos de recuperación en Microsoft Azure, como destino de la replicación.
- Compruebe que se dispone de al menos un servidor de copia de seguridad de Linux localmente, para la tarea de copia de seguridad.
- Compruebe que se dispone de al menos un servidor de copia de seguridad de Linux en Microsoft Azure, para la tarea de máquina virtual instantánea.
- Compruebe que se ha agregado una cuenta de Microsoft Azure.

Limitación

- NO se admiten equipos Linux con UEFI.
- NO se admiten equipos Linux con sistema de archivos Btrfs en varios discos.

Creación de una máquina virtual instantánea en Microsoft Azure

Para crear una máquina virtual instantánea en el plan de Microsoft Azure, se recomienda realizar una de las opciones siguientes:

- Realice la copia de seguridad del nodo local protegido en el almacén de datos de servidor de puntos de recuperación local y, a continuación, realice la replicación en el servidor de puntos de recuperación en Microsoft Azure. Para obtener información sobre cómo agregar un nodo, consulte Cómo agregar nodos a la Consola.
- Realice la copia de seguridad del nodo local protegido en la ubicación del recurso compartido CIFS (NFS) local y, a continuación, copie la ubicación del recurso compartido CIFS (NFS) en Microsoft Azure. Para obtener información sobre cómo realizar la copia de seguridad de un nodo protegido, consulte Cómo crear un plan de copia de seguridad en Linux.

Crear una máquina virtual instantánea implica los cinco pasos generales siguientes:

1. Abrir el asistente de máquina virtual instantánea
2. Seleccionar el punto de recuperación
3. Seleccionar la ubicación de la máquina virtual
4. Seleccionar el servidor de recuperación
5. Especificar los detalles de la máquina virtual instantánea
6. Enviar la tarea de la máquina virtual instantánea

Apertura del asistente de máquina virtual instantánea

Puede configurar y crear una máquina virtual instantánea desde el asistente de máquina virtual instantánea. Existen tres formas de abrir el asistente de máquina virtual instantánea:

- Desde Gestión de nodos
- Desde Gestión de destinos: Servidor de puntos de recuperación
- Desde Gestión de destino: Carpeta compartida

Abra el asistente desde la vista de gestión de nodos.

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.
3. Se muestran todos los nodos en el panel central.
4. Haga clic con el botón secundario del ratón en un nodo y seleccione **Crear una máquina virtual instantánea**.

   Aparecerá el asistente de máquina virtual instantánea.

   Nota: Si un nodo no está asociado a ningún plan, no tendrá la opción **Crear una máquina virtual instantánea**.

Abra el asistente en la vista de gestión del destino

Desde Destinos: Servidor de puntos de recuperación

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Si se han agregado almacenes de datos, estos almacenes se mostrarán en el panel central.
3. Haga clic en el almacén de datos.

   Si ya ha realizado la copia de seguridad de los datos en el servidor de puntos de recuperación, en el panel se mostrarán todos los nodos de origen.
4. Haga clic con el botón secundario del ratón en un nodo y seleccione **Crear una máquina virtual instantánea**.

   Aparecerá el asistente de máquina virtual instantánea.

Desde Destinos: Carpeta compartida

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Carpetas compartidas**.

3. Si se han agregado carpetas compartidas, se mostrarán en el panel central.
4. Haga clic en una carpeta compartida y seleccione **Explorar puntos de recuperación**.

   Si ya ha realizado la copia de seguridad de los datos en la carpeta compartida, se muestran todos los nodos de origen en el panel.
5. Haga clic con el botón secundario del ratón en un nodo y seleccione **Crear una máquina virtual instantánea**.

   Aparecerá el asistente de máquina virtual instantánea.

Selección de un punto de recuperación

En la página Seleccionar un punto de recuperación se muestra la ubicación del punto de recuperación y se puede seleccionar uno. El punto de recuperación puede encontrarse en una ubicación compartida o un almacén de datos del servidor de puntos de recuperación.

La Consola reconoce automáticamente la ubicación del punto de recuperación y realiza una selección previa de los valores para los campos **Tipo de ubicación**, **Servidor de puntos de recuperación** y **Almacén de datos** o **Carpeta de recursos compartidos de red**.

Nota: Seleccione la sesión del servidor de puntos de recuperación (carpeta compartida) como destino de la replicación para ahorrar tiempo y ancho de banda de red.

Amplíe la lista Fecha, seleccione el punto de recuperación requerido en ella y haga clic en **Siguiente**.

Aparecerá la página **Ubicación de la máquina virtual**.

Nota: Si crea una máquina virtual instantánea desde la vista de gestión de nodos, se muestran únicamente los servidores de puntos de recuperación que se encuentran en el mismo sitio que el nodo de origen. Si desea crear una máquina virtual instantánea a partir del servidor de puntos de recuperación gestionado desde un sitio distinto, vaya a ese sitio y abra el asistente en la vista de gestión del destino.

Selección de la ubicación de una máquina virtual

Especifique la ubicación de la máquina virtual donde desea crear la máquina virtual instantánea.

Siga estos pasos:

1. Seleccione Microsoft Azure.
2. Seleccione un nombre de cuenta.

   Nota: Seleccione una cuenta correspondiente, y si no se ha agregado, consulte la sección Adición de una cuenta de la nube de Microsoft Azure.
3. Haga clic en **Siguiente**.

   Se abrirá la página **Servidor de recuperación**.

Selección de un servidor de recuperación

El servidor de recuperación aloja el módulo de núcleo de la máquina virtual instantánea. El servidor de recuperación predeterminado es el servidor de puntos de recuperación. También se puede asignar un nodo como servidor de recuperación.

Para las sesiones de copia de seguridad de Linux, el servidor de recuperación es un servidor de copia de seguridad de Linux.

Siga estos pasos:

1. Seleccione el servidor de copia de seguridad de Linux en la lista desplegable.

   Notas: Seleccione la sesión del servidor de puntos de recuperación (carpeta compartida) como destino de la replicación para ahorrar tiempo y ancho de banda de red.

2. Haga clic en **Siguiente**.

   Aparecerá la página de detalles de la máquina virtual instantánea.

   Nota: Asegúrese de que ha seleccionado el servidor de puntos de recuperación que se encuentra en Microsoft Azure.

Especificar los detalles de la máquina virtual instantánea

Especifique los detalles de la máquina virtual instantánea.

Siga estos pasos:

1. Especifique el nombre y la descripción de la máquina virtual instantánea.

Nombre de VM

Especifica el nombre de la máquina virtual instantánea. El nombre del prefijo del nodo de origen con UDPIVM_ se convierte en el nombre predeterminado de la máquina virtual instantánea. Se puede modificar el nombre. Algunos caracteres especiales como, por ejemplo, ' @', \, etc, no se admiten en el nombre.

Descripción

(Opcional) Especifica la descripción de la máquina virtual instantánea.

Ubicación

Especifica la ubicación de la cuenta de Microsoft Azure.

Tipo de disco

Especifica el tipo de disco.

Tamaño de la máquina virtual de Azure

Especifica el tamaño de la máquina virtual compatible.

Red

Especifica la red existente en la cuenta de Microsoft Azure.

Subred

Especifica la subred existente en la cuenta de Microsoft Azure.

Asignar automática la dirección IP pública

Especifica la dirección IP pública asignada a la máquina virtual. .

Dirección IP primaria

Especifica la dirección IP primaria de la máquina virtual. Se especifica de forma automática, si el usuario no la especifica.

Seleccione un grupo de seguridad

Especifica el grupo de seguridad. Se pueden seleccionar varios grupos. Si el usuario no realiza una selección, se crea automáticamente un nuevo grupo de seguridad.

Avance: Cambiar el nombre de host

Especifica el nombre de host de la nueva máquina virtual.

Avance: Recuperar los datos automáticamente después de iniciar la máquina virtual instantánea

Especifica si la recuperación de datos se realiza automáticamente después de crear la máquina virtual instantánea.

2. Haga clic en **Finalizar**.

   Ahora se puede enviar la tarea.

Envíe la tarea de máquina virtual instantánea.

Para crear la máquina virtual instantánea, envíe la tarea de máquina virtual instantánea. Una vez finalizada la tarea, se puede ver la máquina virtual instantánea en **Recursos**, **Infraestructura**, **Máquina virtual instantánea**.

Siga estos pasos:

1. Haga clic en **Crear máquina virtual**.

   Se abre el cuadro de diálogo **Crear máquina virtual**.

2. Seleccione una de las opciones siguientes:

   Iniciar ahora

   Envía una tarea para crear la máquina virtual instantánea. Cuando se ha creado la máquina virtual, se inicia automáticamente.

   Iniciar más tarde

   Crea una máquina virtual instantánea. Deberá iniciar manualmente la máquina virtual. Una vez finalizada la tarea de máquina virtual instantánea, se puede iniciar la máquina virtual.

   Cancelar

   Cierra el cuadro de diálogo Crear máquina virtual sin crear ninguna máquina virtual. Se vuelve a la página de creación de máquina virtual.

   Se ha creado correctamente la tarea de máquina virtual instantánea.

Gestión de una máquina virtual instantánea

La máquina virtual instantánea se puede gestionar desde la consola. Se puede encender o apagar una máquina virtual instantánea desde la consola. Además, se puede suprimir cualquier máquina virtual instantánea.

Nota: La Consola muestra únicamente las máquinas virtuales instantáneas que se crean a partir de los puntos de recuperación gestionados desde el sitio seleccionado.

- Inicio o detención de una máquina virtual instantánea
- Supresión de una máquina virtual instantánea

Iniciar o detener una máquina virtual instantánea

Se puede iniciar o detener una máquina virtual instantánea después de crearla. El botón de inicio o detención se muestra dependiendo del estado de la máquina virtual.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructuras** y haga clic en **Máquina virtual instantánea**.
3. Seleccione la máquina virtual en el panel central y haga clic en **Acciones**.
4. Seleccione **Encender** o **Apagar**en función del estado de la máquina virtual.

   La máquina virtual se inicia o se detiene correctamente.

Supresión de una máquina virtual instantánea

Se puede suprimir cualquier máquina virtual instantánea que ya no se necesite.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructuras** y haga clic en **Máquina virtual instantánea**.
3. Seleccione la máquina virtual en el panel central y haga clic en **Acciones**.
4. Haga clic en **Suprimir**.

   Aparecerá un diálogo de confirmación.
5. Haga clic en **Aceptar**.

   La máquina virtual se ha suprimido correctamente.

Cómo crear y gestionar una máquina virtual instantánea en servidores Hyper-V y servidores ESX VMware

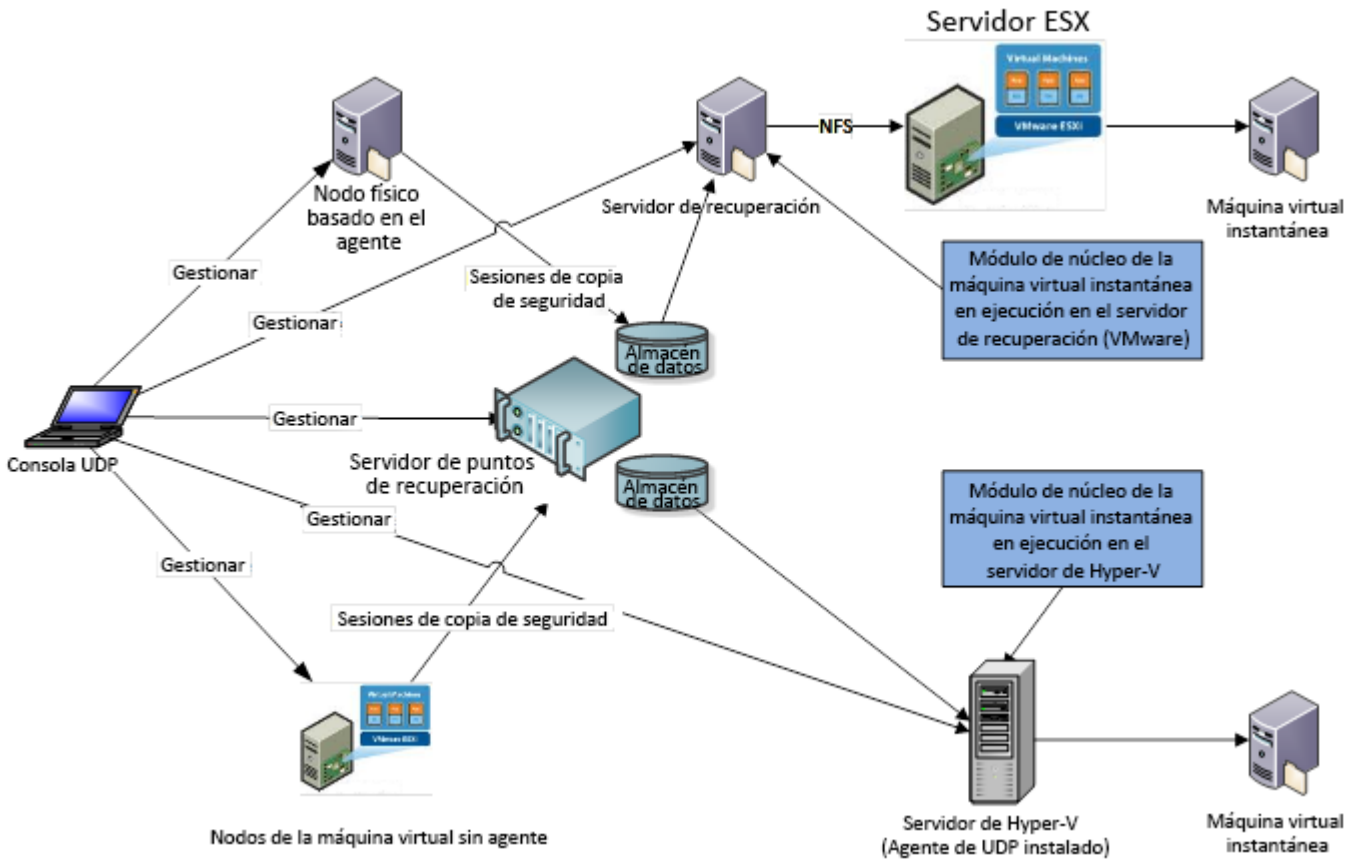
La máquina virtual instantánea crea una máquina virtual en el hipervisor y ejecuta la sesión de copia de seguridad dentro de la máquina virtual sin ninguna conversión anterior. La ventaja de una máquina virtual instantánea es que proporciona un acceso inmediato a los datos y aplicaciones presentes en las sesiones de copia de seguridad de Arcserve UDP. Una máquina virtual instantánea elimina el tiempo de reposo asociado a una restauración tradicional o conversión de la sesión de copia de seguridad a una máquina física o virtual.

Se puede crear una máquina virtual instantánea desde las sesiones de copia de seguridad siguientes:

- Copia de seguridad de Windows basada en el agente
- Copia de seguridad de Linux basada en el agente
- Copia de seguridad sin agente y basada en el host

Como hipervisor se puede seleccionar un servidor de vCenter/ESX(i) de VMware o un servidor de Windows Hyper-V.

El diagrama siguiente explica la arquitectura de una máquina virtual instantánea:



¿Qué hacer a continuación?

- Revisión de los requisitos previos para una máquina virtual instantánea
- Creación de una máquina virtual instantánea
- Gestión de una máquina virtual instantánea

Revisión de los requisitos previos para una máquina virtual instantánea

Complete los siguientes requisitos previos antes de crear una máquina virtual instantánea:

- Asegúrese de tener por lo menos una copia de seguridad de Arcserve UDP.
- Verifique que los agentes de Arcserve UDP ya estén instalados en el servidor de recuperación.
- Compruebe que la función NFS esté instalada en el servidor de recuperación si el hipervisor de destino es un servidor de vCenter/ESX(i) de VMware.
- Verifique que el sistema operativo del servidor de recuperación sea Windows Server 2008 R2 de 64 bits o posterior.
- Compruebe que el servidor de recuperación tenga suficiente espacio para la máquina virtual instantánea.
- Compruebe si se tienen los permisos mínimos para realizar las tareas de máquina virtual instantánea necesarias. Para obtener más información, consulte Permisos mínimos de VMware necesarios para las tareas de IVM.

Nota: El equipo se puede iniciar. Las tarjetas NIC se configuran de acuerdo con la entrada del usuario en la interfaz de usuario.

Consideraciones

- La función de migración de una máquina virtual instantánea entre nodos no es compatible cuando se inicia una máquina virtual instantánea en un clúster de Hyper-V.
- Cuando se crea una máquina virtual instantánea desde una copia de seguridad del agente de Linux, no se pueden modificar los valores de configuración de una máquina virtual creada por la máquina virtual instantánea mediante un cliente de vSphere. Se debe utilizar el cliente web de vSphere para modificar los valores de configuración de la máquina virtual.
- Si el número de almacén de datos de NFS alcanza el número máximo de montajes de NFS en un host de ESX/ESXi y se crea una máquina virtual instantánea, se produce un error en Arcserve UDP al crear el almacén de datos de NFS. Para aumentar el número máximo de montajes de NFS en el host de ESX/ESXi, consulte el artículo de la base de conocimiento de VMware.
- Si el punto de recuperación es de la copia de seguridad sin agente y el hipervisor de destino es vSphere ESX/VC, se requiere el servidor de NFS en el equipo del servidor de copia de seguridad de Linux.

- Si el hipervisor de destino es MS Hyper-V, el comando net debe estar disponible en el servidor de copia de seguridad de Linux. Los paquetes del cliente samba pueden instalar este comando.
- La máquina virtual no funciona en las situaciones siguientes:
  - Reinicios del servidor de recuperación.
  - Bloqueos del servidor de recuperación.
  - Desconexión de la conexión de red entre el servidor de recuperación y el destino de la copia de seguridad (almacén de datos o carpeta de recursos compartidos).

Permisos mínimos de VMware necesarios para las tareas de IVM

La tabla muestra la lista de permisos mínimos de VMware necesarios para realizar todas las tareas de máquina virtual instantánea.

Nota: Los permisos globales se establecen en el nivel de vCenter.

Tareas	Permiso
Almacén de datos	Allocate space
Global	Desactivar métodos
	Activar métodos
	Licencias
Host > Configuración	Configuración de la partición de alma-cenamiento
Red	Asignar red
Recurso	Asignar la máquina virtual a la agrupación de recursos
Máquina virtual > Configuración	Agregar disco existente
	Avanzado
Máquina virtual > Interacción	Apagar
	Encender
	Restablecer
	Interacción de la consola
Máquina virtual > Inventario	Crear nuevo
	Eliminar
Máquina virtual > Aprovisionamiento	Permitir el acceso de disco
	Permitir el acceso de solo lectura al disco
	Permitir la descarga de la máquina virtual
Máquina virtual > Gestión de las ins-tantáneas	Crear instantáneas
	Eliminar instantáneas
	Revertir a instantánea
Máquina virtual > Guest Operations	Guest Operation Queries

Creación de una máquina virtual instantánea

Crear una máquina virtual instantánea implica los cinco pasos generales siguientes:

1. Abrir el asistente de máquina virtual instantánea
2. Selección de un punto de recuperación
3. Especificar la ubicación de la máquina virtual
4. Especificar el servidor de recuperación
5. Especificar los detalles de la máquina virtual instantánea
6. Enviar la tarea de la máquina virtual instantánea

Si la tarea finaliza correctamente, se crea una máquina virtual instantánea.

Apertura del asistente de máquina virtual instantánea

Puede configurar y crear una máquina virtual instantánea desde el asistente de máquina virtual instantánea. Existen tres formas de abrir el asistente de máquina virtual instantánea:

- Desde la gestión de nodos
- Desde la gestión del destinos: Servidor de puntos de recuperación
- Desde la gestión del destinos: Carpeta compartida

Abra el asistente desde la vista de gestión de nodos.

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.
3. Se muestran todos los nodos en el panel central.
4. Haga clic con el botón secundario del ratón en un nodo y seleccione **Crear una máquina virtual instantánea**.

   Aparecerá asistente de máquina virtual instantánea.

   Nota: Si un nodo no se asocia a ningún plan, no aparecerá la opción **Crear una máquina virtual instantánea**.

Abra el asistente en la vista de gestión del destino

Desde destinos: Servidor de punto de recuperación

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Si se han agregado almacenes de datos, estos almacenes se mostrarán en el panel central.
3. Haga clic en el almacén de datos.

   Si ya ha realizado la copia de seguridad de los datos en el servidor de puntos de recuperación, en el panel se mostrarán todos los nodos de origen.
4. Haga clic con el botón secundario del ratón en un nodo y seleccione **Crear una máquina virtual instantánea**.

   Aparecerá asistente de máquina virtual instantánea.

Desde destinos: Carpeta compartida

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Carpetas compartidas**.

3. Si se han agregado carpetas compartidas, se mostrarán en el panel central.
4. Haga clic en una carpeta compartida y seleccione **Explorar puntos de recuperación**.

   Si ya ha realizado la copia de seguridad de los datos en la carpeta compartida, se muestran todos los nodos de origen en el panel.
5. Haga clic con el botón secundario del ratón en un nodo y seleccione **Crear una máquina virtual instantánea**.

   Aparecerá asistente de máquina virtual instantánea.

Selección de un punto de recuperación

En la página Seleccionar un punto de recuperación se muestra la ubicación del punto de recuperación y se puede seleccionar uno. El punto de recuperación puede encontrarse en una ubicación compartida o un almacén de datos del servidor de puntos de recuperación.

La Consola reconoce automáticamente la ubicación del punto de recuperación y realiza una selección previa de los valores para los campos **Tipo de ubicación**, **Servidor de puntos de recuperación** y **Almacén de datos** o **Carpeta de recursos compartidos de red**.

Amplíe la lista Fecha, seleccione el punto de recuperación requerido en ella y haga clic en **Siguiente**.

Aparecerá la página **Ubicación de la máquina virtual**.

Nota: Si crea una máquina virtual instantánea desde la vista de gestión de nodos, se muestran únicamente los servidores de puntos de recuperación que se encuentran en el mismo sitio que el nodo de origen. Si desea crear una máquina virtual instantánea a partir del servidor de puntos de recuperación gestionado desde un sitio distinto, vaya a ese sitio y abra el asistente en la vista de gestión del destino.

Selección de la ubicación de una máquina virtual

Especifique la ubicación de la máquina virtual donde desea crear la máquina virtual instantánea. Puede especificar una máquina virtual de VMware o de Microsoft Hyper-V.

Siga estos pasos:

1. Seleccione un tipo de hipervisor.

   VMware vSphere

   a. Seleccione **VMware vSphere**.

   b. Si ya se ha agregado un nodo de VMware al sitio seleccionado en la Consola, seleccione dicho nodo en la lista desplegable **Host**.

   c. Si no ha agregado ningún nodo de VMware, en la lista desplegable Host, haga clic en **+ Agregar nuevo hipervisor**.

      Aparecerá el cuadro de diálogo Agregar hipervisor.

   d. Especifique los detalles del servidor VMware, vCenter o ESX(i) y haga clic en **Aceptar**.

      El cuadro de diálogo Agregar hipervisor se cierra y se vuelve a ver la página **Ubicación de la máquina virtual**. Todos los ESX(i) o todas las agrupaciones de recursos se muestran en el panel central.

   e. Seleccione el ESX(i), el clúster, la agrupación de recursos o la aplicación virtual como la ubicación.

   Se especifica el equipo VMware vSphere.

   Microsoft Hyper-V

   a. Seleccione **Microsoft Hyper-V**.

   b. Si ya se ha agregado un nodo de Hyper-V al sitio seleccionado en la Consola, seleccione dicho nodo en la lista desplegable **Servidor/clúster de Hyper-V**.

   c. Si no se ha agregado ningún nodo de Hyper-V, haga clic en **Agregar**.

      Se abrirá el cuadro de diálogo **Especificar el destino de la máquina virtual**.

      Nota: Cuando se conecta a la máquina virtual instantánea de Hyper-V mediante una cuenta de administrador local no integrada, el UAC remoto debe estar desactivado. Para obtener más información acerca de cómo desactivar el UAC remoto para los administradores no integrados, consulte Cómo desactivar un UAC remoto para un administrador no integrado.

   d. Especifique los detalles del servidor Hyper-V y haga clic en **Aceptar**.

Se especifica la máquina virtual de Hyper-V.

Nota: El asistente de la máquina virtual instantánea no puede instalar el servicio de integración en máquinas virtuales instantáneas con Microsoft Hyper-V 2016 si el nodo de origen es Windows 2008 o anterior.

2. Haga clic en **Siguiente**.

   Se abrirá la página **Servidor de recuperación**.

Cómo desactivar un UAC remoto para un administrador no integrado

La cuenta administrativa adicional hace referencia a esas cuentas que no son administradores predeterminados. También se hace referencia a tales cuentas como cuentas administrativas no integradas. Para importar una máquina virtual de un host de Hyper-V, se puede utilizar la cuenta del administrador integrada del host de Hyper-V o una cuenta del dominio que está en el grupo de administradores local del host de Hyper-V o un usuario administrativo no integrado.

El usuario con la cuenta administrativa adicional puede utilizar los procedimientos para desactivar el acceso remoto del UAC.

Notas:

- Este procedimiento no es similar a la desactivación del UAC. Mediante este procedimiento, se pueden desactivar algunas de las funciones del UAC.
- Teniendo en cuenta que se utiliza la tecnología del servicio remoto Instrumental de administración de Windows (WMI) para importar, asegúrese de que el cortafuegos no bloquea el WMI.

Siga estos pasos:

1. Haga clic en Inicio, escriba *regedit* en el campo Buscar programas y archivos, y pulse Intro.

   Se abre el Editor del registro de Windows.

   Nota: Puede ser necesario proporcionar credenciales administrativas para poder abrir el Editor del registro de Windows.

2. Busque y haga clic en la clave de registro siguiente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. En el menú Editar, haga clic en Nuevo y luego en Valor de DWORD (32 bits).
4. Especifique *LocalAccountTokenFilterPolicy* como el nombre de la entrada nueva y pulse Intro.
5. Haga clic con el botón secundario del ratón en *LocalAccountTokenFilterPolicy* y haga clic en Modificar.
6. Especifique 1 en el campo de datos Valores y, a continuación, haga clic en Aceptar.
7. Salga del Editor del registro.

   Para obtener más información sobre el comportamiento de Windows, consulte la documentación de Microsoft.

Selección de un servidor de recuperación

El servidor de recuperación aloja el módulo de núcleo de la máquina virtual instantánea. El servidor de recuperación predeterminado es el servidor de puntos de recuperación. También se puede asignar un nodo como servidor de recuperación.

Para las sesiones de copia de seguridad de Linux, el servidor de recuperación es un servidor de copia de seguridad de Linux.

Siga estos pasos:

1. Seleccione uno de los siguientes como servidor de recuperación:

   Uso del servidor de puntos de recuperación

   Especifica que el servidor de puntos de recuperación se utilice como servidor de recuperación.

   Selección de un nodo de Windows de la lista de nodos

   Especifica que el servidor de recuperación es un nodo de Windows. Se puede seleccionar el nodo de la lista. Solo se muestran los nodos que gestione el sitio seleccionado.

   Notas:

   - Debe seleccionar un servidor de recuperación solo cuando el hipervisor sea VMware vSphere.
   - En estos casos, debe instalarse el rol de Network File System (NFS) de Windows en el servidor de puntos de recuperación. Se puede instalar automáticamente a través del proceso de la máquina virtual instantánea. Para instalarlo de forma manual, consulte Cómo instalar el sistema de archivos de red en Windows Server.
   - Si Arcserve Backup está instalado en el servidor de recuperación, es posible que el servicio de sistema de archivos de red (NFS) de Windows no se inicie. Se debe a que el número de puerto predeterminado del servicio NFS de Windows es 111, que es el que utiliza el servicio **Servidor de llamada a procedimiento remoto** de Arcserve Backup. Para cambiar el número de puerto predeterminado del servicio **Servidor de llamada a procedimiento remoto** de Arcserve Backup, consulte Modificación del archivo de configuración de puertos y Puertos de comunicación del servidor primario y del servidor miembro en la documentación de Arcserve Backup.

2. Haga clic en **Siguiente**.

   Aparecerá la página de detalles de la máquina virtual instantánea.

Cómo instalar manualmente el sistema de archivos de red en Windows Server

Se puede instalar manualmente el sistema de archivos de red (NFS) en Windows Server mediante el gestor del servidor.

Siga estos pasos:

1. Abra el gestor de servidores, haga clic en Gestionar y seleccione el asistente para agregar roles y funciones.

   Aparecerá el asistente para agregar roles y funciones.
2. Haga clic en Roles de servidor y seleccione *Servicios de archivo y almacenamiento*.
3. Expanda *Servicios de archivos e iSCSI*.
4. Seleccione el *servidor de archivos* y el *servidor para NFS*.
5. Haga clic en Agregar funciones para incluir las funciones de NFS seleccionadas.
6. Haga clic en Instalar para instalar los componentes de NFS en el servidor.

   Se ha instalado manualmente el sistema de archivos de red en Windows Server.

Especificación de los detalles de la máquina virtual instantánea

Especifique los detalles de la máquina virtual instantánea. Las opciones pueden variar según el hipervisor.

Siga estos pasos:

1. Especifique el nombre y la descripción de la máquina virtual instantánea.

   Nombre de VM

   Especifica el nombre de la máquina virtual instantánea. El nombre del nodo de origen con un prefijo es el nombre predeterminado de la máquina virtual instantánea. No se permiten algunos caracteres especiales en el nombre como, por ejemplo, @, \, etc.

   Descripción

   (Opcional) Especifica la descripción de la máquina virtual instantánea.

2. Especifique la ubicación de la carpeta de la máquina virtual instantánea en el servidor de recuperación.

   Se puede explorar la información sobre el volumen del servidor de recuperación.

   Nota: Si se selecciona **VMware vSphere** como la ubicación de la máquina virtual, la carpeta seleccionada se monta como un almacén de datos de NFS en VMware. Aparecerá un icono compartido en esta carpeta en el equipo local. De forma predeterminada, el almacén de datos de NFS se monta en la misma ubicación de carpeta y solo se puede desmontar manualmente desde el servidor VMware ESX(i).

3. Especifique la configuración de la máquina virtual instantánea.

   Número de CPU

   Especifica el número de CPU que se necesitaría en la máquina virtual instantánea.

   Tamaño de memoria

   Especifica el tamaño de memoria que se necesitaría en la máquina virtual instantánea.

4. Agregue adaptadores de red.

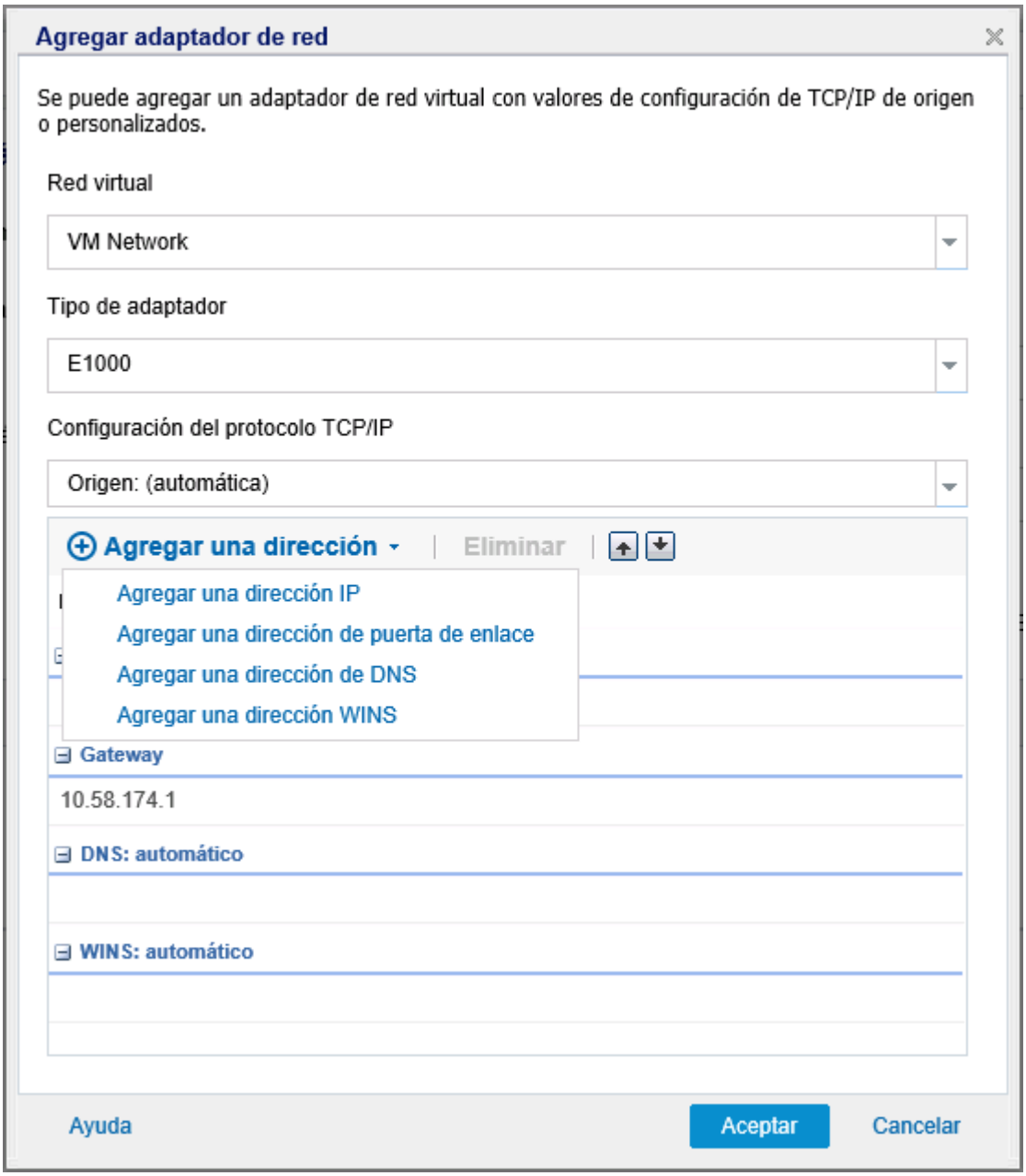
   Nota: Para una máquina virtual instantánea de Linux, se puede utilizar al menos una tarjeta NIC virtual para conectarse al servidor de copia de seguridad de Linux.

a. Haga clic en el botón **Agregar un adaptador** para agregar un adaptador y especificar los detalles de la red.



Se pueden agregar varios adaptadores de red. Después de agregar un adaptador de red, se puede modificar y suprimir el adaptador de red en la columna **Acciones**.

b. Especifique los valores de los campos **Red virtual**, **Tipo de adaptador** y **Configuración de TCP/IP**. Si se desea especificar la dirección IP de la máquina virtual instantánea, se puede hacer clic en **Agregar una dirección** y seleccionar la dirección que se desea configurar.



5. Actualizar DNS.

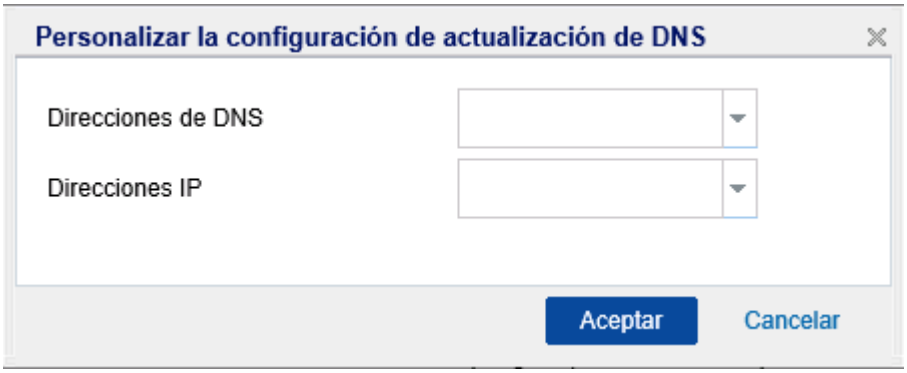
   Nota: Esta función solo está disponible para la máquina virtual instantánea de Windows.

   a. Haga clic en el botón **Actualizar DNS** para especificar los detalles de DNS.



Nota: Se puede especificar la información detallada de la herramienta Actualizar DNS si se ha especificado una dirección IP y una dirección DNS en el adaptador de red y el equipo de origen está en un dominio.

b. Haga clic en **Agregar una dirección DNS** para agregar un registro de actualización de DNS. Haga clic en **Eliminar** para eliminar el registro de actualización de DNS. Haga clic en los botones Arriba y Abajo para ajustar la secuencia de los registros.



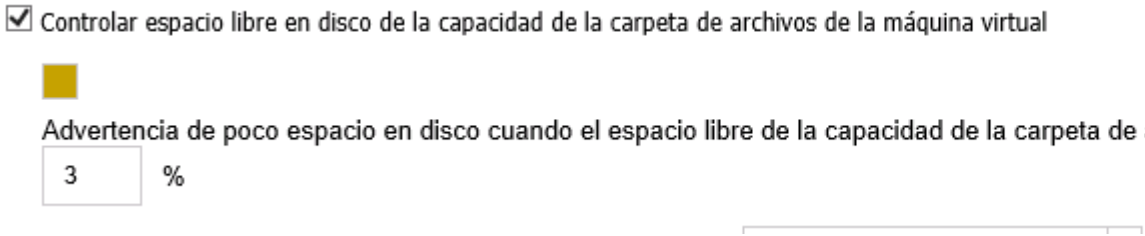
c. Seleccione una dirección de DNS y una dirección IP en la lista desplegable y, a continuación, haga clic en **Aceptar**.

d. Especifique el **Período de vida** (TTL).

e. Especifique la Autenticación de DNS.

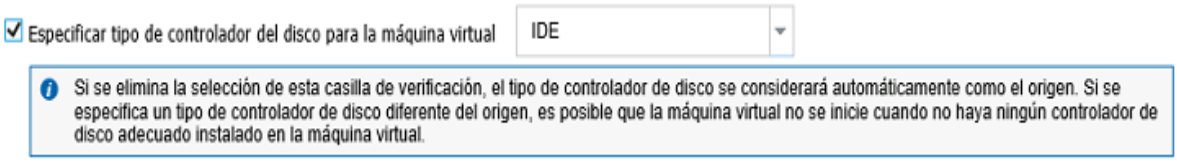
Para Microsoft DNS Server, introduzca el nombre de usuario y la contraseña. Para Servidor BIND, es necesario especificar la ruta completa, incluido el nombre de archivo del archivo de claves en el servidor de recuperación.

6. Compruebe el espacio libre en disco de la capacidad de la carpeta de archivos de la máquina virtual.



Nota: La casilla de verificación **Controlar espacio libre en disco de la capacidad de la carpeta de archivos de la máquina virtual** está activada de forma predeterminada. La barra de capacidad aparece en amarillo en la página de las máquinas virtuales instantáneas si el espacio libre de la capacidad de la carpeta de archivos de la máquina virtual es menor que el valor del umbral. El valor predeterminado del umbral es 3 %. Se puede cambiar el valor, si es necesario.

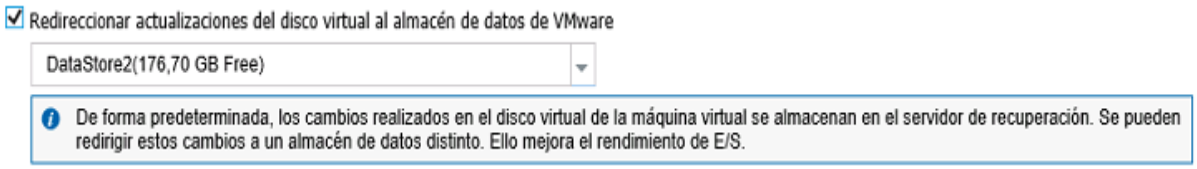
7. Seleccione la casilla de verificación **Especificar el tipo de controlador de disco para la máquina virtual** y seleccione el tipo de controlador de disco para la máquina virtual en la lista desplegable.



Nota: La casilla de verificación **Especificar el tipo de controlador de disco para la máquina virtual** está disponible si se ha seleccionado la casilla de verificación **VMware vSphere** como la ubicación de la máquina virtual.

Se crea la máquina virtual instantánea aplicando el controlador de disco especificado en VMware.

8. Para volver a dirigir las actualizaciones del disco virtual al almacén de datos de VMware, siga estos pasos:
   a. Seleccione la casilla de verificación **Redirigir las actualizaciones del disco virtual al almacén de datos de VMware**.

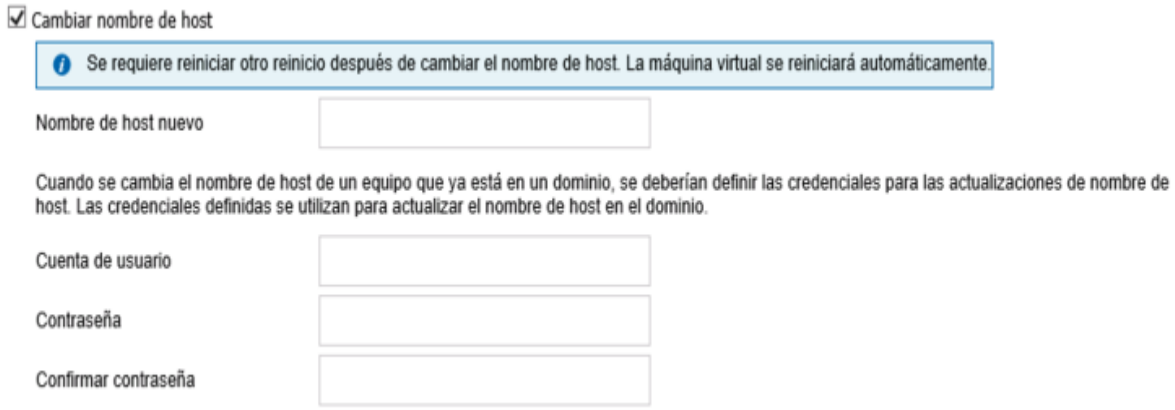


Nota: La casilla de verificación **Redirigir las actualizaciones del disco virtual al almacén de datos de VMware** está disponible si se ha seleccionado la casilla de verificación **VMware vSphere** como ubicación de la máquina virtual.

   b. Seleccione el almacén de datos necesario de VMware en la lista desplegable.

Las actualizaciones del disco virtual se redirigen al almacén de datos seleccionado de VMware.

9. Para cambiar el nombre de host de la máquina virtual instantánea, siga estos pasos:
   a. Haga clic en la casilla de verificación **Cambiar nombre de host** para actualizar el nombre de host de la máquina virtual instantánea.



b. Especifique un nuevo nombre de host para la máquina virtual instantánea. Si el equipo de origen está en un dominio, proporcione la cuenta del usuario y la contraseña.

Nota: Si el equipo de origen está en un dominio, la cuenta debe disponer de los permisos para cambiar el nombre de host en el dominio.

10. (Opcional) Para la **máquina virtual instantánea de Linux**, seleccione la opción **Recuperar los datos automáticamente después de iniciar la máquina virtual instantánea** para activar la recuperación automática de los datos cuando se inicia el destino de la máquina virtual instantánea.

    El comportamiento predeterminado de la **máquina virtual instantánea de Linux** es recuperar primero los datos necesarios e iniciar la máquina virtual. Si no se selecciona la opción, cuando se inicia la máquina virtual los datos restantes no se recuperarán incluso si se utiliza una máquina virtual normal. Si la opción está activada, los datos restantes se recuperan en el servidor back-end cuando se utiliza la máquina virtual. También puede preservar el destino de la máquina virtual instantánea de forma permanente cuando haya finalizado la recuperación de datos.

    Nota: Cuando el estado del destino de la máquina virtual instantánea de Linux es Apagado, se produce un error en la tarea de máquina virtual instantánea. Si ese punto de recuperación se combina, se produce un error en la máquina virtual instantánea de Linux al encenderse.

    Ahora se puede enviar la tarea.

Envíe la tarea de máquina virtual instantánea.

Para crear la máquina virtual instantánea, envíe la tarea de máquina virtual instantánea. Una vez finalizada la tarea, se puede ver la máquina virtual instantánea en **Recursos**, **Infraestructura**, **Máquina virtual instantánea**.

Siga estos pasos:

1. Haga clic en **Finalizar**.

   Se abre el cuadro de diálogo **Arrancar máquina virtual**.

2. Seleccione una de las opciones siguientes:

   Iniciar ahora

   Envía una tarea para crear la máquina virtual instantánea. Cuando se ha creado la máquina virtual, se inicia automáticamente.

   Iniciar más tarde

   Crea una máquina virtual instantánea. Deberá iniciar manualmente la máquina virtual. Una vez finalizada la tarea de máquina virtual instantánea, se puede iniciar la máquina virtual.

   Cancelar

   Cierra el cuadro de diálogo Crear máquina virtual sin crear ninguna máquina virtual. Se vuelve a la página de creación de máquina virtual.

   Se ha creado correctamente la tarea de máquina virtual instantánea.

Gestionar máquina virtual instantánea

La máquina virtual instantánea se puede gestionar desde la consola. Se puede encender o apagar una máquina virtual instantánea desde la consola. Además, se puede suprimir cualquier máquina virtual instantánea.

Nota: La Consola muestra únicamente las máquinas virtuales instantáneas que se creen a partir de los puntos de recuperación gestionados en el sitio seleccionado.

- Iniciar o detener una máquina virtual instantánea
- Reinicio de una máquina virtual instantánea
- Supresión de una máquina virtual instantánea
- Conversión de la máquina virtual instantánea de Linux en una máquina virtual independiente
- Migración de la máquina virtual instantánea de Linux en una máquina física

Iniciar o detener una máquina virtual instantánea

Se puede iniciar o detener una máquina virtual instantánea después de crearla. El botón de inicio o detención se muestra dependiendo del estado de la máquina virtual.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructuras** y haga clic en **Máquina virtual instantánea**.
3. Seleccione la máquina virtual en el panel central y haga clic en **Acciones**.
4. Seleccione **Encender** o **Apagar**en función del estado de la máquina virtual.

   La máquina virtual se inicia o se detiene correctamente.

Reinicio de una máquina virtual instantánea

Se puede reiniciar una máquina virtual instantánea después de crearla.

Nota: Se puede reiniciar una máquina virtual instantánea solo si se encuentra en el estado **Incorrecto** o **Bloqueo de la tarea**.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructura** y haga clic en **Máquinas virtuales instantáneas**.
3. Seleccione la máquina virtual con el estado **Incorrecto** o **Bloqueo de la tarea** en el panel central y haga clic en **Acciones**.
4. Haga clic en **Reiniciar**.

   Se reinicia la máquina virtual.

Supresión de una máquina virtual instantánea

Se puede suprimir cualquier máquina virtual instantánea que ya no se necesite.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructuras** y haga clic en **Máquina virtual instantánea**.
3. Seleccione la máquina virtual en el panel central y haga clic en **Acciones**.
4. Haga clic en **Suprimir**.

   Aparecerá un diálogo de confirmación.
5. Haga clic en **Aceptar**.

   La máquina virtual se ha suprimido correctamente.

Conversión de la máquina virtual instantánea de Linux en una máquina virtual independiente

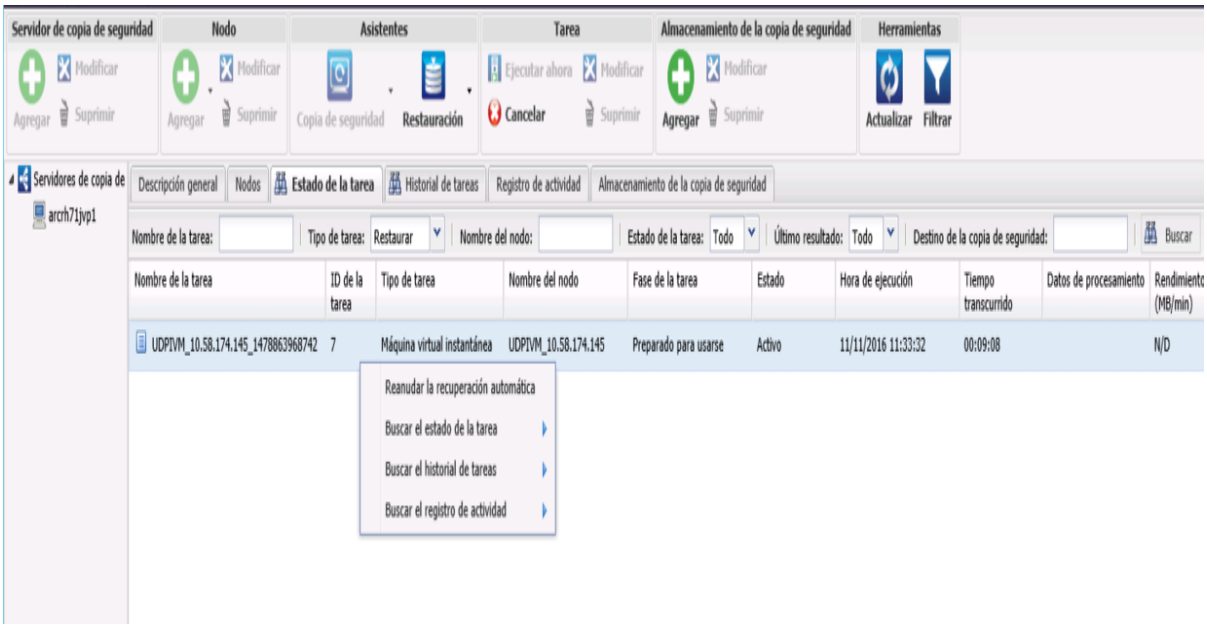
Se puede cambiar una máquina virtual de Linux instantánea (IVM) a una máquina virtual independiente (VM).

Notas:

- Para continuar, se necesita un elemento del menú que está disponible solamente después de que la máquina virtual instantánea se haya ejecutado en la fase de tarea “Preparado para usarse”.
- El elemento del menú no estará disponible si el punto de recuperación es una copia de seguridad sin agente y el hipervisor de destino es vSphere ESX/VC. Es necesario utilizar VMware Storage vMotion para convertir la máquina virtual instantánea en una máquina virtual independiente.

Siga estos pasos:

1. Abra la interfaz de usuario del servidor de copia de seguridad de Linux.



2. En la ficha Estado de la tarea, seleccione la tarea de máquina virtual instantánea y haga clic con el botón secundario para abrir el menú contextual.
3. Seleccione Reanudar la recuperación automática.

   La tarea de máquina virtual instantánea se mueve al historial de tareas cuando el proceso finaliza correctamente.

Migración de la máquina virtual instantánea de Linux en una máquina física

Para migrar la máquina Virtual instantánea de Linux en una máquina física, consulte la sección **Cómo realizar una reconstrucción completa (BMR) de la migración para los equipos de Linux** en la *Guía del usuario del Agente para Linux*.

Cómo crear y gestionar una máquina virtual instantánea en Amazon EC2

La máquina virtual instantánea es compatible con la creación de una máquina virtual en Amazon EC2 instantáneamente. La máquina virtual instantánea en Amazon EC2 tiene las siguientes ventajas:

- Proporciona acceso inmediato a los datos y aplicaciones presentes en las sesiones de copia de seguridad de Arcserve UDP.
- Elimina el tiempo de reposo asociado a una restauración tradicional o conversión de la sesión de copia de seguridad a una máquina virtual.
- Proporciona una alternativa para crear una máquina virtual en la nube, en lugar de crear máquinas virtuales locales.

Se puede crear una máquina virtual instantánea desde las sesiones de copia de seguridad siguientes:

- Copia de seguridad de Linux basada en el agente
- Copia de seguridad sin agente basada en el host

¿Qué hacer a continuación?

- Revisión de los requisitos previos
- Creación de un plan de la máquina virtual instantánea en Amazon EC2
- Gestión de un plan de la máquina virtual instantánea en Amazon EC2

Se puede crear una máquina virtual instantánea a partir de las siguientes sesiones de copia de seguridad: al completar correctamente una tarea, se crea una máquina virtual instantánea en Amazon EC2.

Revisión de los requisitos previos para una máquina virtual instantánea en Amazon EC2

Complete los siguientes requisitos previos antes de crear una máquina virtual instantánea:

- Desde la Matriz de compatibilidad, verifique si la máquina virtual es compatible con Amazon EC2 y UDP.
- Compruebe que se dispone de al menos un servidor de puntos de recuperación en un equipo local, como destino de la copia de seguridad.
- Compruebe que se dispone de al menos un servidor de puntos de recuperación en Amazon EC2, como destino de la replicación.
- Compruebe que se dispone de al menos un servidor de copia de seguridad de Linux localmente, para la tarea de copia de seguridad.
- Compruebe que se dispone de al menos un servidor de copia de seguridad de Linux en Amazon EC2, para la tarea de máquina virtual instantánea.
- Compruebe que la cuenta de Amazon EC2 dispone de suficiente cuota de la instancia en ejecución para la máquina virtual instantánea.

Limitación

NO se admite la copia de seguridad de la máquina virtual de Windows sin agentes basada en el host ni la copia de seguridad de Windows basada en el agente.

Creación de un de la máquina virtual instantánea en Amazon EC2

Crear una máquina virtual instantánea implica los cinco pasos generales siguientes:

1. Abrir el asistente de máquina virtual instantánea
2. Seleccionar el punto de recuperación
3. Seleccionar la ubicación de la máquina virtual
4. Seleccionar el servidor de recuperación
5. Especificar los detalles de la máquina virtual instantánea
6. Enviar la tarea de la máquina virtual instantánea

Apertura del asistente de máquina virtual instantánea

Puede configurar y crear una máquina virtual instantánea desde el asistente de máquina virtual instantánea. Existen tres formas de abrir el asistente de máquina virtual instantánea:

- Desde la gestión de nodos
- Desde la gestión del destinos: Servidor de punto de recuperación
- Desde la gestión del destinos: Carpeta compartida

Abra el asistente desde la vista de gestión de nodos.

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.
3. Se muestran todos los nodos en el panel central.
4. Haga clic con el botón secundario del ratón en un nodo y seleccione **Crear una máquina virtual instantánea**.

   Aparecerá asistente de máquina virtual instantánea.

   Nota: Si un nodo no se asocia a ningún plan, no aparecerá la opción **Crear una máquina virtual instantánea**.

Abra el asistente en la vista de gestión del destino

Desde Destinos: Servidor de punto de recuperación

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Si se han agregado almacenes de datos, estos almacenes se mostrarán en el panel central.
3. Haga clic en el almacén de datos.

   Si ya ha realizado la copia de seguridad de los datos en el servidor de puntos de recuperación, en el panel se mostrarán todos los nodos de origen.
4. Haga clic con el botón secundario del ratón en un nodo y seleccione **Crear una máquina virtual instantánea**.

   Aparecerá asistente de máquina virtual instantánea.

Desde Destinos: Carpeta compartida

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Carpetas compartidas**.

3. Si se han agregado carpetas compartidas, se mostrarán en el panel central.
4. Haga clic en una carpeta compartida y seleccione **Explorar puntos de recuperación**.

   Si ya ha realizado la copia de seguridad de los datos en la carpeta compartida, se muestran todos los nodos de origen en el panel.
5. Haga clic con el botón secundario del ratón en un nodo y seleccione **Crear una máquina virtual instantánea**.

   Aparecerá asistente de máquina virtual instantánea.

Selección de un punto de recuperación

En la página Seleccionar un punto de recuperación se muestra la ubicación del punto de recuperación y se puede seleccionar uno. El punto de recuperación puede encontrarse en una ubicación compartida o un almacén de datos del servidor de puntos de recuperación.

La Consola reconoce automáticamente la ubicación del punto de recuperación y realiza una selección previa de los valores para los campos **Tipo de ubicación**, **Servidor de puntos de recuperación** y **Almacén de datos** o **Carpeta de recursos compartidos de red**.

Nota: Seleccione la sesión del servidor de puntos de recuperación (carpeta compartida) como destino de la replicación para ahorrar tiempo y ancho de banda de red.

Amplíe la lista Fecha, seleccione el punto de recuperación requerido en ella y haga clic en **Siguiente**.

Aparecerá la página **Ubicación de la máquina virtual**.

Nota: Si crea una máquina virtual instantánea desde la vista de gestión de nodos, se muestran únicamente los servidores de puntos de recuperación que se encuentran en el mismo sitio que el nodo de origen. Si desea crear una máquina virtual instantánea a partir del servidor de puntos de recuperación gestionado desde un sitio distinto, vaya a ese sitio y abra el asistente en la vista de gestión del destino.

Selección de la ubicación de una máquina virtual

Especifique la ubicación de la máquina virtual donde desea crear la máquina virtual instantánea. Se puede especificar Amazon EC2 o Amazon EC2 (China) según el tipo de cuenta.

Siga estos pasos:

1. Seleccione Amazon EC2 o Amazon EC2 (China).
2. Seleccione un nombre de cuenta.

   Nota: Seleccione una cuenta correspondiente, y si no se ha agregado, consulte la sección Adición de una cuenta de la nube.
3. Haga clic en **Siguiente**.

   Se abrirá la página **Servidor de recuperación**.

Selección de un servidor de recuperación

El servidor de recuperación hospeda el módulo de núcleo de la máquina virtual instantánea. El servidor de recuperación predeterminado es el servidor de puntos de recuperación. También se puede asignar un nodo como servidor de recuperación.

Para las sesiones de copia de seguridad de Linux, el servidor de recuperación es un servidor de copia de seguridad de Linux.

Siga estos pasos:

1. Seleccione el servidor de copia de seguridad de Linux en la lista desplegable.

   Notas: Seleccione la sesión del servidor de puntos de recuperación (carpeta compartida) como destino de la replicación para ahorrar tiempo y ancho de banda de red.

2. Haga clic en **Siguiente**.

   Aparecerá la página de detalles de la máquina virtual instantánea.

Especificar los detalles de la máquina virtual instantánea

Especifique los detalles de la máquina virtual instantánea.

Siga estos pasos:

1. Especifique el nombre y la descripción de la máquina virtual instantánea.

Nombre de máquina virtual

Especifica el nombre de la máquina virtual instantánea. El nombre del prefijo del nodo de origen con UDPIVM_ se convierte en el nombre predeterminado de la máquina virtual instantánea. Se puede modificar el nombre. Algunos caracteres especiales como, por ejemplo, ' @', \, etc, no se admiten en el nombre.

Descripción

(Opcional) Especifica la descripción de la máquina virtual instantánea.

Region

Especifica la región de la cuenta de Amazon EC2.

Tipo de instancia

Especifica el tipo de instancia compatible.

Tipo de volumen

Especifica el tipo de volumen.

Red

Especifica la red existente en la cuenta de Amazon EC2.

Subred

Especifica la subred existente en la cuenta de Amazon EC2.

Asignar automática la dirección IP pública

Especifica la dirección IP pública asignada a la máquina virtual. .

Dirección IP primaria

Especifica la dirección IP primaria de la máquina virtual. Se especifica de forma automática, si el usuario no la especifica.

Seleccione un grupo de seguridad

Especifica el grupo de seguridad. Se pueden seleccionar varios grupos. Si el usuario no realiza una selección, se crea automáticamente un nuevo grupo de seguridad.

Opciones avanzadas: Cambiar el nombre de host

Especifica el nombre de host de la nueva máquina virtual.

Opciones avanzadas: Recuperar los datos automáticamente después de iniciar la máquina virtual instantánea

Especifica si la recuperación de datos se realiza automáticamente después de crear la máquina virtual instantánea.

2. Haga clic en **Finalizar**.

   Ahora se puede enviar la tarea.

Envíe la tarea de máquina virtual instantánea.

Para crear la máquina virtual instantánea, envíe la tarea de máquina virtual instantánea. Una vez finalizada la tarea, se puede ver la máquina virtual instantánea en **Recursos**, **Infraestructura**, **Máquina virtual instantánea**.

Siga estos pasos:

1. Haga clic en **Crear máquina virtual**.

   Se abre el cuadro de diálogo **Crear máquina virtual**.

2. Seleccione una de las opciones siguientes:

   Iniciar ahora

   Envía una tarea para crear la máquina virtual instantánea. Cuando se ha creado la máquina virtual, se inicia automáticamente.

   Iniciar más tarde

   Crea una máquina virtual instantánea. Deberá iniciar manualmente la máquina virtual. Una vez finalizada la tarea de máquina virtual instantánea, se puede iniciar la máquina virtual.

   Cancelar

   Cierra el cuadro de diálogo Crear máquina virtual sin crear ninguna máquina virtual. Se vuelve a la página de creación de máquina virtual.

   Se ha creado correctamente la tarea de máquina virtual instantánea.

Gestión de una máquina virtual instantánea

La máquina virtual instantánea se puede gestionar desde la consola. Se puede encender o apagar una máquina virtual instantánea desde la consola. Además, se puede suprimir cualquier máquina virtual instantánea.

Nota: La Consola muestra únicamente las máquinas virtuales instantáneas que se crean a partir de los puntos de recuperación gestionados desde el sitio seleccionado.

- Inicio o detención de una máquina virtual instantánea
- Reinicio de una máquina virtual instantánea
- Supresión de una máquina virtual instantánea
- Conversión de la máquina virtual instantánea de Linux en una máquina virtual independiente
- Migración de la máquina virtual instantánea de Linux en una máquina física

Iniciar o detener una máquina virtual instantánea

Se puede iniciar o detener una máquina virtual instantánea después de crearla. El botón de inicio o detención se muestra dependiendo del estado de la máquina virtual.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructuras** y haga clic en **Máquina virtual instantánea**.
3. Seleccione la máquina virtual en el panel central y haga clic en **Acciones**.
4. Seleccione **Encender** o **Apagar**en función del estado de la máquina virtual.

   La máquina virtual se inicia o se detiene correctamente.

Reinicio de una máquina virtual instantánea

Se puede reiniciar una máquina virtual instantánea después de crearla.

Nota: Se puede reiniciar una máquina virtual instantánea solo si se encuentra en el estado **Incorrecto** o **Bloqueo de la tarea**.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructura** y haga clic en **Máquinas virtuales instantáneas**.
3. Seleccione la máquina virtual con el estado **Incorrecto** o **Bloqueo de la tarea** en el panel central y haga clic en **Acciones**.
4. Haga clic en **Reiniciar**.

   Se reinicia la máquina virtual.

Supresión de una máquina virtual instantánea

Se puede suprimir cualquier máquina virtual instantánea que ya no se necesite.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Vaya a **Infraestructuras** y haga clic en **Máquina virtual instantánea**.
3. Seleccione la máquina virtual en el panel central y haga clic en **Acciones**.
4. Haga clic en **Suprimir**.

   Aparecerá un diálogo de confirmación.
5. Haga clic en **Aceptar**.

   La máquina virtual se ha suprimido correctamente.

Conversión de la máquina virtual instantánea de Linux en una máquina virtual independiente

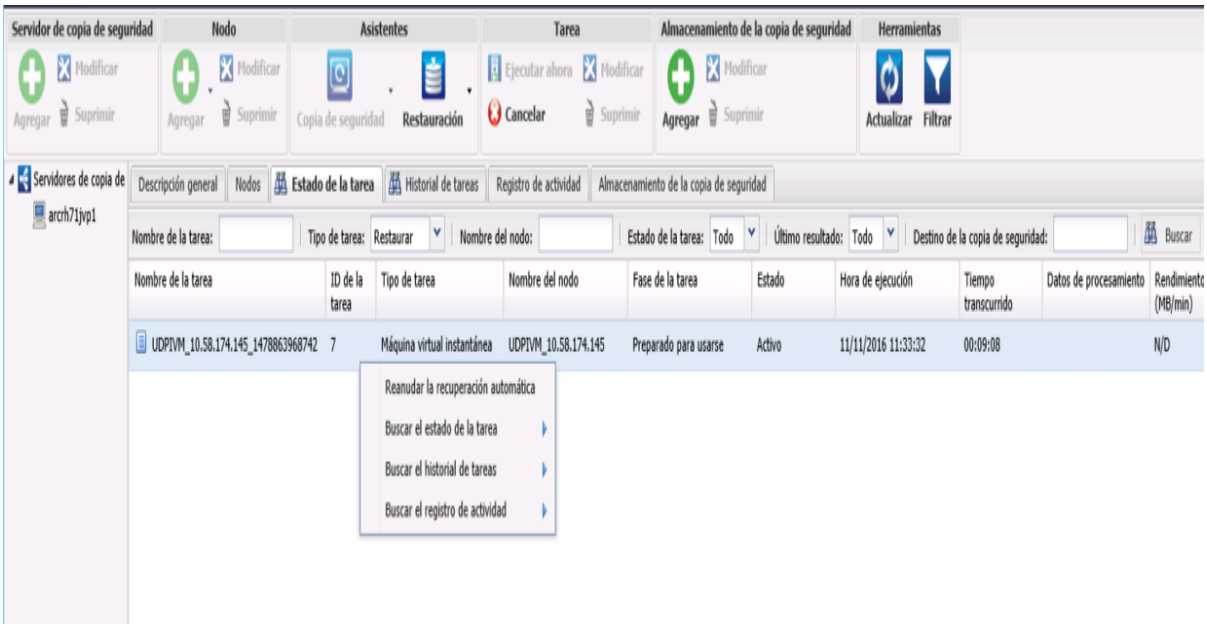
Se puede cambiar una máquina virtual de Linux instantánea (IVM) a una máquina virtual independiente (VM).

Notas:

- Para continuar, se necesita un elemento del menú que está disponible solamente después de que la máquina virtual instantánea se haya ejecutado en la fase de tarea “Preparado para usarse”.
- El elemento del menú no estará disponible si el punto de recuperación es una copia de seguridad sin agente y el hipervisor de destino es vSphere ESX/VC. Es necesario utilizar VMware Storage vMotion para convertir la máquina virtual instantánea en una máquina virtual independiente.

Siga estos pasos:

1. Abra la interfaz de usuario del servidor de copia de seguridad de Linux.



2. En la ficha Estado de la tarea, seleccione la tarea de máquina virtual instantánea y haga clic con el botón secundario para abrir el menú contextual.
3. Seleccione Reanudar la recuperación automática.

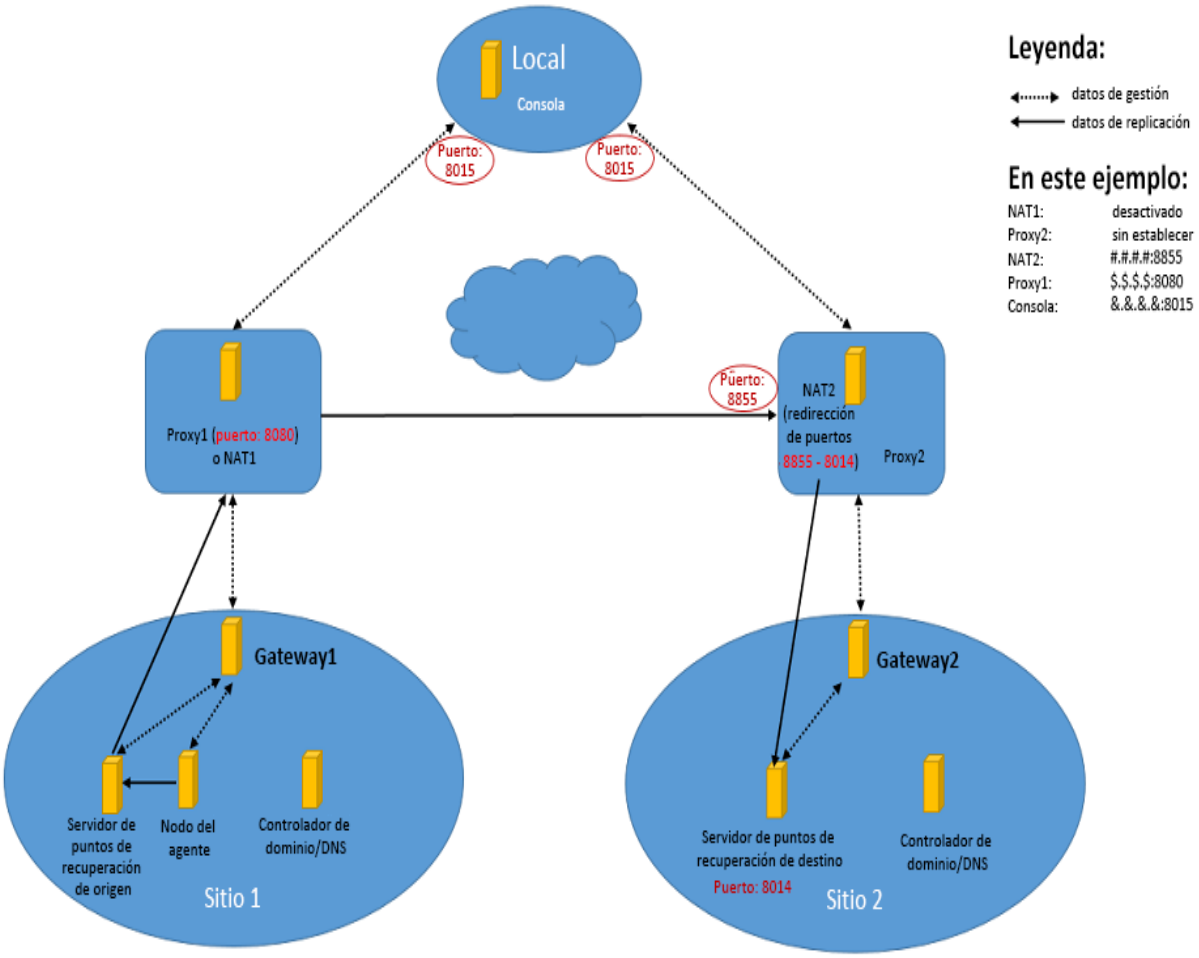
   La tarea de máquina virtual instantánea se mueve al historial de tareas cuando el proceso finaliza correctamente.

Migración de la máquina virtual instantánea de Linux desde Amazon EC2 a una máquina física

Para migrar la máquina virtual instantánea de Linux a un equipo físico, consulte la sección **Cómo realizar una reconstrucción completa de la migración para los equipos Linux de Amazon EC2 a un destino local** en la *Guía del usuario del Agente para Linux*.

Cómo crear un plan para la replicación entre sitios

La función de replicación entre sitios permite usar la misma Consola para replicar datos entre distintos sitios. En el siguiente diagrama se muestra la conexión entre la Consola, el sitio 1 y el sitio 2:



La Consola (por ejemplo, en una red pública), el sitio 1 (por ejemplo, en una red privada) y el sitio 2 (por ejemplo, en otra red privada) pueden encontrarse en distintos segmentos de red. El sitio 1 y el 2 se gestionan mediante la Consola a través de la puerta de enlace.

El diagrama muestra un ejemplo para ilustrar esta función de UDP, que solo es una referencia ya que es posible que el entorno real que se está utilizando no sea similar al entorno que se describe aquí. El ejemplo pretende replicar datos desde el servidor de puntos de recuperación de origen del sitio 1 al servidor de puntos de recuperación de destino del sitio 2. La puerta de enlace del sitio 1 y del sitio 2 se puede conectar a la Consola mediante el proxy o NAT. El proxy y NAT se deben configurar correctamente.

Descripción del diagrama:

- Proxy1 o NAT1 tiene tanto la interfaz pública como la privada. Por ejemplo: IP-1 como dirección IP pública está en el mismo segmento que la Consola e IP-2 como dirección IP privada está en el mismo segmento que el sitio 1. En la configuración de red del equipo Gateway1, la puerta de enlace predeterminada se establece en la dirección IP privada de Proxy1 o NAT1.
- Proxy2 y NAT2 también tienen la misma configuración que Proxy1/NAT1. Además, NAT2 necesita una configuración adicional para una regla de redirección de puertos para que desde la red pública se pueda acceder al servicio privado mediante esta asignación. En este ejemplo, es el servidor de puntos de recuperación de origen a través del cual la redirección de puertos de NAT2 puede conectarse al servidor de puntos de recuperación de destino.
- Con el sistema operativo Windows Server 2012 R2, tanto la interfaz gráfica de usuario como el comando de Windows pueden establecer la redirección de puertos para NAT. A continuación se muestra un comando de ejemplo que significa lo siguiente: introduzca esta dirección del explorador web del servidor de puntos de recuperación https o http://<NAT2 IP-1 >: <número de puerto=8855> y se le redirigirá al servidor de puntos de recuperación de destino https o http://<dirección IP del servidor de puntos de recuperación de destino=192.168.30.102>:8014. A continuación, se podrá ejecutar la replicación entre sitios.

netsh interface portproxy add v4tov4 listenport=8855 connectaddress="192.168.30.102" connectport=8014 protocol=tcp

Creación de un plan para la replicación entre sitios

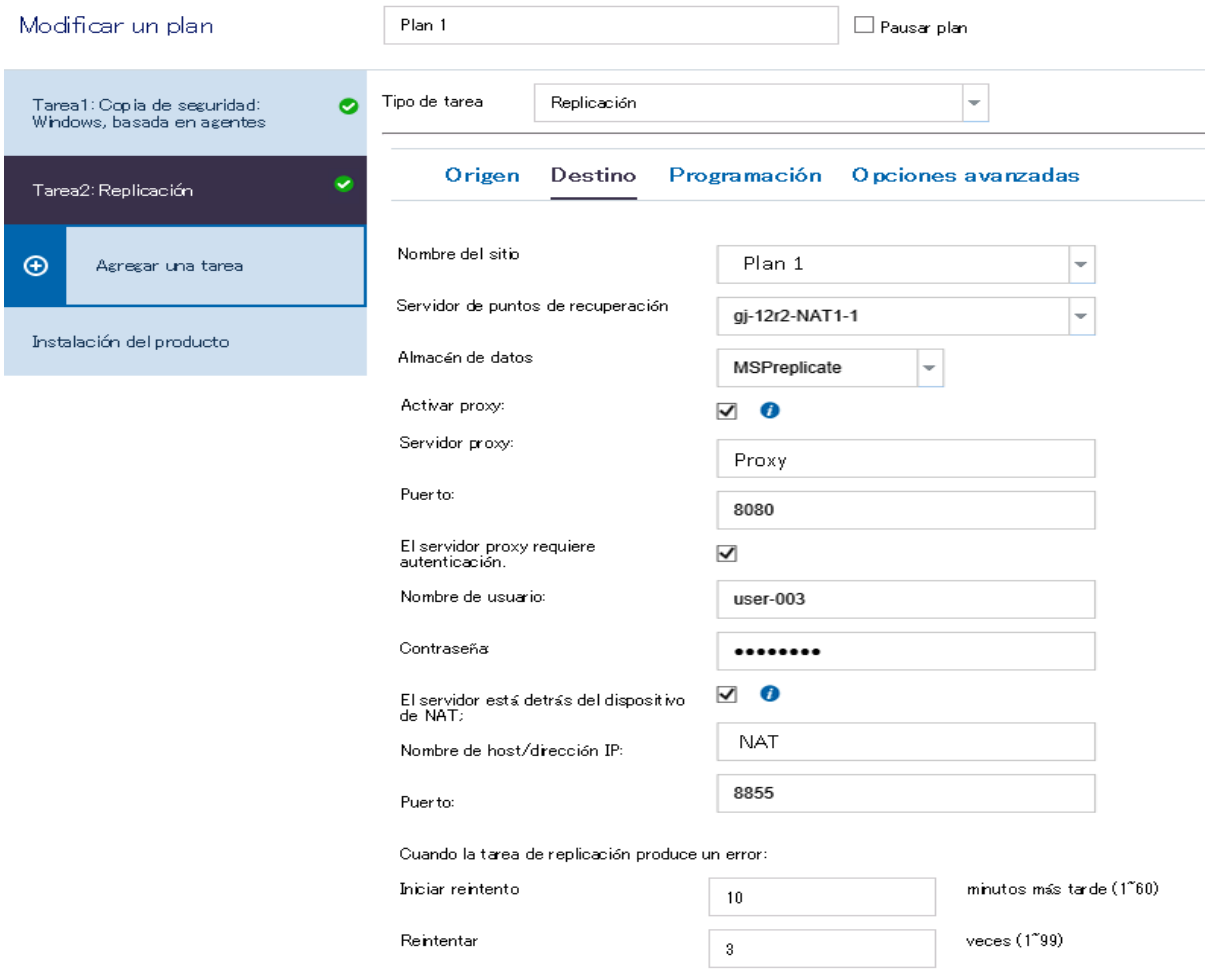
Se puede crear un plan para la replicación entre sitios.

Siga estos pasos:

1. En el sitio 1, que es el servidor de puntos de recuperación, cree una tarea de copia de seguridad, Tarea 1.
2. Agregue una tarea **Replicación** al mismo plan.
3. En la ficha **Destino**, seleccione el otro sitio (el sitio 2 en el ejemplo) donde se encuentra el servidor de puntos de recuperación de destino o el almacén de datos.
4. (Opcional) Active los detalles del proxy (servidor, puerto y autenticación).

   Nota: Antes de activar los detalles del servidor proxy, debe configurar el servidor proxy entre el sitio 1 y la Consola.
5. (Opcional) Active los detalles de NAT.

   Nota: Antes de activar los detalles de NAT, debe configurar el servidor de NAT y la redirección de puertos entre la Consola y el sitio 2.



6. Configure las otras fichas, como **Programación** y **Opciones avanzadas**, y guarde el plan.
7. Cuando se ejecute la tarea, verifique el controlador y el estado del catálogo para la copia de seguridad, la replicación (salida) y la replicación (entrada).

Cómo proteger los datos de Microsoft Office 365

Esta sección incluye los siguientes temas:

Autenticación moderna

Esta sección proporciona información sobre cómo configurar los requisitos previos para las copias de seguridad de Office 365 utilizando la autenticación moderna. Para configurar, siga estos pasos:

1. Preparación del equipo proxy
2. Configuración de una aplicación en Azure Portal
3. Asignación de los permisos de administrador global a la aplicación de Azure
4. Descarga del certificado de UDP y carga del certificado a Azure
5. Asignación del rol de suplantación de la aplicación a la cuenta de usuario especificada para la copia de seguridad

Preparación del equipo proxy

Esta sección proporciona información sobre cómo preparar el equipo proxy.

Siga estos pasos:

1. Instale PowerShell versión 5.1 o posterior (forma parte de Windows Management Framework (WMF)).

   Nota: Para comprobar la versión de PowerShell, ejecute el siguiente comando:

   Get-Host | Select-Object Version

2. Para instalar los componentes necesarios del sistema, realice una de las siguientes acciones:
   - Para instalar los componentes necesarios del sistema de forma automática, realice lo siguiente:
     a. Descargue el script de PowerShell. Para descargar, haga clic en *Script2InstallPrerequisites.ps1_*.
     b. Renombre *Script2InstallPrerequisites.ps1_* a *Script2InstallPrerequisites.ps1*.

c. Abra la ventana de PowerShell mediante la opción *Ejecutar como administrador* y, a continuación, ejecute *Script-t2InstallPrerequisites.ps1*.

- Para instalar los componentes necesarios del sistema manualmente, ejecute los siguientes comandos de PowerShell:
  - *Install-Module -Name AzureAD -Force*
  - *Install-Module -Name ExchangeOnlineManagement -Force*
  - *Install-Module -Name PackageManagement -Force*
  - *Install-Module -Name PowerShellGet -Force*

  Nota: Cuando se instalan módulos de PowerShell utilizando los comandos anteriores, es posible que se instale una versión más nueva de los módulos en función de la versión de disponibilidad general del componente disponible en el repositorio de Microsoft.

Configuración de una aplicación en Azure Portal

Esta sección proporciona información sobre cómo configurar una aplicación en Azure Portal.

Siga estos pasos:

1. Inicie sesión en Azure Portal.
2. Para ir a la página de registros de la aplicación, realice una de las siguientes acciones:
   - En el panel izquierdo, seleccione **Azure Active Directory** y, a continuación, haga clic en **Registros de aplicaciones**.
   - Busque registros de aplicaciones en la barra de búsqueda y, a continuación, seleccione **Registros de aplicaciones**.
3. En la página de registros de aplicaciones, haga clic en **Nuevo registro**.
4. En la página Registrar una aplicación, haga lo siguiente y, a continuación, haga clic en **Registrar**.
   - Nombre: Introduzca un nombre para la aplicación. Por ejemplo, *UDP365*.
   - Tipos de cuenta admitidos: seleccione la opción **Accounts in this organizational directory only ("your-domain" only – Single tenant)**.
5. Copie y guarde el **ID de cliente de aplicación** para uso futuro.

Asignación de los permisos de administrador global a la aplicación de Azure

Esta sección proporciona información sobre cómo asignar los permisos de administrador global a la aplicación de Azure.

Para asignar el rol de administrador global a la aplicación AzureAD, realice una de las siguientes acciones:

- Para asignar el rol automáticamente, siga estos pasos:
  1. Descargue el script de PowerShell. Para descargarlo, haga clic en *AssignGlobalAdminRoleToADApplication.ps1*.
  2. Abra la ventana de PowerShell utilizando la opción *Ejecutar como administrador*, vaya a la ruta del script descargado y, a continuación, ejecute lo siguiente:

     .\AssignGlobalAdminRoleToADApplication.ps1 <ID de la aplicación (cliente) generado desde Azure Portal>

     Por ejemplo:

     .\AssignGlobalAdminRoleToADApplication.ps1 60f92079-d1bf-40f7-9ab5-59caab8e7534
- Para asignar el rol manualmente mediante los cmdlets de PowerShell, siga estos pasos:
  1. Para instalar el módulo MSOnline, ejecute el siguiente comando desde la ventana de PowerShell utilizando la opción Ejecutar como administrador:

     Install-Module MSOnline
  2. Para iniciar una conexión con Azure Active Directory (AzureAD), ejecute el siguiente comando:

     Connect-MSolService
  3. Obtenga el ID de la aplicación mediante el siguiente comando:

     $sp = Get-MsolServicePrincipal -AppPrincipalID <GUID ID APLICACIÓN>

     Nota: El GUID del ID de la aplicación es el ID de la aplicación de UDP.
  4. Obtenga el rol de administrador global/de la compañía mediante el siguiente comando:

     $role = Get-MsolRole -RoleName "Administrador de empresa"

5. Para agregar el rol de administrador global/de la compañía a la aplicación AzureAD, utilice el siguiente comando:

   Add-MsolRoleMember -RoleObjectId $role.ObjectId -RoleMemberType ServicePrincipal -RoleMemberObjectId $Sp.ObjectId

Descarga del certificado de UDP y carga del certificado a Azure

Esta sección proporciona información sobre cómo descargar el certificado de UDP y cómo cargarlo en Azure Portal.

En la Consola de UDP, mientras se crea un plan de Office 365 nuevo o existente para Exchange Online, SharePoint u OneDrive, después de seleccionar la opción Autenticación moderna, realice una de las siguientes acciones:

Método 1: Para generar y descargar un nuevo certificado autofirmado para la autenticación, siga estos pasos:

1. Para generar un nuevo certificado autofirmado, seleccione **Generar y descargar un nuevo certificado autofirmado**.
2. Escriba y vuelva a escribir la contraseña del certificado según sea necesario.
3. Para descargar el certificado, haga clic en una de las siguientes opciones:
   - **Certificado público:** Descargue el certificado para cargarlo en el portal de Azure.
   - **Certificado privado:** Descargue el certificado para guardarlo en su equipo para uso futuro.

     Nota: Después de descargar el certificado público, se activa la opción de descarga para el certificado privado.
4. Inicie sesión en Azure Portal.
5. Busque registros de aplicaciones en la barra de búsqueda y, a continuación, seleccione **Registros de aplicaciones**.
6. En la lista de aplicaciones registradas, haga clic en la aplicación que se ha creado previamente en la sección *Configuración de una aplicación en Azure Portal*.
7. Vaya a Certificados y secretos, haga clic en **Cargar certificado**, examine el certificado existente [archivo .cer] y, a continuación, haga clic en **Agregar**.
8. En el panel izquierdo, seleccione los permisos de la API y, a continuación, haga clic en **Conceder consentimiento de administrador para <nombre de inquilino>**.

Aparecerá un mensaje de confirmación.

9. Haga clic en **Sí**.
10. En la Consola de UDP, haga clic en **Siguiente** para continuar con el registro de nodos.

Método 2: Para autenticar utilizando un certificado existente, siga estos pasos:

Notas:

- Cuando se selecciona la opción *Utilizar certificado existente*, se espera que el usuario tenga los archivos del certificado (archivo .cer) y del certificado de clave privada (archivo .PFX con contraseña). Estos certificados pueden estar autofirmados o firmados por una autoridad de certificación.
- Si se utiliza el mismo certificado para crear varios planes, basta con cargar el certificado una sola vez en Azure Portal.
- Si está utilizando Internet Explorer (IE 11), se bloquea para continuar cuando se selecciona la opción *Utilizar certificado existente*. Para solucionar este problema, consulte Configurar los valores de configuración de seguridad de Internet Explorer (IE 11).

1. Inicie sesión en Azure Portal.
2. Busque registros de aplicaciones en la barra de búsqueda y, a continuación, seleccione **Registros de aplicaciones**.
3. En la lista de aplicaciones registradas, haga clic en la aplicación que se ha creado previamente en la sección *Configuración de una aplicación en Azure Portal*.
4. Vaya a Certificados y secretos, haga clic en **Cargar certificado**, examine el certificado existente [archivo .cer] y, a continuación, haga clic en **Agregar**.
5. En el panel izquierdo, seleccione los permisos de la API y, a continuación, haga clic en **Conceder consentimiento de administrador para <nombre de inquilino>**.

   Aparecerá un mensaje de confirmación.
6. Haga clic en **Sí**.
7. Siga estos pasos desde la Consola de UDP:
   a. Busque el certificado de la clave privada [archivo .PFX] e introduzca la contraseña.
   b. Haga clic en **Siguiente** para continuar con el registro del nodo.

Asignación del rol de suplantación de la aplicación a la cuenta de usuario especificada para la copia de seguridad

Esta sección proporciona información sobre cómo agregar la cuenta de copia de seguridad al grupo de roles de la gestión de detecciones y cómo asignar el permiso de suplantación de la aplicación.

Para agregar el rol y el grupo necesarios, realice una de las siguientes acciones:

Método 1: Uso de Office 365 Portal

Siga estos pasos:

1. Inicie sesión en Office 365 Portal como administrador o con una cuenta que disponga de permisos de administrador global.

   Se abre la página Centro de administración de Exchange.

2. Vaya a los **permisos** y, en el menú desplegable **Agregar**, haga doble clic en **Administración de detecciones**.

   Aparecerá el cuadro de diálogo Administración de detecciones.

   Nota: Un miembro del grupo de rol de la Administración de detecciones puede realizar búsquedas de buzones de correo en la organización de Exchange para buscar los datos que se adapten a unos criterios específicos.

3. En **Roles**, haga clic en **+** para agregar el rol ApplicationImpersonation.

   Aparecerá el cuadro de diálogo Seleccionar un rol.

4. En la lista desplegable **Nombre para mostrar**, seleccione **ApplicationImpersonation**.

   Nota: *El rol ApplicationImpersonation permite que las aplicaciones suplanten a usuarios en una organización para realizar las tareas en nombre del usuario.*

5. Haga clic en **Agregar** para agregar el rol ApplicationImpersonation y, a continuación, haga clic en **Aceptar**.

6. En el cuadro de diálogo Administración de detección, en **Miembros**, haga clic en **+** para agregar la cuenta de la copia de seguridad como miembro.

   Aparecerá el cuadro de diálogo Seleccionar miembros.

7. En el menú desplegable Nombre, seleccione la cuenta de copia de seguridad, haga clic en **Agregar** para agregar el miembro y, a continuación, haga clic en **Aceptar**.

La cuenta de copia de seguridad seleccionada se muestra en **Miembros** en el cuadro de diálogo **Gestión de la detección**.

8. Haga clic en **Guardar**.

Método 2: Uso de PowerShell remoto

Siga estos pasos:

1. Conéctese al inquilino de Exchange Online mediante PowerShell remoto. Para obtener más información, consulte Conexión a Exchange Online PowerShell.
2. Una vez conectado, para agregar la cuenta de copia de seguridad como miembro del grupo de rol de la gestión de la detección, debe utilizar el siguiente comando:

   `"Add-RoleGroupMember" cmdlet`

   Por ejemplo: *Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.*
3. Para asignar el rol de suplantación de la aplicación a la cuenta de copia de seguridad, utilice el siguiente comando:

   `"New-ManagementRoleAssignment" cmdlet`

   Por ejemplo: *New-ManagementRoleAssignment -Name: impersonationAssignmentName -Role:ApplicationImpersonation - User: "username@domain.onmicrosoft.com"*

El rol *ApplicationImpersonation* y el grupo de miembros se agregan a la cuenta de la copia de seguridad de Exchange Online.

Cómo crear un plan de copia de seguridad de Exchange Online

Exchange Online es una aplicación de correo electrónico que se aloja en la nube de Microsoft. Para proteger los elementos de correo de Exchange Online (correos, elementos del calendario, contactos, etc.) desde la nube de Microsoft, es necesario crear un plan. El plan para Exchange Online está formado por una tarea de copia de seguridad. Esta tarea de copia de seguridad le permite especificar los nodos de Exchange Online que se desean proteger, el destino de la copia de seguridad y la programación de la copia de seguridad.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Creación de un plan de copia de seguridad de Exchange Online
3. (Opcional) Realización de una copia de seguridad manual
4. Realización de la configuración de la autenticación multifactor

Revisión de las consideraciones y requisitos previos

Revise las consideraciones y los requisitos previos antes de crear un plan de copia de seguridad de Exchange Online.

Creación de un plan de copia de seguridad de Exchange Online:

Requisitos previos:

Para la cuenta de la copia de seguridad:

- Utilice una cuenta de servicio de copia de seguridad con permisos de administrador globales.
- Agregue el permiso de suplantación para el usuario de la copia de seguridad a la cuenta de la copia de seguridad de Exchange Online para conectar la organización de Exchange Online, realizar copias de seguridad y restaurar.

  Nota: Si no se agrega la cuenta de la copia de seguridad al grupo de rol de gestión de la detección y no se asigna el permiso de suplantación de la aplicación, se producirá un error en la copia de seguridad.

- Asocie la cuenta del usuario de la copia de seguridad con un buzón de Exchange Online.

Para el proxy de la copia de seguridad:

- Inicie sesión en la consola.
- Instale el Agente de Arcserve UDP en el equipo proxy donde se desea ejecutar la copia de seguridad o la restauración.

Consideraciones:

- Al realizar la copia de seguridad de un conjunto grande de usuarios, puede utilizar grupos de Exchange para mejorar la copia de seguridad y la optimización.
- La configuración predeterminada para la copia de seguridad Exchange Online utiliza 4 subprocesos de copia de seguridad (un subproceso por usuario) a la vez. También se pueden modificar los subprocesos en el archivo de configuración de *Engine\BIN\Office365\Arcserve.Office365.Exchange.config*como sigue:

```
<!--#region for multi thread--> <!--MultiThreadEnable default
value:0. if enable, set 1.--> <add

                                                    <add
```

```
<!--set how many thread will be used to backup mailbox.
default value is 4--
> key="MaxDegreeOfParallelismForMailbox" value="4"/> <add
key="MaxDegreeOfParallelismForMailbox" value="4"/> <!--#en-
dregion-->
```

Se recomienda establecer el valor de 1 a 5. El valor máximo posible es 10. Pero no se recomienda establecer el valor de 6 a 10.

Nota: UDP 8.0 admite lo siguiente:

- Buzón de correo del usuario
- Buzón de correo compartido
- Carpetas públicas habilitadas para el correo
- Buzones de correo de sala
- Buzones de correo de equipamiento
- Buzones de correo de grupo

Nota: Para obtener más información sobre las prácticas recomendadas para Exchange Online, consulte.Relacionados con Exchange Online.

Creación de un plan de copia de seguridad de Exchange Online utilizando la autenticación básica (BA):

Revise los siguientes requisitos previos:

- Instale PowerShell versión 5.1 o posterior (forma parte de Windows Management Framework (WMF)) en el servidor proxy (equipo de 64 bits).
- Instale los siguientes módulos de PowerShell en el servidor proxy mediante la ventana PowerShell:
  - Para instalar el módulo Azure, ejecute el siguiente comando:

    Install-Module -Name AzureAD -Force
  - Para instalar el módulo ExchangeOnlineManagement, ejecute el siguiente comando:

    Install-Module -Name ExchangeOnlineManagement -Force

Nota: Cuando se instalan módulos de PowerShell utilizando los comandos anteriores, es posible que se instale una versión más nueva de los módulos en función de la versión de disponibilidad general del componente disponible en el repositorio de Microsoft.

Creación de un plan de copia de seguridad de Exchange Online utilizando la autenticación moderna (MA):

Revise los requisitos previos antes de crear un plan utilizando la autenticación moderna.

Asignación del rol de suplantación de la aplicación a la cuenta de usuario especificada para la copia de seguridad

Esta sección proporciona información sobre cómo agregar la cuenta de copia de seguridad al grupo de roles de la gestión de detecciones y cómo asignar el permiso de suplantación de la aplicación.

Para agregar el rol y el grupo necesarios, realice una de las siguientes acciones:

Método 1: Uso de Office 365 Portal

Siga estos pasos:

1. Inicie sesión en Office 365 Portal como administrador o con una cuenta que disponga de permisos de administrador global.

   Se abre la página Centro de administración de Exchange.

2. Vaya a los **permisos** y, en el menú desplegable **Agregar**, haga doble clic en **Administración de detecciones**.

   Aparecerá el cuadro de diálogo Administración de detecciones.

   Nota: Un miembro del grupo de rol de la Administración de detecciones puede realizar búsquedas de buzones de correo en la organización de Exchange para buscar los datos que se adapten a unos criterios específicos.

3. En **Roles**, haga clic en **+** para agregar el rol ApplicationImpersonation.

   Aparecerá el cuadro de diálogo Seleccionar un rol.

4. En la lista desplegable **Nombre para mostrar**, seleccione **ApplicationImpersonation**.

   Nota: *El rol ApplicationImpersonation permite que las aplicaciones suplanten a usuarios en una organización para realizar las tareas en nombre del usuario.*

5. Haga clic en **Agregar** para agregar el rol ApplicationImpersonation y, a continuación, haga clic en **Aceptar**.

6. En el cuadro de diálogo Administración de detección, en **Miembros**, haga clic en **+** para agregar la cuenta de la copia de seguridad como miembro.

   Aparecerá el cuadro de diálogo Seleccionar miembros.

7. En el menú desplegable Nombre, seleccione la cuenta de copia de seguridad, haga clic en **Agregar** para agregar el miembro y, a continuación, haga clic en **Aceptar**.

La cuenta de copia de seguridad seleccionada se muestra en **Miembros** en el cuadro de diálogo **Gestión de la detección**.

8. Haga clic en **Guardar**.

Método 2: Uso de PowerShell remoto

Siga estos pasos:

1. Conéctese al inquilino de Exchange Online mediante PowerShell remoto. Para obtener más información, consulte Conexión a Exchange Online PowerShell.
2. Una vez conectado, para agregar la cuenta de copia de seguridad como miembro del grupo de rol de la gestión de la detección, debe utilizar el siguiente comando:

   `"Add-RoleGroupMember" cmdlet`

   Por ejemplo: *Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.*
3. Para asignar el rol de suplantación de la aplicación a la cuenta de copia de seguridad, utilice el siguiente comando:

   `"New-ManagementRoleAssignment" cmdlet`

   Por ejemplo: *New-ManagementRoleAssignment -Name: impersonationAssignmentName -Role:ApplicationImpersonation - User: "username@domain.onmicrosoft.com"*

El rol *ApplicationImpersonation* y el grupo de miembros se agregan a la cuenta de la copia de seguridad de Exchange Online.

Creación de un plan de copia de seguridad de Exchange Online

Un plan de copia de seguridad incluye una tarea de copia de seguridad que realiza una copia de seguridad de los elementos de datos del correo de Exchange Online (correos, elementos del calendario, contactos, etc.) y almacena los datos en un almacén de datos sin deduplicación o en un almacén de datos de deduplicación. Además, este plan de copia de seguridad permite a UDP detectar y especificar los grupos de Exchange Online para los que se realiza una tarea de copia de seguridad. Cada tarea está formada por parámetros que definen el origen, destino, programación y otros detalles de la copia de seguridad.

Siga estos pasos:

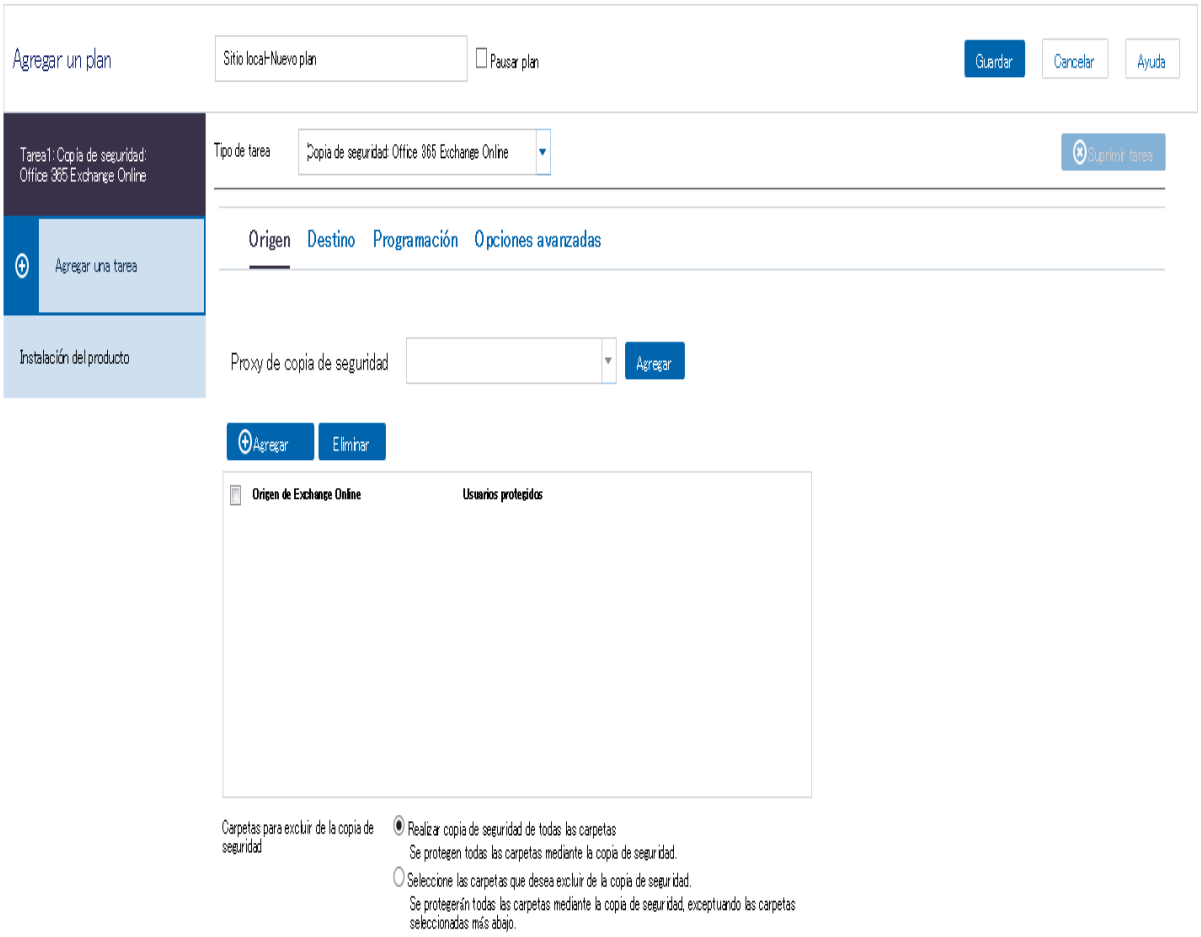
1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre el cuadro de diálogo **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecuta hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable Tipo de tarea seleccione **Copia de Seguridad: Office 365 Exchange Online**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

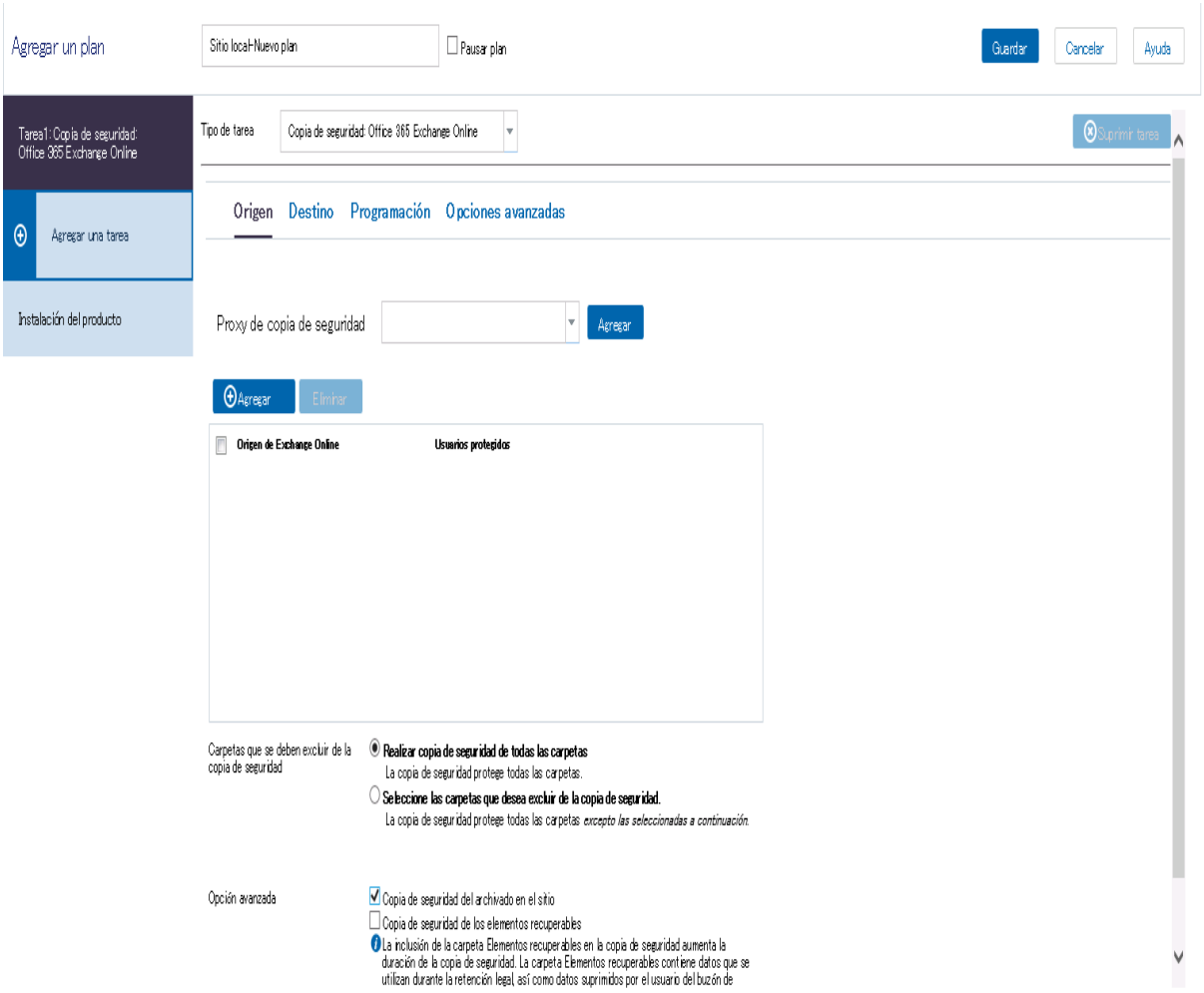
La página Origen le permite especificar los nodos de origen de Exchange Online que se desean proteger. Se puede seleccionar más de un nodo de origen de Exchange Online en el plan. Si no se han agregado nodos a la Consola, se pueden agregar nodos de origen de Exchange Online desde la página Origen.

Nota: Se puede guardar un plan sin agregar nodos de origen pero el plan no se muestra a menos que se agreguen nodos.

También se pueden gestionar los nodos de Exchange Online utilizando Compatibilidad con el buzón de correo de la carpeta pública para la protección de Exchange Online.

Siga estos pasos:

1. Haga clic en la ficha **Origen**.



2. Para el servidor proxy de la copia de seguridad, realice una de las siguientes acciones:
   - En la lista desplegable, seleccione un servidor proxy de la copia de seguridad existente.
   - Para agregar un nuevo servidor proxy de la copia de seguridad, haga clic en **Agregar** junto a la lista desplegable.
3. Agregue el nodo de Exchange Online utilizando una de las siguientes opciones:

   Método 1

   a. Haga clic en **Agregar** y, a continuación, haga clic en **Seleccionar nodos para proteger en Arcserve UDP**.

      Se muestra el cuadro de diálogo Agregar nodos al plan.

   b. Seleccione un nodo y haga clic en **Conectar**.

      Nota: También se pueden buscar los nodos de origen de Exchange Online que se desean proteger en **Buscar**.

   c. Seleccione la casilla de verificación **Proteger todo el origen de Office 365 Exchange** para proteger todas las cuentas de Exchange Online en todas las páginas.

      Nota: Para agregar todas las cuentas de Exchange Online a la lista protegida, se puede hacer clic en la flecha hacia la derecha (>).

      Se agregan las cuentas de Exchange Online que se han seleccionado.

   Método 2

   - Haga clic en **Agregar** y, a continuación, haga clic en **Agregar origen de Exchange Online**.

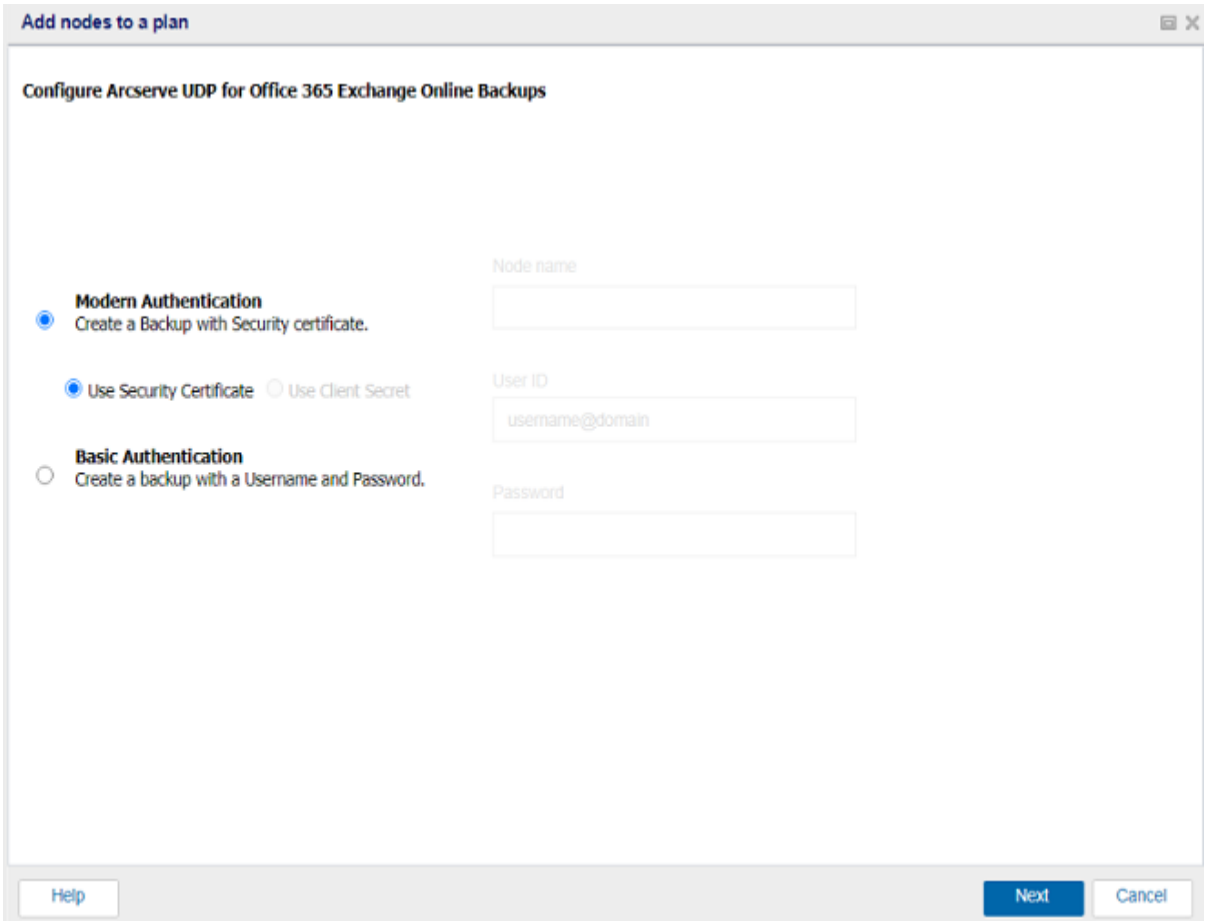
     Aparece el cuadro de diálogo Agregar nodos a un plan.

     Nota: A diferencia de otros nodos, no se puede agregar el nodo de Exchange Online desde la página **Todos los nodos**. Solo se puede agregar un nodo de Exchange Online a un plan o cuando se modifica un plan.

     Varios nodos de Exchange Online pueden utilizar la misma cuenta de usuario (cuenta de servicio) de Exchange Online.
4. Para aplicar la autenticación, realice una de las siguientes acciones:

Autenticación moderna

Para la autenticación moderna, se puede ejecutar una copia de seguridad con un certificado de seguridad.



Utilizar certificado de seguridad

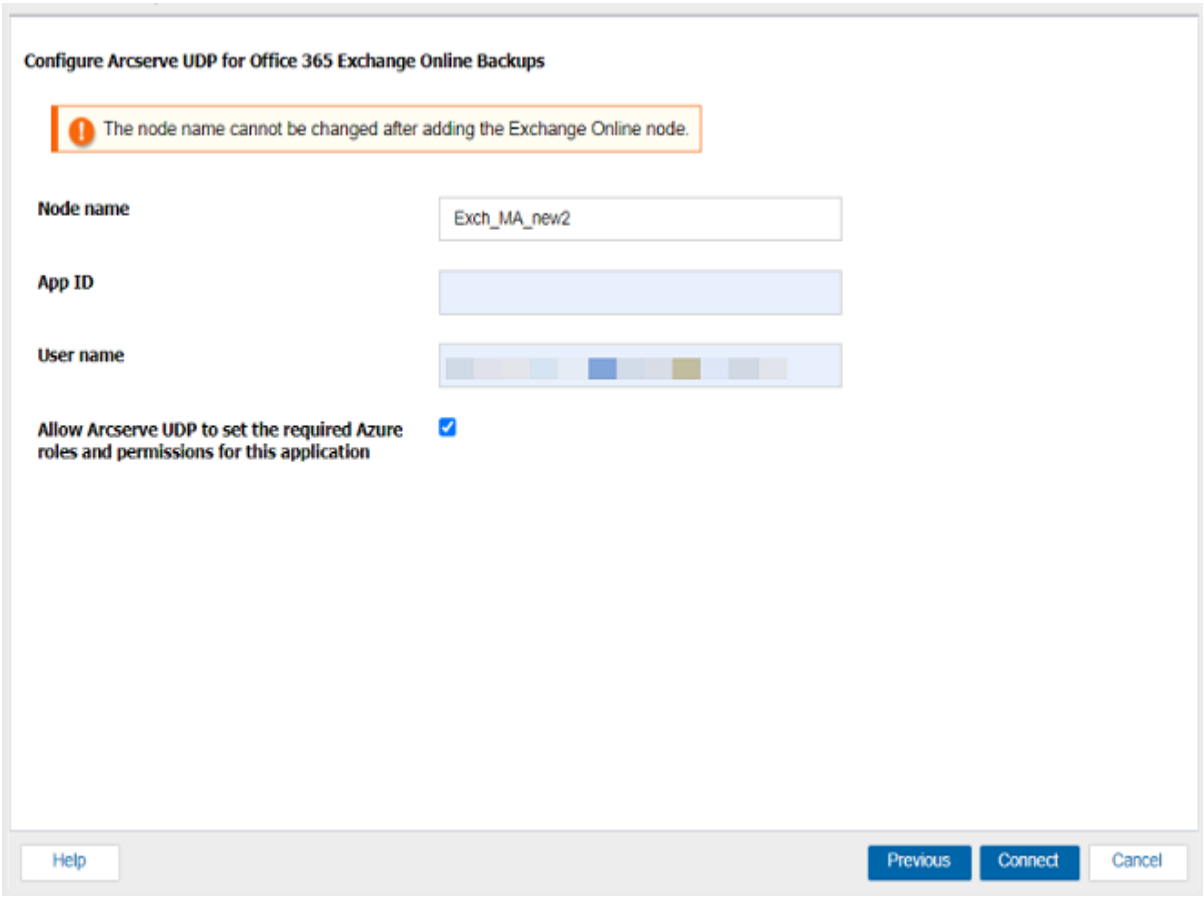
Nota: De forma predeterminada, el plan de copia de seguridad selecciona **Utilizar certificado de seguridad** para la autenticación moderna.

Siga estos pasos:

a. Para autenticar la aplicación de UDP con certificados de seguridad, consulte Descarga del certificado de UDP y carga del certificado en Azure.

b. Introduzca los siguientes detalles:

- Nombre de nodo
- ID de aplicación
- Nombre de usuario



c. Para aplicar los permisos de API automáticamente, seleccione la casilla de verificación **Permitir que Arcserve UDP establezca los permisos de la API necesarios para esta aplicación**.

   Nota: Para aplicar los permisos manualmente sin utilizar el rol de administrador global o de la compañía, consulte Configuración de los permisos de la API manualmente sin utilizar el rol de administrador global o de la compañía.

d. Haga clic en **Conectar**.

Notas:

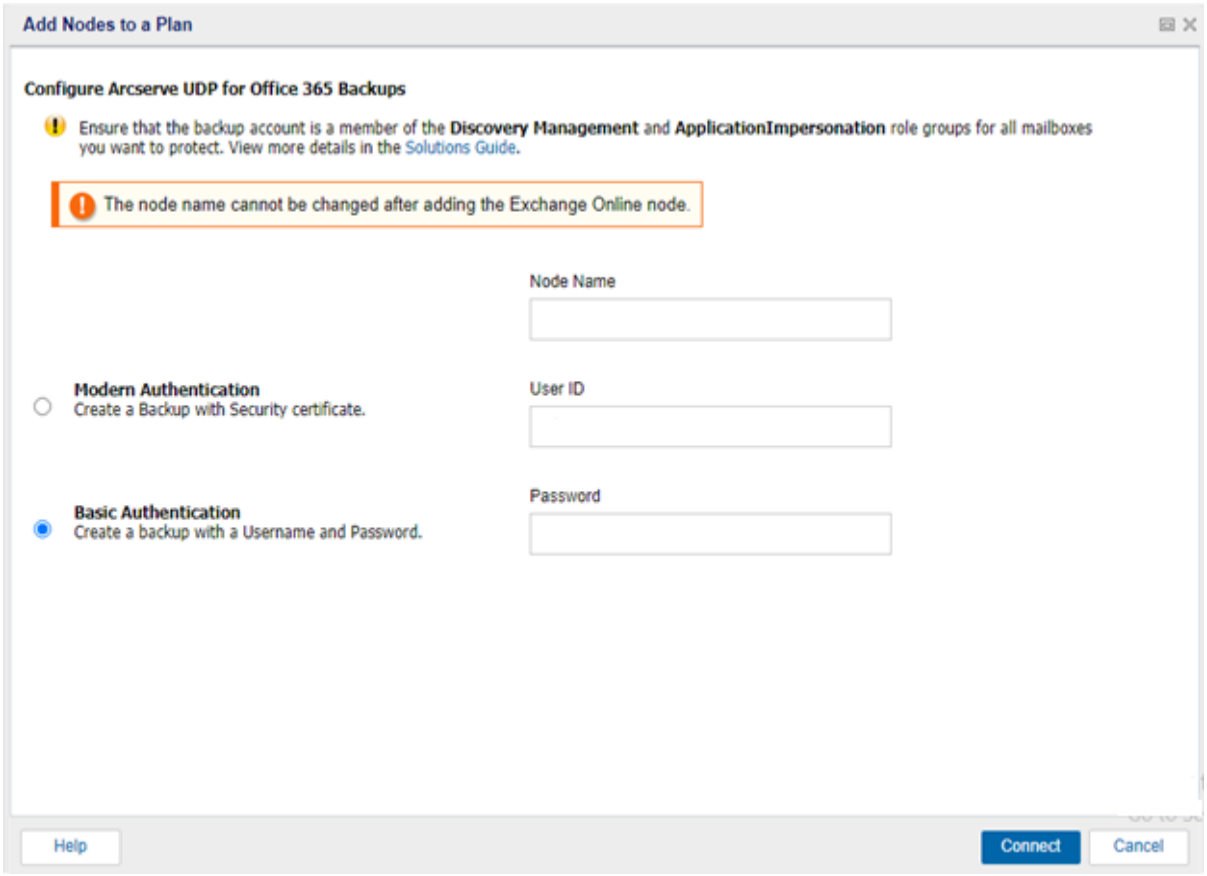
- El nombre del nodo de Exchange Online no se puede cambiar después de agregar el nodo.
- Introduzca el nombre de usuario de la cuenta de copia de seguridad de Exchange Online que cumpla los requisitos previos en **Nombre de usuario del administrador**.
- La autenticación moderna no se aplica a lo siguiente:

- Los clientes que utilizan Microsoft 365 (Office 365) para sus instancias de Arcserve Cloud Hybrid o Arcserve Cloud Backup para Office 365, que se creó antes del 18 de octubre de 2020, no permiten la autenticación moderna.
- Los clientes que continúan utilizando la autenticación básica.

Autenticación básica

Para la autenticación básica, para continuar con la copia de seguridad, proporcione la siguiente información y, a continuación, haga clic en **Conectar**:

- Nombre de nodo
- ID de usuario
- Contraseña



Nota: Es posible que al realizar una actualización o cambio en la cuenta de usuario se pueda cambiar el número de buzones de correo protegidos. Se debe comprobar que las cuentas de servicio nuevas o actualizadas tienen derechos de suplantación para que los buzones puedan estar protegidos.

5. Para proteger los buzones de correo de Exchange Online, realice una de las siguientes acciones:

   - Para proteger todos los grupos y buzones de correo de Exchange Online, seleccione la casilla de verificación **Proteger todo el origen de Office 365 Exchange**.

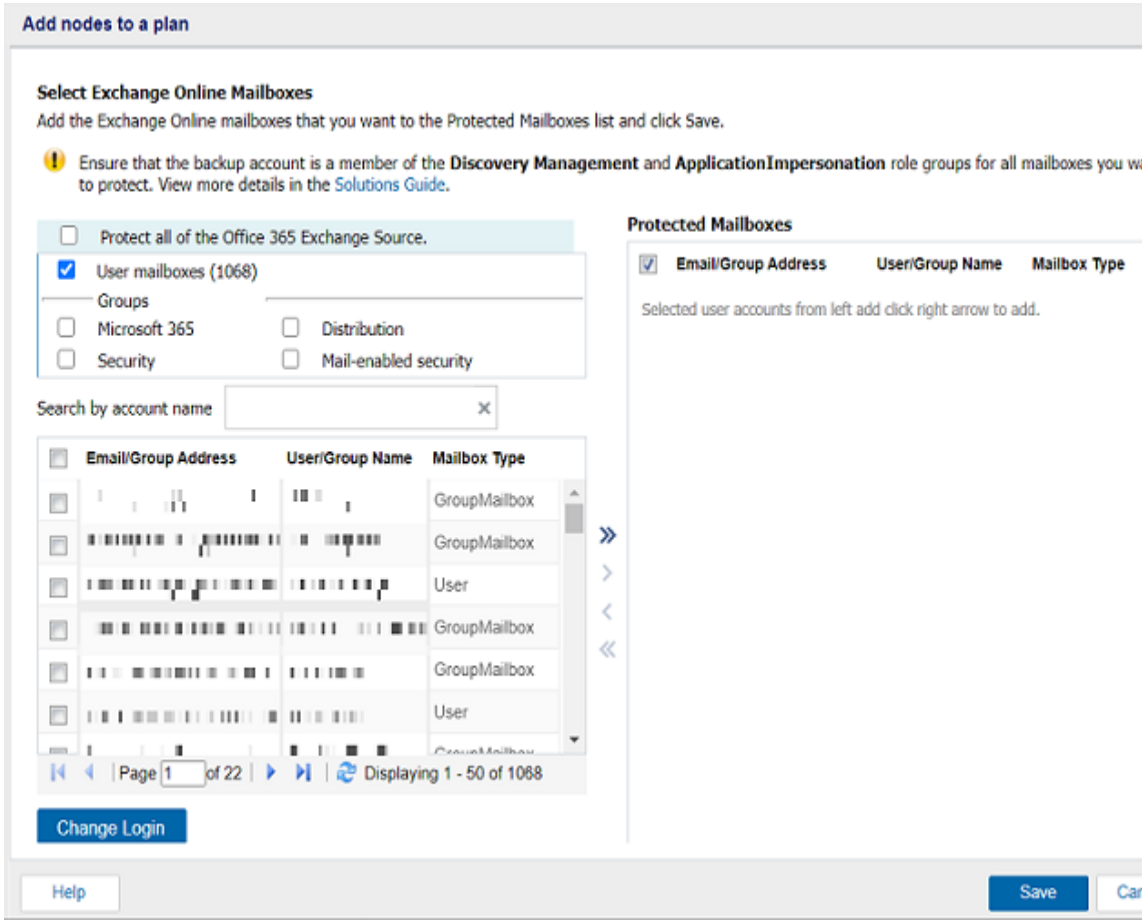
     Nota: Esta opción se selecciona automáticamente de forma predeterminada cuando aparece la pantalla Seleccionar buzones de correo de Exchange Online.

   - Para obtener los buzones de correo del usuario, siga estos pasos:

     a. Seleccione la casilla de verificación **Buzones de correo del usuario**.

        Aparecerá una lista de los buzones de correo del usuario.

     b. (Opcional) Para buscar una cuenta en la lista, en el campo Buscar por nombre de cuenta escriba el nombre de la cuenta.



c. En la lista de buzones de correo del usuario, seleccione los buzones de correo que se desean proteger.

d. Haga clic en la flecha hacia la derecha (>) para mover los buzones de correo seleccionados a la lista de buzones de correo protegidos.

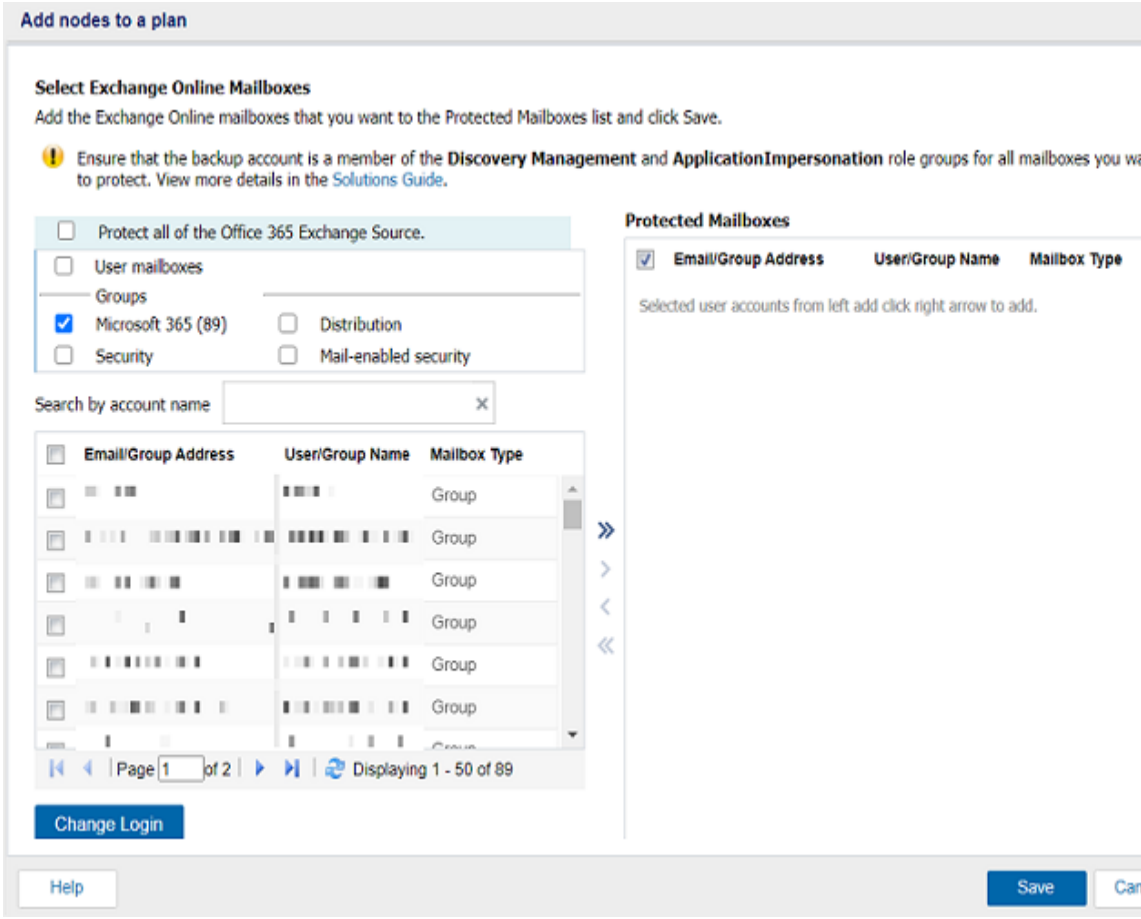
- Para obtener los grupos, siga estos pasos:

a. Seleccione la casilla de verificación **Microsoft 365**.

Aparece una lista de grupos.

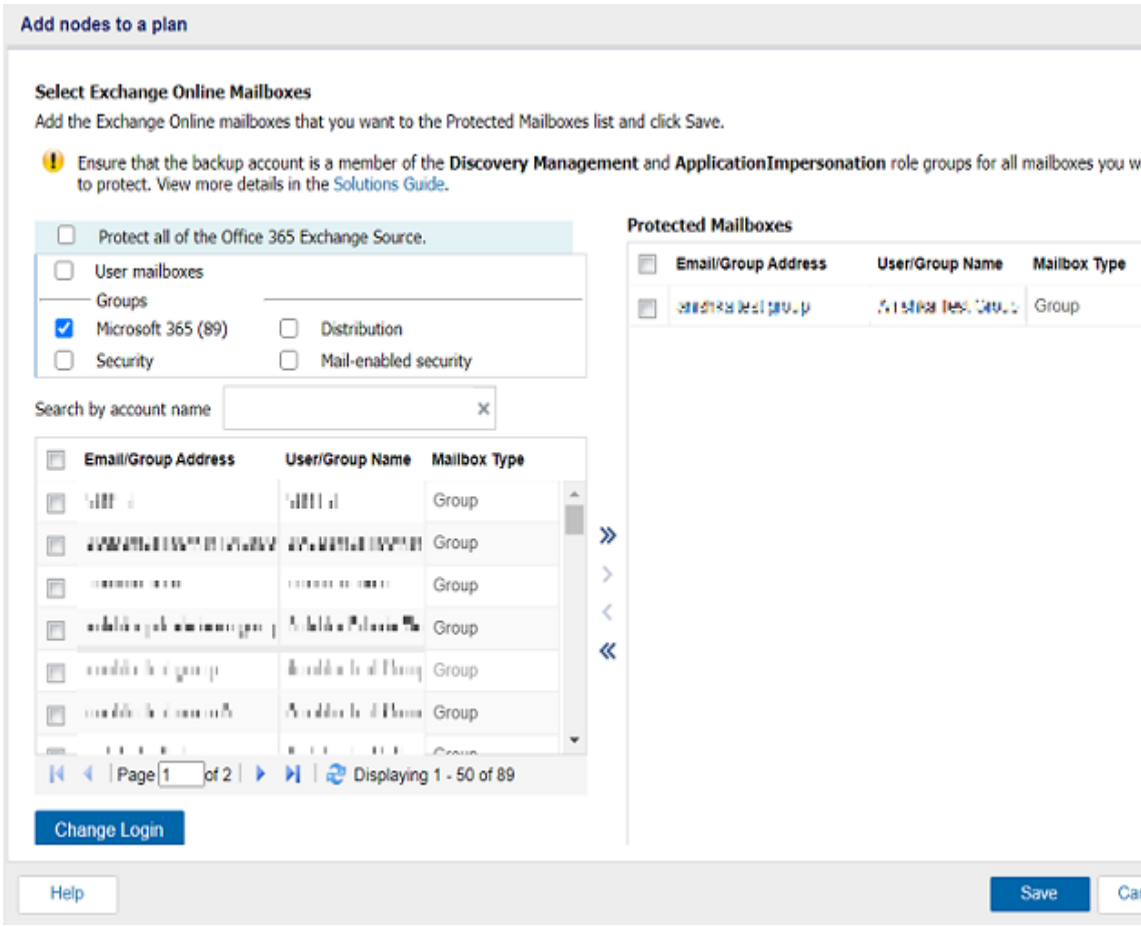
Nota: Si desea seleccionar grupos junto con subgrupos como, por ejemplo, **Distribución**, **Seguridad** o **Seguridad activada para el correo**, seleccione la casilla de verificación **Microsoft 365** y, a continuación, seleccione una casilla de verificación del subgrupo según sea necesario.

b. (Opcional) Para buscar una cuenta en la lista, en el campo Buscar por nombre de cuenta escriba el nombre de la cuenta.



c. En la lista de grupos, seleccione los grupos que desea proteger.

d. Haga clic en la flecha hacia la derecha (>) para mover los grupos seleccionados a la lista de buzones de correo protegidos.



6. Haga clic en **Guardar**.
7. En la ficha Orígenes, vaya a **Carpetas que se deben excluir de la copia de seguridad** y, a continuación, seleccione la casilla de verificación deseada.
8. En Opción avanzada, seleccione la casilla de verificación deseada.
   - Para permitir que la protección de Exchange Online sea compatible con el Buzón archivado, active la casilla de verificación **Backup up In-Place Archiving**.

     Nota: Para obtener más información sobre el archivado de buzones, consulte el vínculo.
   - Active la casilla de verificación **Backup up Recoverable items** para activar la protección del buzón que se activa la función Conservación local o Suspensión por litigio.

Nota: Para la Conservación local o la Suspensión por litigio del archivado para Exchange Online, consulte este vínculo.

Nota: Para activar las características en el buzón al mismo tiempo para hacer la copia de seguridad de los elementos recuperables en el buzón archivado, seleccione tanto la opción **Backup up In-Place Archiving** como la opción **Backup up Recoverable items**

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Haga clic en la ficha **Destino**.
2. Seleccione la opción **Servidor de puntos de recuperación de Arcserve UDP. Servidor de puntos de recuperación de Arcserve UDP** especifica que el destino de la copia de seguridad es un servidor de puntos de recuperación. Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.
3. Proporcione los siguientes detalles:
   a. Seleccione un servidor de puntos de recuperación.
   b. Seleccione un almacén de datos sin deduplicación o de deduplicación. La lista muestra todos los almacenes de datos que se han creado en el servidor de puntos de recuperación especificado.
   c. Proporcione una contraseña de la sesión. La contraseña de sesión es opcional cuando el destino de copia de seguridad es un almacén de datos del servidor de puntos de recuperación no cifrado.
   d. Confirme la contraseña de la sesión.

   Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y se pueden proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

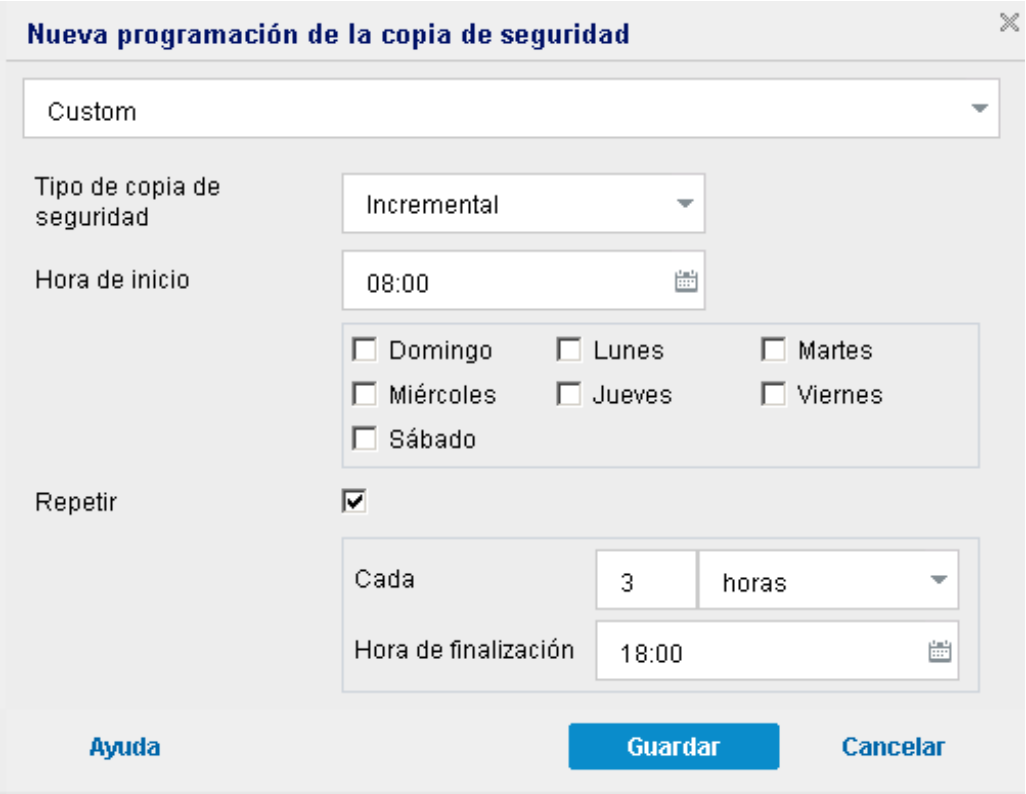
Siga estos pasos:

1. Agregue las programaciones de la copia de seguridad, de la combinación y del regulador.

   Agregar programación de la copia de seguridad

   a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

      Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de las copias de seguridad incrementales consisten en que la copia de seguridad es una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en **Agregar** y seleccione **Agregar programación de la combinación**.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

b. Especifique la hora de inicio para iniciar la tarea de combinación.

c. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

d. Haga clic en **Guardar**.

La programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

Se abre el cuadro de diálogo **Agregar nueva programación del limitador**.

b. Especifique el límite de rendimiento en MB por minuto.

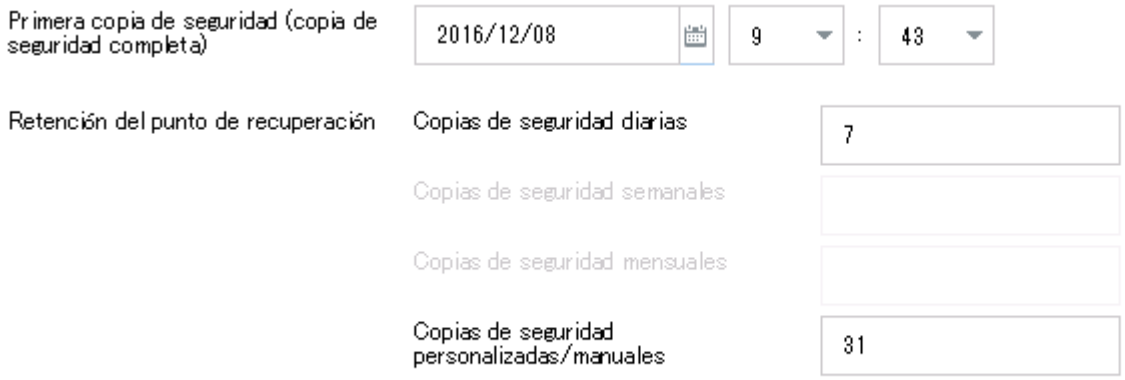
c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

La programación del limitador se especifica y se muestra en la página **Programación**.

2. Especifique la hora de inicio para la copia de seguridad programada.



3. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo **Programación de la copia de seguridad**.

Se especifica la programación.

Funcionamiento de la programación avanzada y de la retención

La opción de programación le permite especificar una programación personalizada, una programación diaria/semanal/mensual o ambas. En la programación personalizada, se puede configurar la programación de la copia de seguridad durante cada día de la semana y se pueden agregar hasta cuatro programaciones de copia de seguridad cada día. Se puede seleccionar un día específico de una semana y crear un período de tiempo para definir cuando se desea ejecutar la copia de seguridad y con qué frecuencia.

Programación	Tarea compatible	Comentarios
Copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para ejecutar las tareas de copia de seguridad.
Regulación de la copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para controlar la velocidad de la copia de seguridad.
Combinar	Tarea de combinación	Defina cuando se deben ejecutar las tareas de combinación.
Programación diaria	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad diarias.
Programación semanal	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad semanales.
Programación mensual	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad mensuales.

Se pueden especificar también los valores de configuración de retención para los puntos de recuperación.

Nota: Establezca la configuración de la retención en cada plan para controlar cómo se retienen los datos para los nodos asignados a ese plan en el almacén de datos de destino.

Las programaciones para las copias de seguridad diarias/semanales/mensuales son independientes de la programación personalizada y de las unas a las otras. Se puede configurar solamente ejecutar una copia de seguridad diaria, una copia de seguridad semanal o una copia de seguridad mensual sin configurar la programación personalizada.

Programación de la tarea de copia de seguridad

Se pueden agregar cuatro períodos de tiempo por día en la programación de la copia de seguridad. Un período de tiempo válido es desde las 12:00 horas hasta las 23:59 horas. No se puede especificar un período de tiempo como, por

ejemplo, de las 18:00 horas a las 06:00 horas. En tales casos, se debe especificar manualmente dos períodos de tiempo diferentes.

Para cada período de tiempo, la hora de inicio está incluida y, en cambio, no se incluye la hora de finalización. Por ejemplo, se ha configurado ejecutar una copia de seguridad incremental ejecutada todas las horas entre las 06:00 horas y las 09:00 horas y la copia de seguridad se iniciará a las 06:00 horas. Esto significa que la copia de seguridad se ejecuta a las 06:00 horas, a las 07:00 horas y a las 08:00 horas, pero NO a las 09:00 horas.

Nota: Si desea ejecutar la tarea de copia de seguridad reiteradamente hasta el final del día, configure la programación hasta las 12:00 horas. Por ejemplo, para ejecutar la tarea de copia de seguridad cada 15 minutos durante todo el día, configure la programación de las 12:00 a las 12:00, cada 15 minutos.

Programación del regulador de la copia de seguridad

La programación del regulador de la copia de seguridad le permite controlar la velocidad del rendimiento de la copia de seguridad, que a su vez controla el uso de recursos (E/S del disco, CPU, ancho de banda de la red) del servidor del que se está realizando la copia de seguridad. Esto es útil si no se desea afectar al rendimiento del servidor durante el horario comercial. Se pueden agregar cuatro períodos de tiempo por día en la programación del regulador de la copia de seguridad. Para cada período de tiempo, se puede especificar un valor en MB por minuto. Este valor se utiliza para controlar el rendimiento de la copia de seguridad. Los valores válidos van desde 1 MB/minuto a 99999 MB/minuto.

Si una tarea de copia de seguridad excede el tiempo especificado, el límite del regulador se ajusta según el período de tiempo especificado. Por ejemplo, se ha definido el límite del regulador de la copia de seguridad en 500 MB/minuto desde las 08:00 horas a las 20:00 horas y en 2500 MB/minuto de las 20:00 horas a las 22:00 horas. Si una tarea de copia de seguridad se inicia a las 19:00 horas y se ejecuta durante tres horas, el límite del regulador es de 500 MB/minuto de las 19:00 horas a las 20:00 horas y de 2500 MB/minuto de las 20:00 horas a las 22:00 horas.

Si no se define ninguna programación de la copia de seguridad ni ninguna programación del rendimiento de la copia de seguridad, la copia de seguridad se ejecuta tan deprisa como pueda.

Programación de la combinación

Le permite combinar puntos de recuperación basándose en la programación proporcionada.

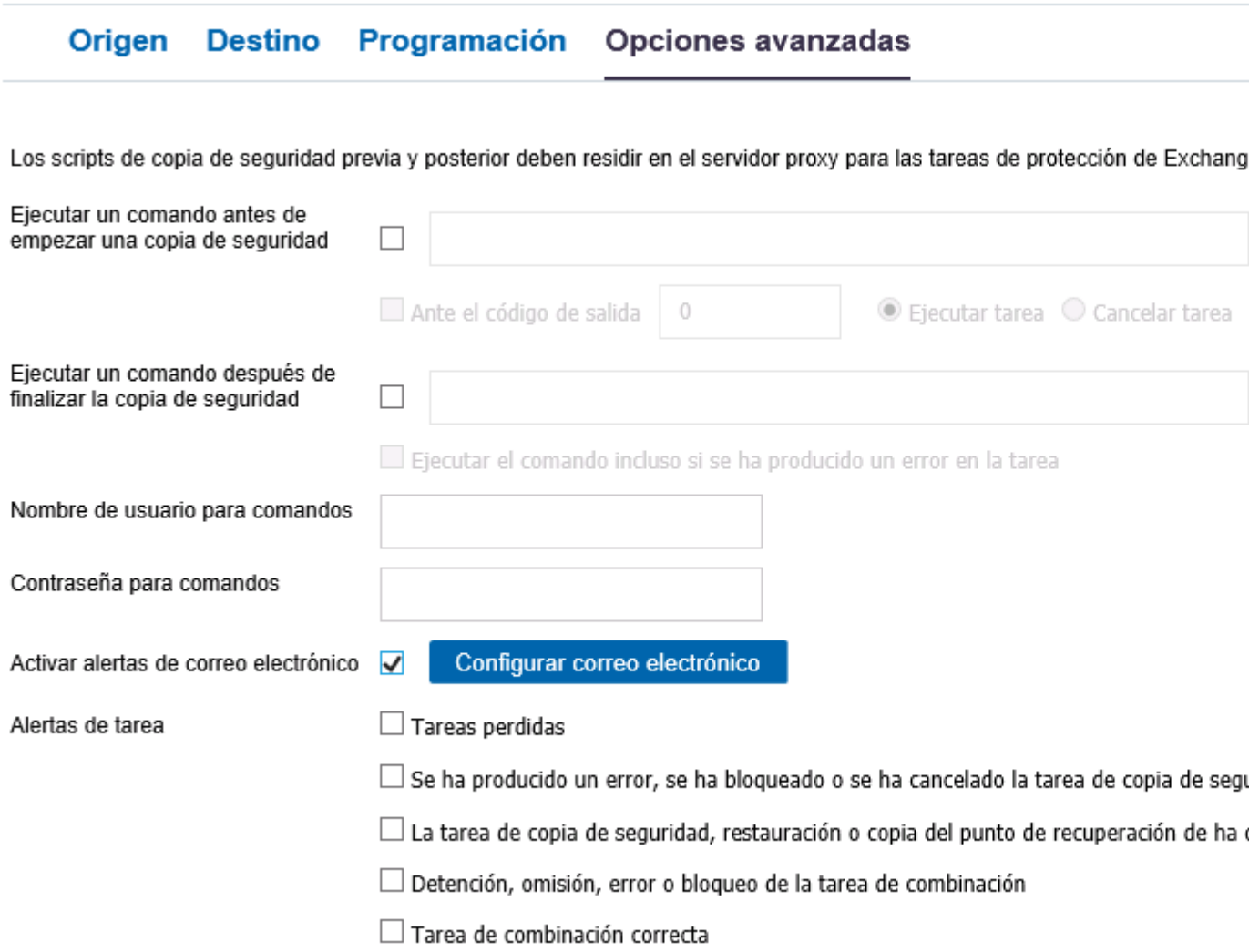
Tenga en cuenta los puntos siguientes para la tarea de combinación:

- Solamente una tarea de combinación puede ejecutarse para un nodo en cualquier momento proporcionado.
- Si se inicia una tarea de combinación, se tiene que completar antes de que la siguiente tarea de combinación se pueda iniciar. Esto no significa que, si uno o más conjuntos de puntos de recuperación se combinan, no se pueda agregar un punto de recuperación nuevo a este proceso de combinación hasta que el proceso de combinación del conjunto actual de puntos de recuperación se complete.
- Si una tarea de combinación está procesando más de un conjunto de puntos de recuperación (por ejemplo, el conjunto [1~4], el conjunto [5~11] y el conjunto [12~14] son tres conjuntos), el servidor de puntos de recuperación procesará estos conjuntos uno a uno.
- Si una tarea de combinación se reanuda después de una pausa, la tarea detecta en qué punto se ha pausado y reanuda la combinación a partir del punto de pausa.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye proporcionar la ubicación de algunos scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha **Avanzada**:



Siga estos pasos:

1. Especifique los siguientes detalles:

   Ejecutar un comando antes de empezar una copia de seguridad

   Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde está almacenado el script en el nodo del proxy. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de

seguridad continúa cuando el script devuelve el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detiene cuando el script devuelve el código de salida.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta completa donde está almacenado el script.

Ejecutar el comando incluso si se ha producido un error en la tarea

Si se selecciona esta casilla de verificación, el script especificado en **Ejecutar un comando después de finalizar una copia de seguridad** se ejecuta incluso cuando se produce un error en la tarea de copia de seguridad. De lo contrario, este script se ejecuta solamente cuando la tarea de copia de seguridad finaliza correctamente.

Nombre de usuario para comandos

Permite especificar el nombre de usuario para ejecutar los comandos.

Contraseña para comandos

Permite especificar la contraseña para ejecutar los comandos.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy. Para obtener más información sobre cómo configurar Configuración del correo electrónico, consulte la sección Configuración del correo electrónico y alertas.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de alerta de las tareas que se desean recibir.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el agente está instalado en el nodo del proxy y si la versión instalada del agente corresponde a la versión más reciente disponible. Arcserve UDP muestra, a continuación, un cuadro de

diálogo de verificación que enumera todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en **Guardar**.

Los cambios se guardan y aparecerá una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se debe agregar otra tarea, se debe seleccionar el plan en la ficha **Recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar. Se pueden agregar las tareas **Copiar punto de recuperación**, **Copia en cinta**, **Replicar** y **Replicar desde un servidor de puntos de recuperación** como tareas de seguimiento.

El plan se implementa automáticamente en el nodo del servidor proxy.

Se crea el plan de copia de seguridad de Exchange Online para el servidor proxy. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación**. Se puede realizar también una copia de seguridad manual en cualquier momento.

(Opcional) Realización de una copia de seguridad manual

Normalmente, en función de la configuración de la programación aplicada, las copias de seguridad se realizan automáticamente. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario. Por ejemplo, si tiene una programación de repetición para las copias de seguridad completas e incrementales y desea hacer cambios importantes en el equipo, puede realizar una copia de seguridad manual inmediata sin necesidad de esperar a la siguiente copia de seguridad programada.

Para realizar una copia de seguridad manual de los nodos de Exchange Online, siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Los nodos de Exchange Online se muestran en el panel central.
3. Seleccione los nodos de Exchange Online (por ejemplo, Mailbox@<nombreorganización.com) de los que se desea realizar la copia de seguridad y asegúrese de que tienen un plan asignado. El nombre del nodo es la cuenta que se utiliza cuando se agrega el nodo de Exchange Online y se conecta.
4. Haga clic con el botón derecho en el nodo y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
5. Seleccione el tipo de copia de seguridad que desea realizar y, a continuación, haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.
6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.
7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   La copia de seguridad manual se realiza correctamente.

   Para realizar una copia de seguridad manual de un plan de Exchange Online, siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Planes** y, a continuación, haga clic en **Todos los planes**.

   Los planes de copia de seguridad de Exchange Online se muestran en el panel central.
3. Seleccione el plan del que desea realizar la copia de seguridad y asegúrese de que tiene un plan asignado.
4. Haga clic con el botón secundario del ratón en el plan y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
5. Seleccione el tipo de copia de seguridad que desea realizar y, a continuación, haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.
6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.
7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   La copia de seguridad manual se realiza correctamente.

Verificación de la copia de seguridad.

Para verificar la tarea de copia de seguridad, confirme que se ha creado correctamente el plan de copia de seguridad. Después de verificar que el plan se ha creado correctamente, confirme si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Se puede verificar el estado de las tareas de copia de seguridad en la ficha **Tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga uno de estos métodos para verificar las tareas de copia de seguridad:

Método 1

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas finalizadas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Método 2

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Tareas correctas**.

   La lista de tareas de copia de seguridad completadas aparecerá en el panel central.
3. Haga clic en la tarea que desea verificar.

   Se actualiza el panel derecho.
4. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
5. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Realización de la configuración de la autenticación multifactor

Cuando una organización tiene la autenticación multifactor (MFA) activada para los usuarios, utilice la autenticación moderna para agregar nodos.

Nota: Aunque la autenticación básica esté activada en el cliente, se puede utilizar la autenticación moderna para agregar nodos. Para obtener más información sobre cómo agregar nodos a un plan mediante la autenticación moderna, consulte Autenticación moderna.

Cómo crear un plan de copia de seguridad de SharePoint Online

La protección de SharePoint se utiliza para la copia de seguridad y la restauración de los elementos de lista y el sitio de Microsoft SharePoint Online. SharePoint Online es uno de los productos principales de Microsoft Office 365. Para proteger el contenido de SharePoint, es necesario crear un plan.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Creación de un plan de copia de seguridad de SharePoint Online
3. Verificación del plan de copia de seguridad
4. Realización de la configuración de la autenticación multifactor

Revisión de los requisitos previos

Revise los siguientes requisitos previos antes de crear un plan de copia de seguridad de SharePoint Online.

Creación de un plan de copia de seguridad de SharePoint Online:

Requisitos previos:

La cuenta de la copia de seguridad es miembro de los grupos de Administradores de la colección de sitios o se ha asignado con el rol *Administrador de SharePoint*.

Para agregar una cuenta al grupo Administradores de la colección de sitios, consulte el vínculo.

Creación de un plan de copia de seguridad de SharePoint Online utilizando la autenticación básica:

Revise los siguientes requisitos previos:

- Instale PowerShell versión 5.1 o posterior (forma parte de Windows Management Framework (WMF)) en el servidor proxy (equipo de 64 bits).
- Instale los siguientes módulos de PowerShell en el servidor proxy mediante la ventana PowerShell:
  - Para instalar el módulo Azure, ejecute el siguiente comando:

    Install-Module -Name AzureAD -Force
  - Para instalar el módulo ExchangeOnlineManagement, ejecute el siguiente comando:

    Install-Module -Name ExchangeOnlineManagement -Force

  Nota: Cuando se instalan módulos de PowerShell utilizando los comandos anteriores, es posible que se instale una versión más nueva de los módulos en función de la versión de disponibilidad general del componente disponible en el repositorio de Microsoft.

Creación de un plan de copia de seguridad de SharePoint Online utilizando la autenticación moderna:

Revise los requisitos previos antes de crear un plan utilizando la autenticación moderna.

Creación de un sitio personal en SharePoint

Esta sección proporciona información sobre cómo crear un sitio personal en SharePoint.

Siga estos pasos:

1. Vaya a la página Inicio de sesión de Microsoft y, a continuación, inicie sesión en la cuenta de administrador de Microsoft Office 365.
2. Vaya a la página **Centro de administración de SharePoint** y, a continuación, haga clic en **Más características** en el panel izquierdo.
3. En la Página de colecciones de sitios clásicos, haga clic en **Abrir**.

   Aparecerá la página Colecciones de sitios.
4. En la página Colecciones de sitios, haga clic en **Nuevo** > **Colección de sitios privados**.

   Aparecerá el cuadro de diálogo Nueva colección de sitios.
5. En el cuadro de diálogo Nueva colección de sitios, proporcione los detalles siguientes y, a continuación, haga clic en **Aceptar**.
   - **Título:** Especifique un nombre para el sitio.
   - **Dirección del sitio web:** En las listas desplegables, seleccione un nombre de dominio y una ruta de URL según sea necesario y, a continuación, escriba un nombre de URL para el sitio.
   - **Selección de plantilla**: En la sección Selección de plantilla, haga lo siguiente:
     - En la lista desplegable **Seleccionar un idioma**, seleccione un idioma para el sitio.
     - En **Seleccionar una plantilla**, seleccione la plantilla para el sitio.
   - **Zona horaria**: Seleccione la zona horaria en función de la ubicación del sitio.
   - **Administrador:** Escriba el nombre de la persona que desea que sea el administrador del sitio. También puede utilizar el botón Comprobar nombres o Examinar para buscar usuarios y convertirlos en administradores del sitio.
   - **Cuota de almacenamiento:** Escriba el tamaño (MB) del sitio que desea asignar.
   - **Cuota de recursos del servidor:** Acepte la cuota de recursos predeterminada.

   Se crea el sitio personal en SharePoint.

Creación de un plan de copia de seguridad de SharePoint Online

Un plan de copia de seguridad incluye la tarea **copia de seguridad: Office 365 SharePoint Online** que realiza una copia de seguridad de los elementos de SharePoint Online (listas, bibliotecas, documentos, etc.) y almacena los datos en un almacén de datos de deduplicación o sin deduplicación. Además, este plan de copia de seguridad permite a UDP detectar y especificar los grupos de SharePoint Online para los que se realiza una tarea de copia de seguridad. Cada tarea está formada por parámetros que definen el origen, destino, programación y otros detalles de la copia de seguridad.

Siga estos pasos:

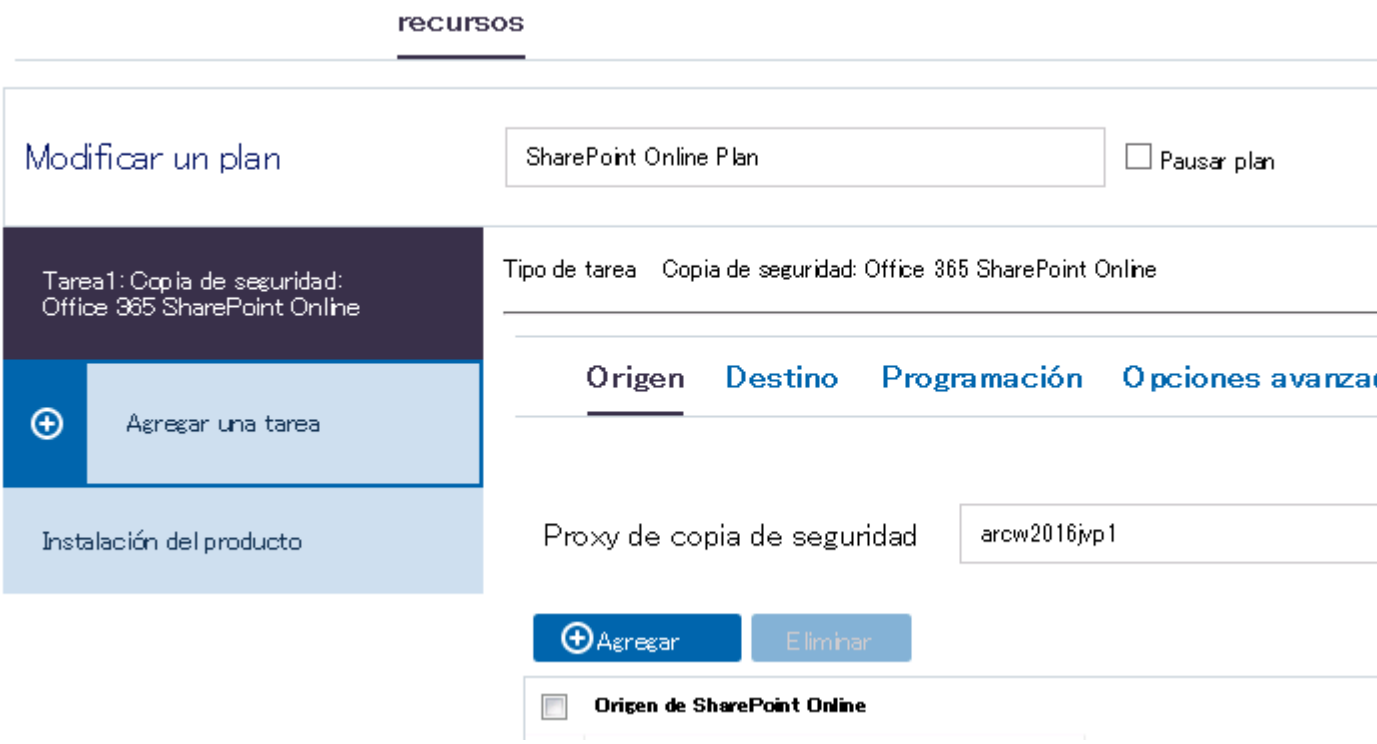
1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre el cuadro de diálogo **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecuta hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable Tipo de tarea seleccione **Copia de Seguridad: Office 365 SharePoint Online**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

La página Origen le permite especificar los nodos de origen de SharePoint Online que se desean proteger. Se puede seleccionar más de un nodo de origen de SharePoint Online en el plan.

Nota: Se puede guardar un plan sin agregar nodos de origen pero el plan no se muestra a menos que se agregue un nodo.

Siga estos pasos:

1. Haga clic en la ficha **Origen**.
2. Seleccione **Servidor proxy de copia de seguridad** en la lista desplegable.
3. Agregue el nodo de SharePoint Online utilizando uno de los siguientes métodos:

   Método 1:

   a. Haga clic en **Agregar** y, a continuación, haga clic en **Seleccionar nodos para proteger en Arcserve UDP**.

      Se muestra el cuadro de diálogo Agregar nodos al plan.

      Nota: Utilice esta opción solamente cuando ya se haya agregado el nodo de SharePoint.

   b. Seleccione un nodo y haga clic en **Conectar**.

      Nota: Para buscar los nodos de SharePoint Online que se desean proteger, utilice **Búsqueda**.

   Método 2:

   - Haga clic en **Agregar** y, a continuación, haga clic en **Agregar origen de SharePoint Online**.

     Aparece el cuadro de diálogo Agregar nodos a un plan.

     Nota:

     - Utilice esta opción para detectar y especificar elementos en línea para el origen de SharePoint Online.
     - A diferencia de otros nodos, no se puede agregar el nodo de SharePoint Online desde la página Todos los nodos. Solo se puede agregar un nodo de SharePoint Online a un plan al crear o modificar un plan.
4. Para aplicar la autenticación, realice una de las siguientes acciones:

Autenticación moderna

Para la autenticación moderna, se puede ejecutar una copia de seguridad con un certificado de seguridad.

Utilizar certificado de seguridad

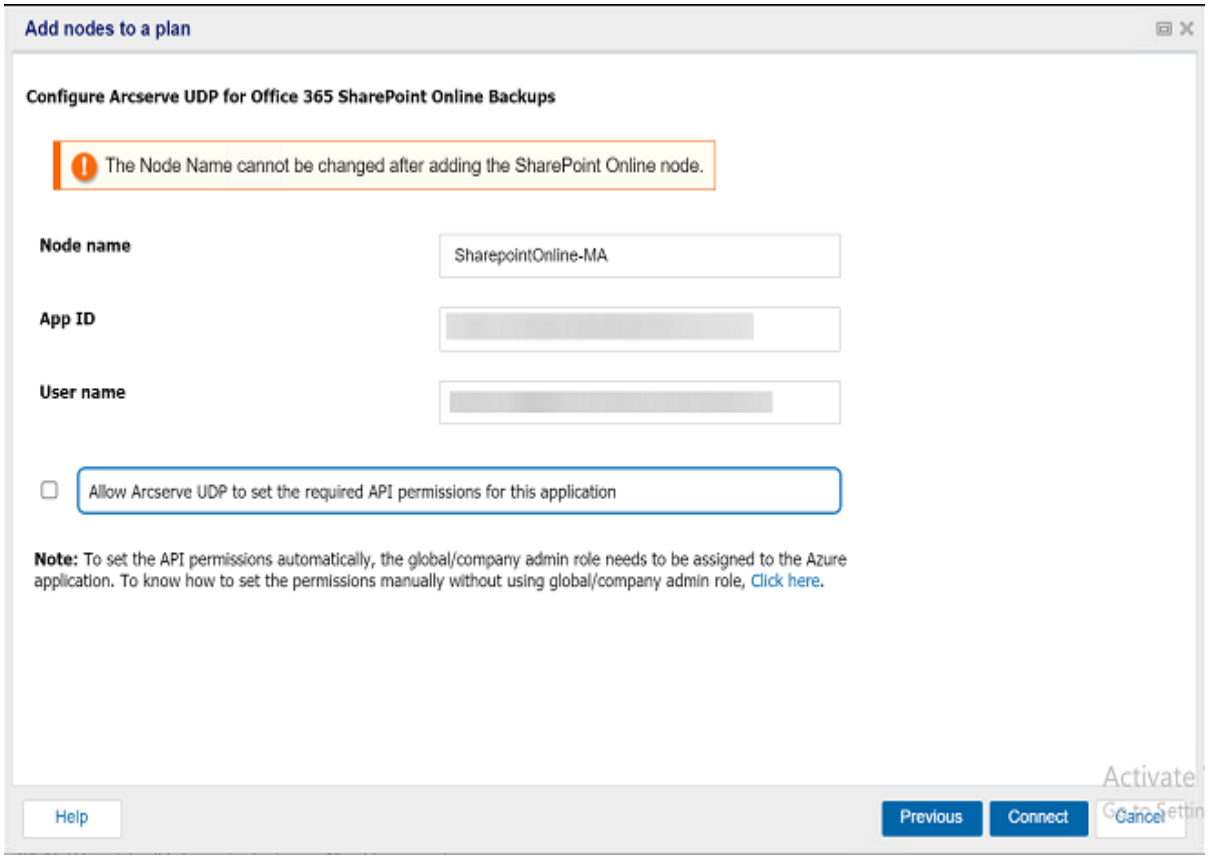
Nota: De forma predeterminada, el plan de copia de seguridad selecciona **Utilizar certificado de seguridad** para la autenticación moderna.

Siga estos pasos:

a. Para autenticar la aplicación de UDP con certificados de seguridad, consulte Descarga del certificado de UDP y carga del certificado en Azure.

b. Introduzca los siguientes detalles:

- Nombre de nodo
- ID de aplicación
- Nombre de usuario



c. Para aplicar los permisos de API automáticamente, seleccione la casilla de verificación **Permitir que Arcserve UDP establezca los permisos de la API necesarios para esta aplicación**.

Nota: Para aplicar los permisos manualmente sin utilizar el rol de administrador global o de la compañía, consulte Configuración de los permisos de la API manualmente sin utilizar el rol de administrador global o de la compañía.

d. Haga clic en **Conectar**.

Notas:

- Los nombres del nodo de origen de SharePoint Online no se pueden cambiar después de crear el nodo.
- Se puede utilizar una única cuenta para proteger varios nodos de SharePoint Online.

Autenticación básica

Para la autenticación básica, para continuar con la copia de seguridad, proporcione la siguiente información y, a continuación, haga clic en **Conectar**:

- Nombre de nodo
- ID de usuario
- Contraseña

5. Para proteger elementos de SharePoint Online, haga lo siguiente y, a continuación, haga clic en **Guardar**.
   - En la lista desplegable Tipo de sitio, seleccione el tipo de sitio que desea proteger como, por ejemplo, Sitios de SharePoint o Sitios personales.
   - Para Proteger todos los sitios y subsitios, realice lo siguiente:

     Notas:

     - Esta opción se selecciona automáticamente de forma predeterminada cuando aparece la pantalla Seleccionar contenido de SharePoint Online.
       - Para proteger todos los elementos del tipo de sitio seleccionado, seleccione la casilla de verificación **Proteger todos los sitios y subsitios**.
       - Para proteger elementos específicos en el tipo de sitio seleccionado, desactive la casilla de verificación **Proteger**

todos los sitios y subsitios y, a continuación, seleccione los elementos específicos que desea proteger.

- Al configurar el plan de SharePoint Online existente, si se han seleccionado sitios manualmente para la protección y ahora se desea seleccionar la casilla de verificación **Proteger todos los sitios y subsitios**, siga estos pasos:
  a. Modifique el plan de SharePoint Online existente.
  b. Borre los sitios de SharePoint que se seleccionan manualmente para la protección.
  c. Seleccione la casilla de verificación **Proteger todos los sitios y subsitios** y, a continuación, guarde el plan.

- Para excluir elementos específicos de la protección, seleccione la casilla de verificación **Excluir sitios seleccionados** y, a continuación, seleccione elementos específicos en el tipo de sitio seleccionado.

Los orígenes de SharePoint Online que desea proteger se agregan al plan.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Haga clic en la ficha **Destino**.

   La opción **Servidor de puntos de recuperación de Arcserve UDP**. **Servidor de puntos de recuperación de Arcserve UDP** especifica que el destino de la copia de seguridad es un servidor de puntos de recuperación.

   No se pueden almacenar los datos como conjuntos de recuperación.

2. Realice los pasos siguientes:

   a. Seleccione un servidor de puntos de recuperación.

   b. Seleccione un almacén de datos sin deduplicación o de deduplicación.

      La lista muestra todos los almacenes de datos que se han creado en el servidor de puntos de recuperación especificado.

   c. Proporcione una contraseña de la sesión.

      La contraseña de sesión es opcional cuando el destino de copia de seguridad es un almacén de datos del servidor de puntos de recuperación no cifrado.

   d. Confirme la contraseña de la sesión.

   Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

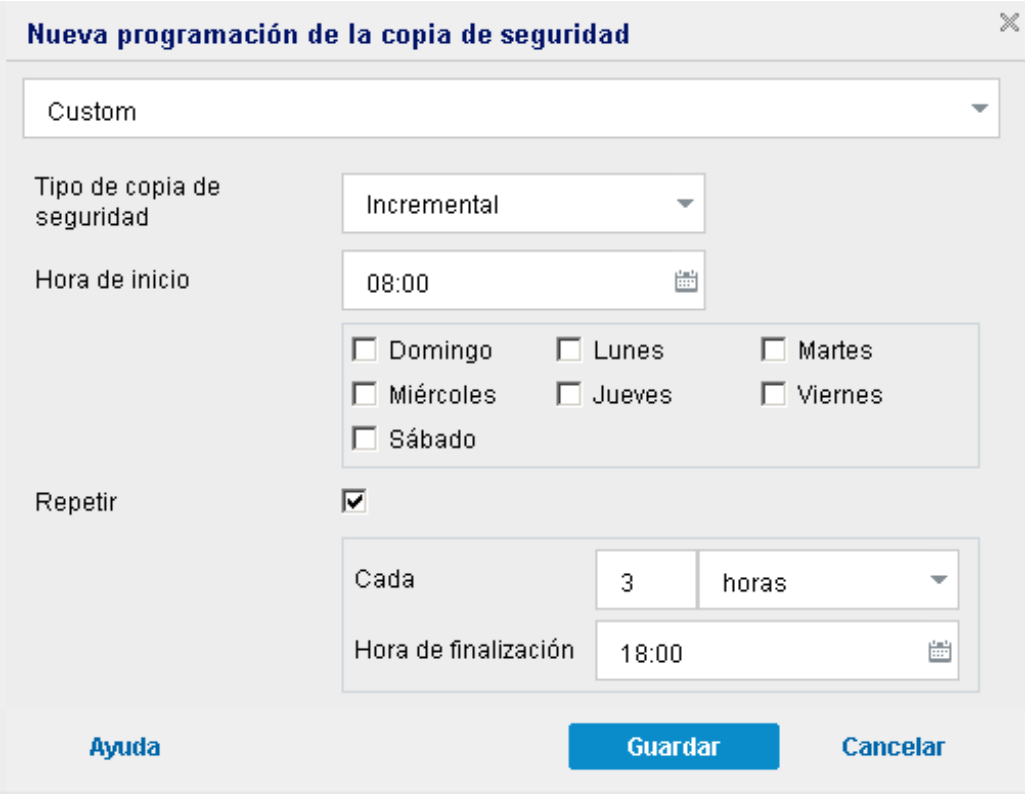
Siga estos pasos:

1. Agregue las programaciones de la copia de seguridad, de la combinación y del regulador.

   Agregar programación de la copia de seguridad

   a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

      Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como está previsto, Arcserve UDP realizará una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

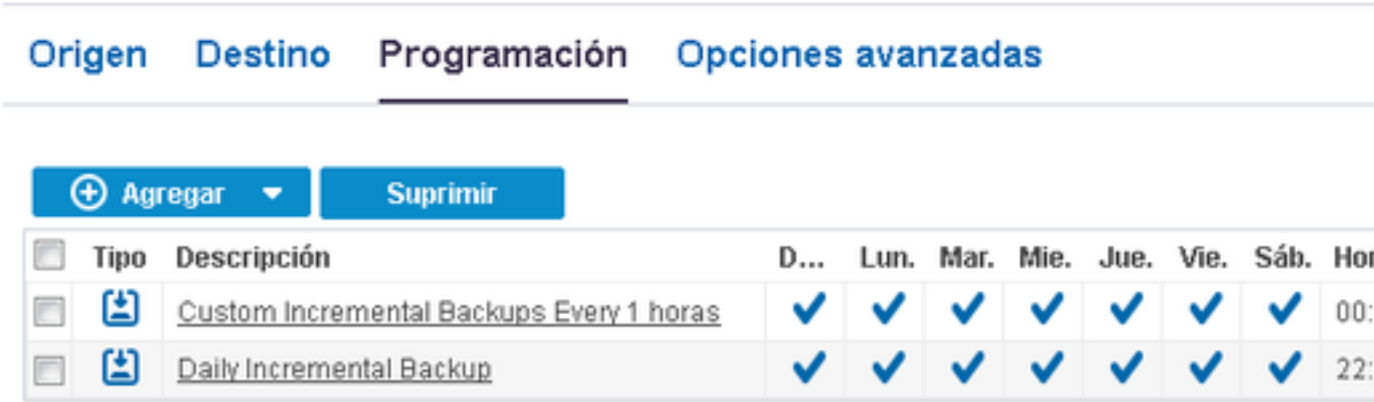
Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de las copias de seguridad incrementales consisten en que la copia de seguridad es una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en **Agregar** y seleccione **Agregar programación de la combinación**.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

b. Especifique la hora de inicio de la tarea de combinación.

c. Especifique **Hasta** para proporcionar una hora de finalización para la tarea de combinación.

d. Haga clic en **Guardar**.

La programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

Se abre el cuadro de diálogo **Agregar nueva programación del limitador.**

b. Especifique el límite de rendimiento en MB por minuto.

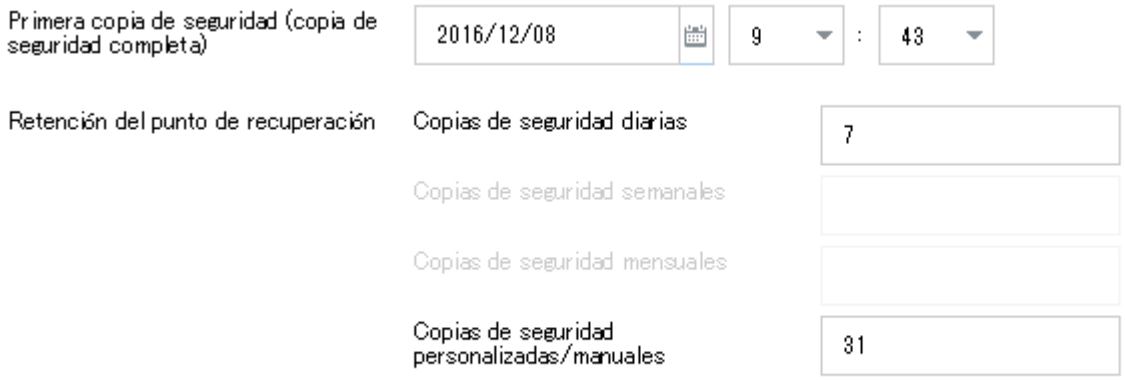
c. Especifique la hora de inicio de la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para proporcionar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

La programación del limitador se especifica y se muestra en la página **Programación**.

2. Especifique la hora de inicio para la copia de seguridad programada.



3. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

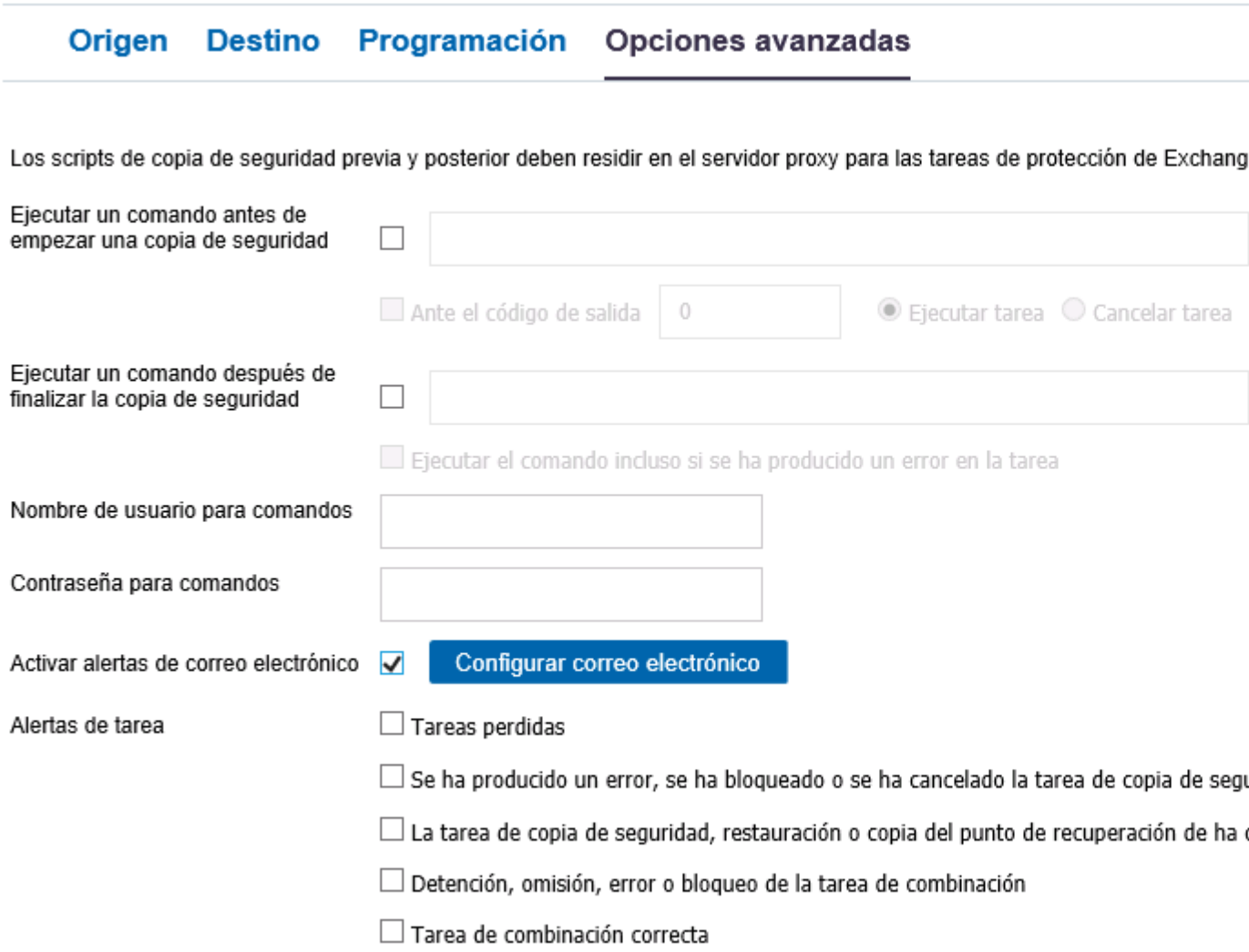
Las opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo **Programación de la copia de seguridad**.

Se especifica la programación.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye proporcionar la ubicación de algunos scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha **Avanzada**:



Siga estos pasos:

1. Especifique los siguientes detalles:

   Ejecutar un comando antes de empezar una copia de seguridad

   Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde está almacenado el script en el nodo del proxy. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de

seguridad continúa cuando el script devuelve el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detiene cuando el script devuelve el código de salida.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta completa donde está almacenado el script.

Ejecutar el comando incluso si se ha producido un error en la tarea

Si se selecciona esta casilla de verificación, el script especificado en **Ejecutar un comando después de finalizar una copia de seguridad** se ejecuta incluso cuando se produce un error en la tarea de copia de seguridad. De lo contrario, este script se ejecuta solamente cuando la tarea de copia de seguridad finaliza correctamente.

Nombre de usuario para comandos

Permite especificar el nombre de usuario para ejecutar los comandos.

Contraseña para comandos

Permite especificar la contraseña para ejecutar los comandos.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy. Para obtener más información sobre cómo configurar Configuración del correo electrónico, consulte la sección Configuración del correo electrónico y alertas.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de alerta de las tareas que se desean recibir.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo del servidor proxy y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera

todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en **Guardar**.

Los cambios se guardan y aparecerá una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar. Se pueden agregar las tareas **Copiar punto de recuperación**, **Copia en cinta**, **Replicar** y **Replicar desde un servidor de puntos de recuperación** como tareas de seguimiento.

El plan se implementa automáticamente en el nodo del servidor proxy.

Se crea el plan de copia de seguridad de SharePoint Online para el servidor proxy. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

(Opcional) Realización de una copia de seguridad manual

Normalmente, en función de la configuración de la programación aplicada, las copias de seguridad se realizan automáticamente. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario. Por ejemplo, si tiene una programación de repetición para las copias de seguridad completas e incrementales y desea hacer cambios importantes en el equipo, puede realizar una copia de seguridad manual inmediata sin necesidad de esperar a la siguiente copia de seguridad programada.

Para realizar una copia de seguridad manual de los nodos de SharePoint Online, siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Los nodos de SharePoint Online se muestran en el panel central.
3. Seleccione los nodos de SharePoint Online (por ejemplo, Mailbox@<nombreorganización.com) de los que se desea realizar la copia de seguridad y que tienen un plan asignado. El nombre del nodo es la cuenta que se utiliza cuando se agrega el nodo de SharePoint Online y se conecta.

4. Haga clic con el botón derecho en el nodo y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.

5. Seleccione el tipo de copia de seguridad que desea realizar y, a continuación, haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.

6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.

7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   La copia de seguridad manual se realiza correctamente.

Para realizar una copia de seguridad manual del plan de SharePoint Online, siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Planes** y, a continuación, haga clic en **Todos los planes**.

   Los planes de copia de seguridad de SharePoint Online se muestran en el panel central.

3. Seleccione el plan del que desea realizar la copia de seguridad y asegúrese de que tiene un plan asignado.
4. Haga clic con el botón secundario del ratón en el plan y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.

5. Seleccione el tipo de copia de seguridad que desea realizar y, a continuación, haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.

6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.

7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   La copia de seguridad manual se realiza correctamente.

Verificación de la copia de seguridad.

Para verificar la tarea de copia de seguridad, confirme que se ha creado correctamente el plan de copia de seguridad. Después de verificar que el plan se ha creado correctamente, confirme si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Se puede verificar el estado de las tareas de copia de seguridad en la ficha **Tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga uno de estos métodos para verificar las tareas de copia de seguridad:

Método 1

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas finalizadas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Método 2

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Tareas correctas**.

   La lista de tareas de copia de seguridad completadas aparecerá en el panel central.
3. Haga clic en la tarea que desea verificar.

   Se actualiza el panel derecho.
4. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
5. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Realización de la configuración de la autenticación multifactor

Cuando una organización tiene la autenticación multifactor (MFA) activada para los usuarios, utilice la autenticación moderna para agregar nodos.

Nota: Aunque la autenticación básica esté activada en el cliente, se puede utilizar la autenticación moderna para agregar nodos. Para obtener más información sobre cómo agregar nodos a un plan mediante la autenticación moderna, consulte Autenticación moderna.

Cómo crear un plan de copia de seguridad de Microsoft Office 365 OneDrive

OneDrive, que forma parte del servicio de la nube de Microsoft Office 365, facilita el proceso de almacenamiento en la nube y el uso compartido de archivos. Para proteger los elementos de OneDrive (archivos, carpetas, etc.) en la nube de Microsoft, se debe crear un plan. El plan para OneDrive está formado por una tarea de copia de seguridad. Esta tarea de copia de seguridad le permite especificar los nodos que se desean proteger, el destino de la copia de seguridad y la programación de la copia de seguridad.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y los requisitos previos
2. Creación de un plan de copia de seguridad de OneDrive
3. (Opcional) Realización de una copia de seguridad manual
4. Realización de la configuración de la autenticación multifactor

Revisión de las consideraciones y del requisito previo

Revise los siguientes requisitos previos y consideraciones antes de crear un plan de copia de seguridad de OneDrive.

Creación de un plan de copia de seguridad de OneDrive:

Requisito previo:

- La ejecución del script de PowerShell está activada en el servidor proxy. Si no está activada, ejecute el comando: *Set-ExecutionPolicy RemoteSigned*
- El servidor proxy debe conectarse con Microsoft Azure.

Consideraciones:

Los servicios de Microsoft Cloud son diferentes de las nubes nacionales del gobierno de Estados Unidos, China y Alemania. Para obtener más detalles, consulte el vínculo. Se deberá modificar la configuración cuando se implemente el producto en estas regiones.

Siga estos pasos:

1. Abra el archivo de configuración cuya ruta sea la ruta de instalación de $UDP.

   $/Engine/Bin/Office365/Arcserve.Office365.Onedrive.json

2. Busque la configuración de **Regiónn** y establezca el valor en Alemania, China o gobierno de Estados Unidos.

   Valor predeterminado: Normal

Creación de un plan de copia de seguridad de OneDrive utilizando la autenticación básica (BA):

Revise lo siguiente:

- Instale PowerShell versión 5.1 o posterior (forma parte de Windows Management Framework (WMF)) en el servidor proxy (equipo de 64 bits).
- Instale los siguientes módulos de PowerShell en el servidor proxy mediante la ventana PowerShell:
  - Para instalar el módulo Azure, ejecute el siguiente comando:

    Install-Module -Name AzureAD -Force
  - Para instalar el módulo ExchangeOnlineManagement, ejecute el siguiente comando:

    Install-Module -Name ExchangeOnlineManagement -Force

  Nota: Cuando se instalan módulos de PowerShell utilizando los comandos anteriores, es posible que se instale una versión más nueva de los módulos en función de la versión de disponibilidad general del componente disponible en el repositorio de Microsoft.

Creación de un plan de copia de seguridad de OneDrive utilizando la autenticación moderna (MA):

Revise los requisitos previos antes de crear un plan utilizando la autenticación moderna.

Creación de un plan de copia de seguridad de OneDrive

Un plan de copia de seguridad incluye una tarea de copia de seguridad que realiza una copia de seguridad de los elementos de datos de OneDrive (archivos, carpetas, etc.) y almacena los datos en un almacén de datos sin deduplicación o en un almacén de datos de deduplicación. Además, este plan de copia de seguridad permite a UDP detectar y especificar los grupos de OneDrive para los que se realiza una tarea de copia de seguridad. Cada tarea está formada por parámetros que definen el origen, destino, programación y otros detalles de la copia de seguridad.

Siga estos pasos:

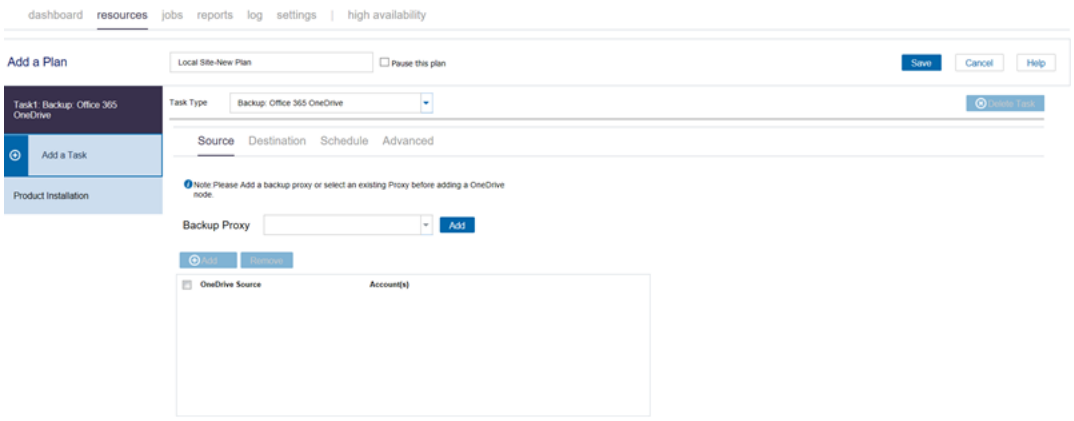
1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre el cuadro de diálogo **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecuta hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable Tipo de tarea seleccione **Copia de Seguridad: Office 365 OneDrive**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

La página Origen le permite especificar los nodos de origen de OneDrive que se desean proteger. Se puede seleccionar más de un nodo de origen de OneDrive en el plan. Si no se han agregado nodos a la Consola, se pueden agregar nodos de origen de OneDrive desde la página Origen.

Nota: Se puede guardar un plan sin agregar nodos de origen pero el plan no se muestra a menos que se agreguen nodos.

Siga estos pasos:

1. Haga clic en la ficha **Origen**.
2. Seleccione **Servidor proxy de copia de seguridad** en la lista desplegable.
3. Agregue el nodo de OneDrive utilizando uno de los siguientes métodos:

   Método 1

   a. Haga clic en **Agregar** y, a continuación, haga clic en **Seleccionar nodos para proteger en Arcserve UDP**.

      Se muestra el cuadro de diálogo Agregar nodos al plan.

   b. Seleccione un nodo y haga clic en **Conectar**.

      Nota: También se pueden buscar los nodos de origen de OneDrive que se desean proteger en Buscar.

   c. Seleccione la casilla de verificación **Proteger todas las cuentas de OneDrive** para proteger todas las cuentas de OneDrive en todas las páginas. Para seleccionar unas pocas cuentas, haga clic en la flecha ubi-

cada en el lado derecho de la casilla de verificación y especifique las cuentas.

Se agregan las cuentas de OneDrive que se han seleccionado.

Método 2

a. Haga clic en **Agregar** y, a continuación, haga clic en **Agregar origen de OneDrive**.

Notas:

- Utilice esta opción para detectar y especificar grupos de distribución para OneDrive.
- A diferencia de otros nodos, no se puede agregar el nodo de OneDrive desde la página Todos los nodos. Solo se puede agregar un nodo de OneDrive a un plan o cuando se modifica un plan.

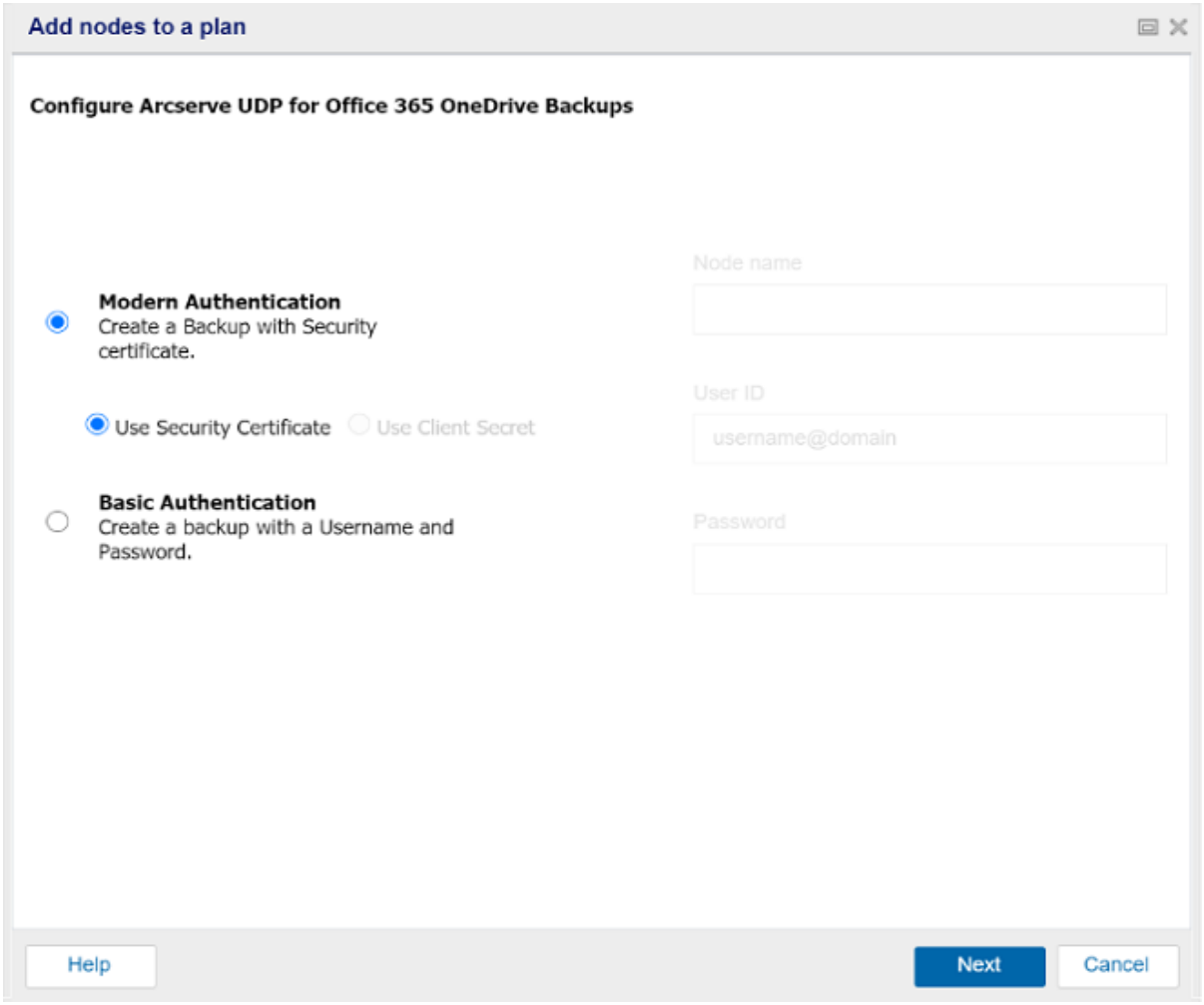
b. Para agregar el nodo de OneDrive por plan, especifique el nombre del nodo, el ID de usuario y la contraseña. No se puede cambiar el nombre de nodo después de crear el nodo de OneDrive. Varios nodos de OneDrive pueden utilizar la misma cuenta de usuario (cuenta de servicio) de OneDrive.

Nota: Se recomienda seleccionar cuentas de usuario del grupo de administradores de Azure Active Directory.

4. Para aplicar la autenticación, realice una de las siguientes acciones:

Autenticación moderna

Para la autenticación moderna, se puede ejecutar una copia de seguridad con un certificado de seguridad.



Utilizar certificado de seguridad

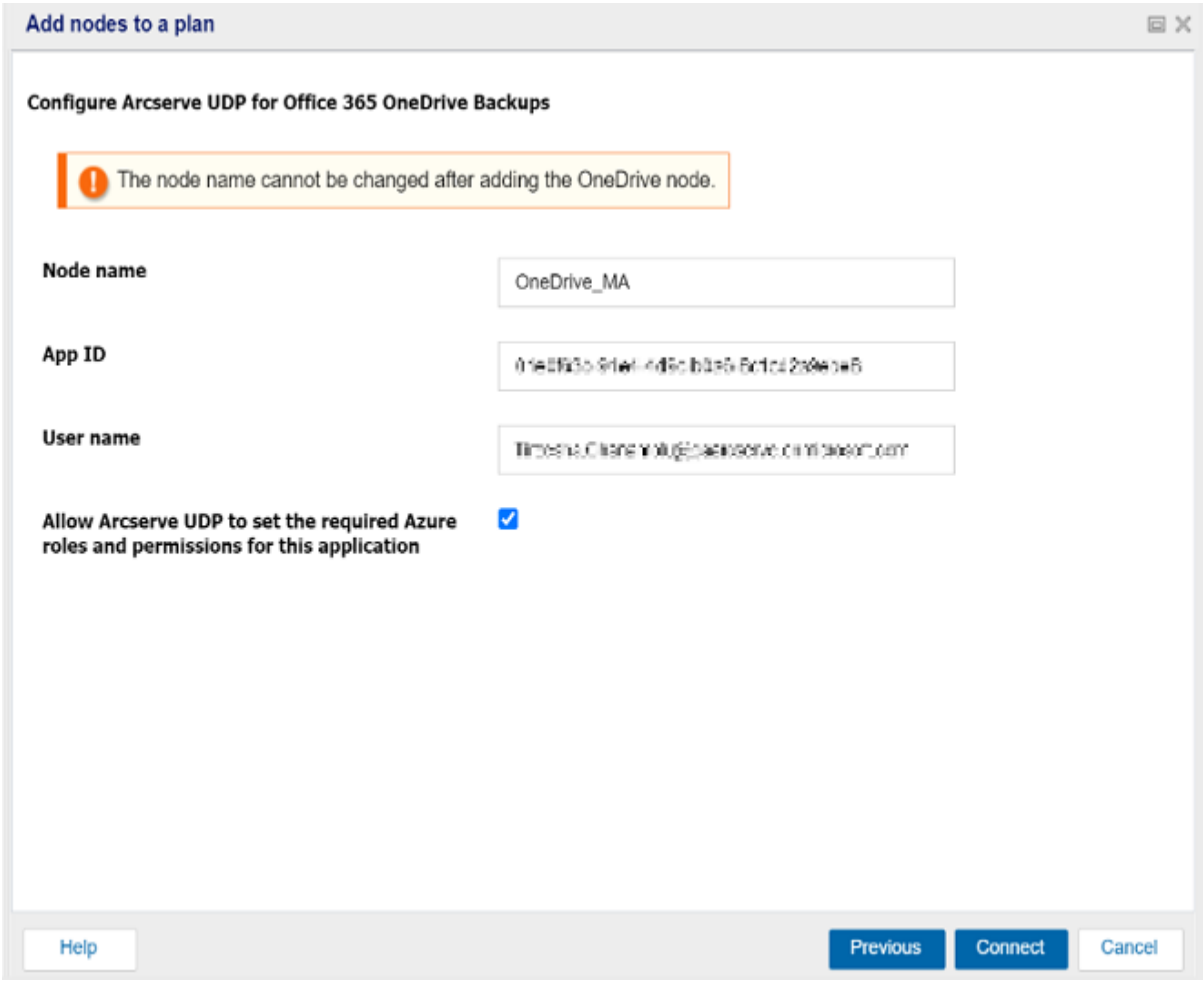
Nota: De forma predeterminada, el plan de copia de seguridad selecciona **Utilizar certificado de seguridad** para la autenticación moderna.

Siga estos pasos:

a. Para autenticar la aplicación de UDP con certificados de seguridad, consulte Descarga del certificado de UDP y carga del certificado en Azure.

b. Introduzca los siguientes detalles:

- Nombre de nodo
- ID de aplicación
- Nombre de usuario



Nota: Los nombres de nodo de OneDrive no se pueden cambiar después de crear un nodo.

c. Para aplicar los permisos de API automáticamente, seleccione la casilla de verificación **Permitir que Arcserve UDP establezca los permisos de la API necesarios para esta aplicación**.

Nota: Para aplicar los permisos manualmente sin utilizar el rol de administrador global o de la compañía, consulte Configuración de los permisos de la API manualmente sin utilizar el rol de administrador global o de la compañía.

d. Haga clic en **Conectar**.

Autenticación básica

Para la autenticación básica, para continuar con la copia de seguridad, siga estos pasos:

a. Seleccione Autenticación básica, especifique el Nombre de nodo, el Nombre de usuario y la Contraseña y, a continuación, haga clic en **Conectar**.

   La dirección URL de Arcserve UDP se abre en un explorador y solicita permiso para todos los datos de lectura y escritura de Arcserve UDP desde el portal de OneDrive.

b. En el explorador, utilice las credenciales de administrador de Microsoft Azure para iniciar sesión.

   Se abrirá el portal de Azure.

c. En el portal de Microsoft Azure, realice los pasos siguientes para configurar la aplicación de UDP:

   I. Haga clic en **Permisos de API**.

   ii. En el panel derecho, haga clic en el botón **Conceder permisos a**.

   iii. Haga clic en **Sí** para estar de acuerdo con la concesión de permisos.

   iv. Después de conceder el permiso, en Arcserve UDP, vaya a **Agregar un plan > Agregar nodos a un plan** y, a continuación, haga clic en el botón **Siguiente**.

Nota: Si cierra la dirección URL del permiso de concesión y desea volver a abrirla, haga clic en el botón Aquí en la pantalla Agregar nodo al plan de UDP.

Arcserve UDP enumera todas las cuentas que se encuentran en el cliente actual.

5. Para proteger las cuentas de OneDrive, realice una de las siguientes acciones:

   - Para proteger todas las cuentas y grupos de OneDrive, seleccione la casilla de verificación **Proteger todas las cuentas de OneDrive**.

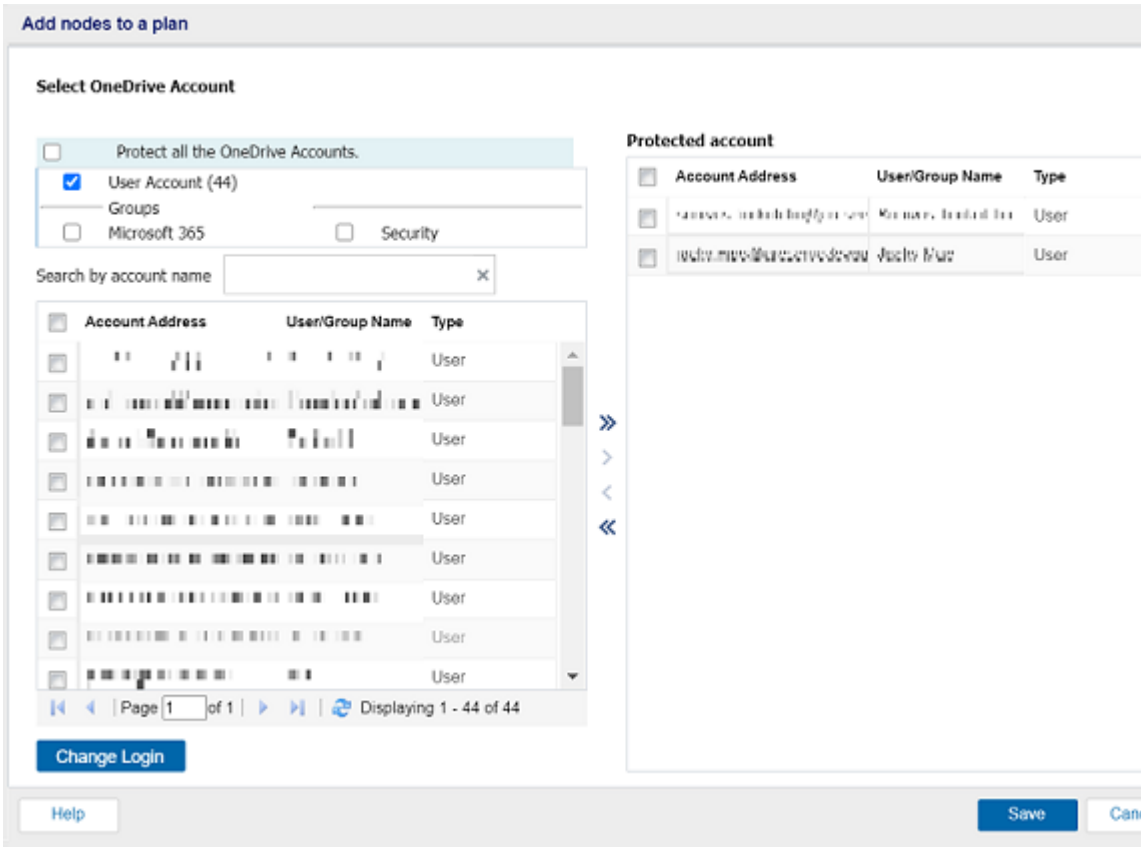
     Nota: Esta opción está seleccionada automáticamente de forma predeterminada cuando aparece la pantalla Seleccionar cuenta de OneDrive.

   - Para la Cuenta de usuario, siga estos pasos:

     a. Seleccione la casilla de verificación **Cuenta de usuario**.

        Aparece una lista de cuentas de usuario.

b. (Opcional) Para buscar una cuenta en la lista, en el campo Buscar por nombre de cuenta escriba el nombre de la cuenta.



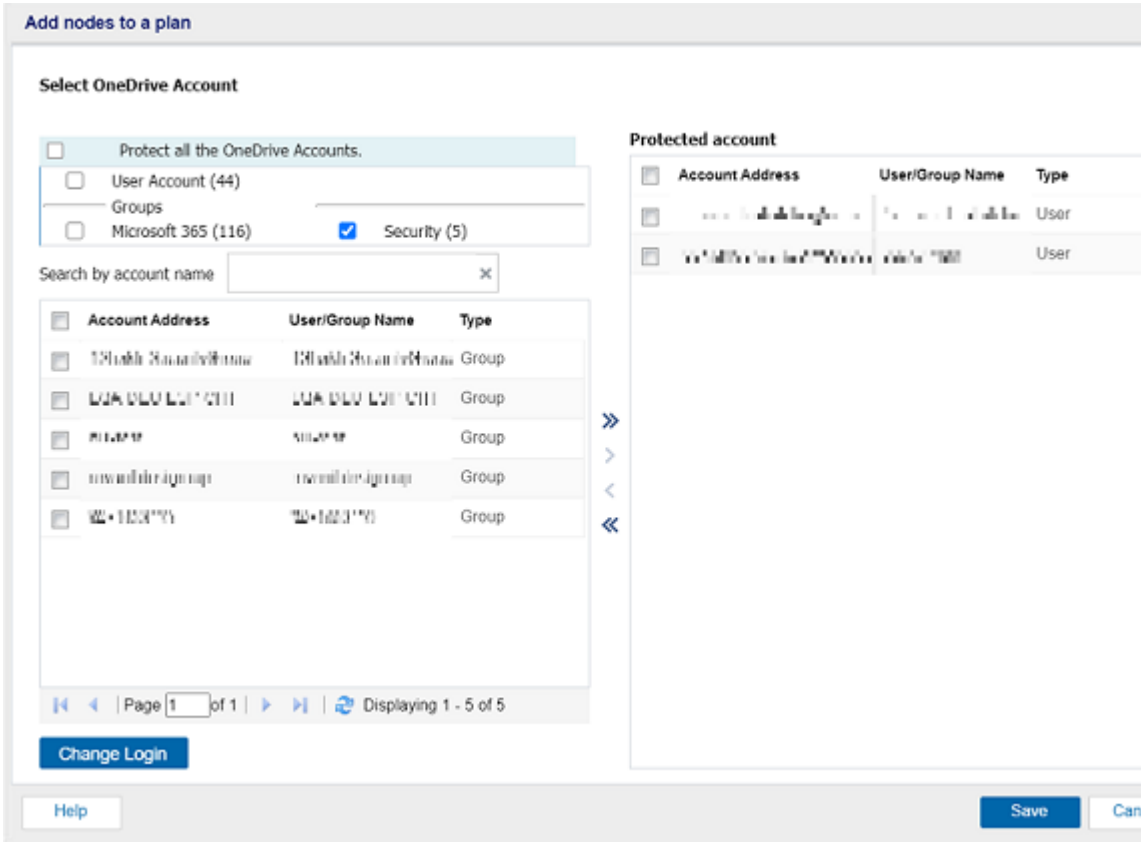
c. En la lista de cuentas de usuario, seleccione las cuentas que desea proteger.

d. Haga clic en la flecha hacia la derecha (>) para mover las cuentas seleccionadas a la lista de cuentas protegidas.

- Para obtener los grupos, siga estos pasos:

  a. Seleccione la casilla de verificación **Microsoft 365** o **Seguridad**.

  En función de la selección, aparece una lista de grupos.



b. (Opcional) Para buscar una cuenta en la lista, en el campo Buscar por nombre de cuenta escriba el nombre de la cuenta.

c. En la lista de grupos, seleccione los grupos que desea proteger.

d. Haga clic en la flecha hacia la derecha (>) para mover los grupos seleccionados a la lista de cuentas protegidas.

6. Haga clic en **Guardar**.

   Se agregan las cuentas de OneDrive seleccionadas.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Haga clic en la ficha **Destino**.

   La opción **Servidor de puntos de recuperación de Arcserve UDP** está seleccionada automáticamente. **Servidor de puntos de recuperación de Arcserve UDP** especifica que el destino de la copia de seguridad es un servidor de puntos de recuperación.

Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.

2. Proporcione los siguientes detalles:
    a. Seleccione un servidor de puntos de recuperación.
    b. Seleccione un almacén de datos sin deduplicación o de deduplicación. La lista muestra todos los almacenes de datos que se han creado en el servidor de puntos de recuperación especificado.
    c. Proporcione una contraseña de la sesión. La contraseña de sesión es opcional cuando el destino de copia de seguridad es un almacén de datos del servidor de puntos de recuperación no cifrado.
    d. Confirme la contraseña de la sesión.

    Se especifica el destino. Ahora especifique los detalles de los campos Programación y Avanzada.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y se pueden proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

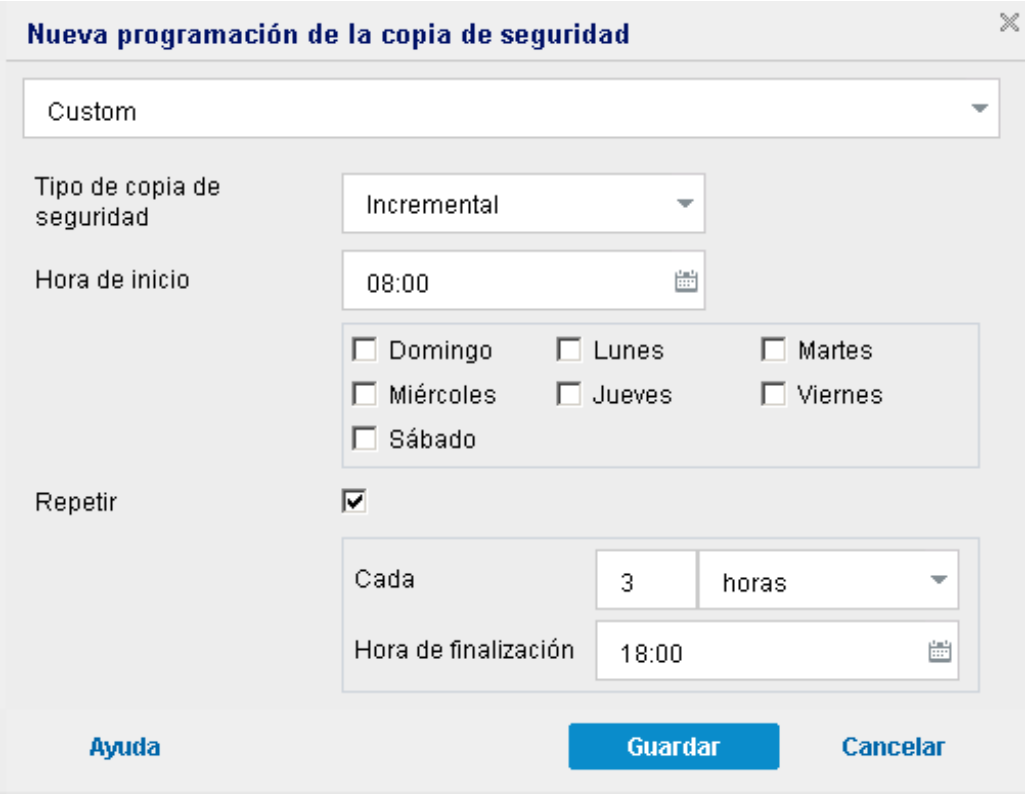
Siga estos pasos:

1. Agregue las programaciones de la copia de seguridad, de la combinación y del regulador.

    Agregar programación de la copia de seguridad

    a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

        Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de las copias de seguridad incrementales consisten en que la copia de seguridad es una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Esta opción es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en **Agregar** y seleccione **Agregar programación de la combinación**.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

b. Especifique la hora de inicio para iniciar la tarea de combinación.

c. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

d. Haga clic en **Guardar**.

La programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

Se abre el cuadro de diálogo **Agregar nueva programación del limitador.**

b. Especifique el límite de rendimiento en MB por minuto.

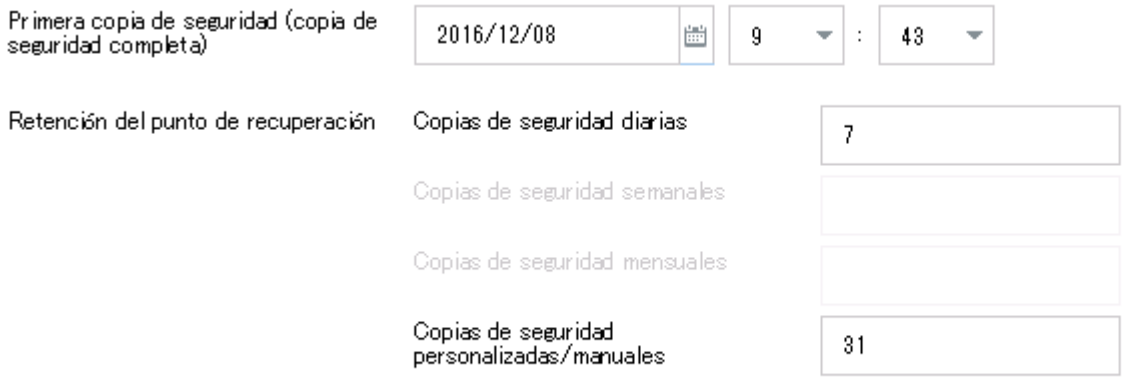
c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

La programación del limitador se especifica y se muestra en la página **Programación**.

2. Especifique la hora de inicio para la copia de seguridad programada.



3. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

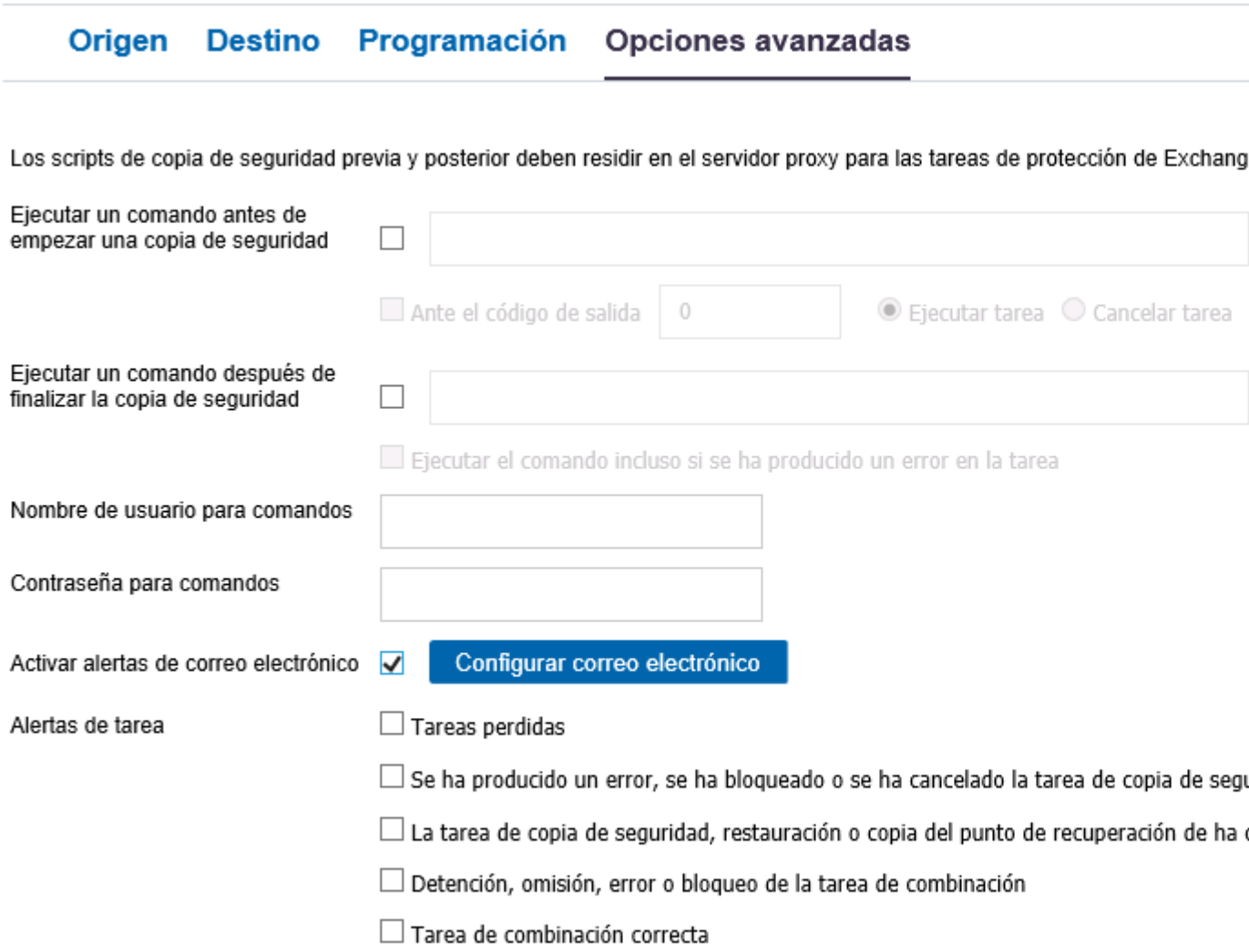
Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo **Programación de la copia de seguridad**.

Se especifica la programación. Ahora especifique los detalles del campo Avanzada.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye proporcionar la ubicación de algunos scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha **Avanzada**:



Siga estos pasos:

1. Especifique los siguientes detalles:

   Ejecutar un comando antes de empezar una copia de seguridad

   Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde está almacenado el script en el nodo del proxy. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de seguridad continúa cuando el script devuelve el código de salida. **Cancelar**

tarea indica que la tarea de copia de seguridad se detiene cuando el script devuelve el código de salida.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta completa donde está almacenado el script.

Ejecutar el comando incluso si se ha producido un error en la tarea

Si se selecciona esta casilla de verificación, el script especificado en **Ejecutar un comando después de finalizar una copia de seguridad** se ejecuta incluso cuando se produce un error en la tarea de copia de seguridad. De lo contrario, este script se ejecuta solamente cuando la tarea de copia de seguridad finaliza correctamente.

Nombre de usuario para comandos

Permite especificar el nombre de usuario para ejecutar los comandos.

Contraseña para comandos

Permite especificar la contraseña para ejecutar los comandos.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy. Para obtener más información sobre cómo configurar Configuración del correo electrónico, consulte la sección Configuración del correo electrónico y alertas.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de alerta de las tareas que se desean recibir.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo del servidor proxy y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo

tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en **Guardar**.

Los cambios se guardan y aparecerá una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar. Se pueden agregar las tareas **Copiar punto de recuperación**, **Copia en cinta**, **Replicar** y **Replicar desde un servidor de puntos de recuperación** como tareas de seguimiento.

El plan se implementa automáticamente en el nodo del servidor proxy.

Se crea el plan de copia de seguridad de Exchange Online para el servidor proxy. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

(Opcional) Realización de una copia de seguridad manual

Normalmente, en función de la configuración de la programación aplicada, las copias de seguridad se realizan automáticamente. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario. Por ejemplo, si tiene una programación de repetición para las copias de seguridad completas e incrementales y desea hacer cambios importantes en el equipo, puede realizar una copia de seguridad manual inmediata sin necesidad de esperar a la siguiente copia de seguridad programada. Se puede enviar la tarea de copia de seguridad desde la interfaz de usuario de la Consola y del servidor proxy. Si utiliza el controlador de tareas, podrá ver el estado de la tarea y cancelar la tarea en curso.

para realizar una copia de seguridad manual de los nodos de OneDrive, Siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Los nodos de OneDrive se muestran en el panel central.
3. Seleccione los nodos de OneDrive de los que desea realizar la copia de seguridad y que tienen un plan asignado.
4. En el panel central, haga clic en **Acciones**, **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo **Ejecutar ahora una copia de seguridad**.

5. Seleccione un tipo de copia de seguridad y opcionalmente proporcione un nombre para la tarea de copia de seguridad.
6. Haga clic en **Aceptar**.

   Se ejecuta la tarea de copia de seguridad.

Siga estos pasos: para realizar una copia de seguridad manual de un plan de OneDrive

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Los planes de copia de seguridad de OneDrive se muestran en el panel central.
3. Seleccione el plan del que desea realizar la copia de seguridad y asegúrese de que tiene un plan asignado.
4. En el panel central, haga clic en **Acciones**, **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo **Ejecutar ahora una copia de seguridad**.
5. Seleccione un tipo de copia de seguridad y opcionalmente proporcione un nombre para la tarea de copia de seguridad.
6. Haga clic en **Aceptar**.

   Se ejecuta la tarea de copia de seguridad.

   La copia de seguridad manual se realiza correctamente. Ahora se puede verificar la copia de seguridad.

Verificación de la copia de seguridad.

Para verificar la tarea de copia de seguridad, confirme que se ha creado correctamente el plan de copia de seguridad. Después de verificar que el plan se ha creado correctamente, confirme si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Se puede verificar el estado de las tareas de copia de seguridad en la ficha **Tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

   Siga uno de estos métodos para verificar las tareas de copia de seguridad:

   Método 1

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas finalizadas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

   Método 2
1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Tareas correctas**.

   La lista de tareas de copia de seguridad completadas aparecerá en el panel central.
3. Haga clic en la tarea que desea verificar.

   Se actualiza el panel derecho.
4. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
5. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Realización de la configuración de la autenticación multifactor

Cuando una organización tiene la autenticación multifactor (MFA) activada para los usuarios, utilice la autenticación moderna para agregar nodos.

Nota: Aunque la autenticación básica esté activada en el cliente, se puede utilizar la autenticación moderna para agregar nodos. Para obtener más información sobre cómo agregar nodos a un plan mediante la autenticación moderna, consulte Autenticación moderna.

Gestión de la copia de seguridad y la restauración de Microsoft Teams

Esta sección proporciona información sobre cómo realizar copias de seguridad y restauraciones de los datos de Microsoft Teams utilizando Exchange Online y SharePoint Online. Arcserve UDP proporciona la copia de seguridad de mensajes (chats) y archivos compartidos a través de los canales privados, públicos y de grupo.

Siempre que se crea un canal de grupo, público o privado en Microsoft Teams, se crea automáticamente un sitio de SharePoint Online. Este sitio de SharePoint Online tiene una carpeta de biblioteca de documentos predeterminada, en la que se guardan automáticamente todos los archivos compartidos en todas las conversaciones. También se pueden personalizar los permisos y las opciones de seguridad para proteger la información confidencial.

Esta sección incluye los siguientes temas:

Cómo realizar una copia de seguridad y restauración de los mensajes (chats) de Microsoft Teams utilizando Exchange Online

Se puede realizar una copia de seguridad de los chats individuales utilizando el buzón de correo del usuario en la copia de seguridad del nodo de Exchange Online de UDP. Todos los mensajes se almacenan en Exchange Online Server en la carpeta TeamsMessagesData, que se encuentra en una carpeta de raíz. Esta sección proporciona información sobre cómo restaurar y realizar copias de seguridad de mensajes de Microsoft Teams (chats) utilizando Exchange Online.

Esta sección incluye los siguientes temas:

Copia de seguridad de los mensajes (chats) de Microsoft Teams utilizando Exchange Online

Esta sección proporciona información sobre cómo realizar una copia de seguridad de los mensajes (chats) de Microsoft Teams utilizando Exchange Online.

Esta sección incluye los siguientes temas:

Cómo crear un plan de copia de seguridad de Exchange Online

Exchange Online es una aplicación de correo electrónico que se aloja en la nube de Microsoft. Para proteger los elementos de correo de Exchange Online (correos, elementos del calendario, contactos, etc.) desde la nube de Microsoft, es necesario crear un plan. El plan para Exchange Online está formado por una tarea de copia de seguridad. Esta tarea de copia de seguridad le permite especificar los nodos de Exchange Online que se desean proteger, el destino de la copia de seguridad y la programación de la copia de seguridad.

Esta sección incluye los siguientes temas:

Revisión de las consideraciones y requisitos previos

Revise las consideraciones y los requisitos previos antes de crear un plan de copia de seguridad de Exchange Online.

Creación de un plan de copia de seguridad de Exchange Online:

Requisitos previos:

Para la cuenta de la copia de seguridad:

- Utilice una cuenta de servicio de copia de seguridad con permisos de administrador globales.
- Agregue el permiso de suplantación para el usuario de la copia de seguridad a la cuenta de la copia de seguridad de Exchange Online para conectar la organización de Exchange Online, realizar copias de seguridad y restaurar.

  Nota: Si no se agrega la cuenta de la copia de seguridad al grupo de rol de gestión de la detección y no se asigna el permiso de suplantación de la aplicación, se producirá un error en la copia de seguridad.

- Asocie la cuenta del usuario de la copia de seguridad con un buzón de Exchange Online.

Para el proxy de la copia de seguridad:

- Inicie sesión en la consola.
- Instale el Agente de Arcserve UDP en el equipo proxy donde se desea ejecutar la copia de seguridad o la restauración.

Consideraciones:

- Al realizar la copia de seguridad de un conjunto grande de usuarios, puede utilizar grupos de Exchange para mejorar la copia de seguridad y la optimización.
- La configuración predeterminada para la copia de seguridad Exchange Online utiliza 4 subprocesos de copia de seguridad (un subproceso por usuario) a la vez. También se pueden modificar los subprocesos en el archivo de configuración de *Engine\BIN\Office365\Arcserve.Office365.Exchange.config*como sigue:

```
<!--#region for multi thread--> <!--MultiThreadEnable default
value:0. if enable, set 1.--> <add

                                                    <add
```

```
<!--set how many thread will be used to backup mailbox.
default value is 4--
> key="MaxDegreeOfParallelismForMailbox" value="4"/> <add
key="MaxDegreeOfParallelismForMailbox" value="4"/> <!--#en-
dregion-->
```

Se recomienda establecer el valor de 1 a 5. El valor máximo posible es 10. Pero no se recomienda establecer el valor de 6 a 10.

Nota: UDP 8.0 admite lo siguiente:

- Buzón de correo del usuario
- Buzón de correo compartido
- Carpetas públicas habilitadas para el correo
- Buzones de correo de sala
- Buzones de correo de equipamiento
- Buzones de correo de grupo

Nota: Para obtener más información sobre las prácticas recomendadas para Exchange Online, consulte.Relacionados con Exchange Online.

Creación de un plan de copia de seguridad de Exchange Online utilizando la autenticación básica (BA):

Revise los siguientes requisitos previos:

- Instale PowerShell versión 5.1 o posterior (forma parte de Windows Management Framework (WMF)) en el servidor proxy (equipo de 64 bits).
- Instale los siguientes módulos de PowerShell en el servidor proxy mediante la ventana PowerShell:
  - Para instalar el módulo Azure, ejecute el siguiente comando:

    Install-Module -Name AzureAD -Force
  - Para instalar el módulo ExchangeOnlineManagement, ejecute el siguiente comando:

    Install-Module -Name ExchangeOnlineManagement -Force

Nota: Cuando se instalan módulos de PowerShell utilizando los comandos anteriores, es posible que se instale una versión más nueva de los módulos en función de la versión de disponibilidad general del componente disponible en el repositorio de Microsoft.

Creación de un plan de copia de seguridad de Exchange Online utilizando la autenticación moderna (MA):

Revise los requisitos previos antes de crear un plan utilizando la autenticación moderna.

Adición del rol y del grupo necesarios a la cuenta de copia de seguridad de Exchange Online para realizar la copia de seguridad y la restauración

Agregue la cuenta de copia de seguridad al grupo de rol de gestión de la detección y asígnele el permiso de suplantación de la aplicación.

Siga estos pasos:

1. Agregue el rol y el grupo necesarios mediante cualquiera de las formas siguientes:

   Utilización del portal Office 365

a. Inicie sesión en el Portal Office 365 como administrador o con una cuenta que disponga de permisos de administrador global.

   Se abre la página Centro de administración de Exchange.

b. Vaya a los **permisos** y, en la lista desplegable Agregar, haga doble clic en **Administración de detecciones**.

   Aparecerá el cuadro de diálogo Administración de detecciones.

   Nota: Un miembro del grupo de rol de la Administración de detecciones puede realizar búsquedas de buzones de correo en la organización de Exchange para buscar los datos que se adapten a unos criterios específicos.

c. En **Roles**, haga clic en **+** para agregar el rol ApplicationImpersonation.

   Aparecerá el cuadro de diálogo Seleccionar un rol.

d. En la lista desplegable **Nombre para mostrar**, seleccione **ApplicationImpersonation**.

   Nota: El rol ApplicationImpersonation permite que las aplicaciones suplanten a usuarios en una organización para realizar las tareas en nombre del usuario.

e. Haga clic en **Agregar** para agregar el rol ApplicationImpersonation y, a continuación, haga clic en **Aceptar**.

f. En el cuadro de diálogo Administración de detección, en **Miembros**, haga clic en **+** para agregar la cuenta de la copia de seguridad como miembro.

   Aparecerá el cuadro de diálogo Seleccionar miembros.

g. En el menú desplegable Nombre, seleccione la cuenta de copia de seguridad, haga clic en **Agregar** para agregar el miembro y, a continuación, haga clic en **Aceptar**.

   La cuenta de copia de seguridad seleccionada se muestra en **Miembros** en el cuadro de diálogo **Gestión de la detección**.

h. Haga clic en **Guardar**.

Uso de PowerShell remoto

a. Para conectarse al cliente de Exchange Online mediante PowerShell remoto, consulte el vínculo.

b. Una vez conectado, para agregar la cuenta de copia de seguridad como miembro del grupo de rol de la gestión de la detección, debe utilizar el siguiente comando:

   `"Add-RoleGroupMember" cmdlet`

   Por ejemplo: Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.

c. Para asignar el rol de suplantación de la aplicación a la cuenta de copia de seguridad, utilice el comando:

   `"New-ManagementRoleAssignment" cmdlet`

   Por ejemplo:

   New-ManagementRoleAssignment -Name: impersonationAssignmentName -Role:ApplicationImpersonation - User: "username@domain.onmicrosoft.com"

El rol ApplicationImpersonation y el grupo de miembros se agregan a la cuenta de copia de seguridad de Exchange Online.

Creación de un plan de copia de seguridad de Exchange Online

Un plan de copia de seguridad incluye una tarea de copia de seguridad que realiza una copia de seguridad de los elementos de datos del correo de Exchange Online (correos, elementos del calendario, contactos, etc.) y almacena los datos en un almacén de datos sin deduplicación o en un almacén de datos de deduplicación. Además, este plan de copia de seguridad permite a UDP detectar y especificar los grupos de Exchange Online para los que se realiza una tarea de copia de seguridad. Cada tarea está formada por parámetros que definen el origen, destino, programación y otros detalles de la copia de seguridad.

Siga estos pasos:

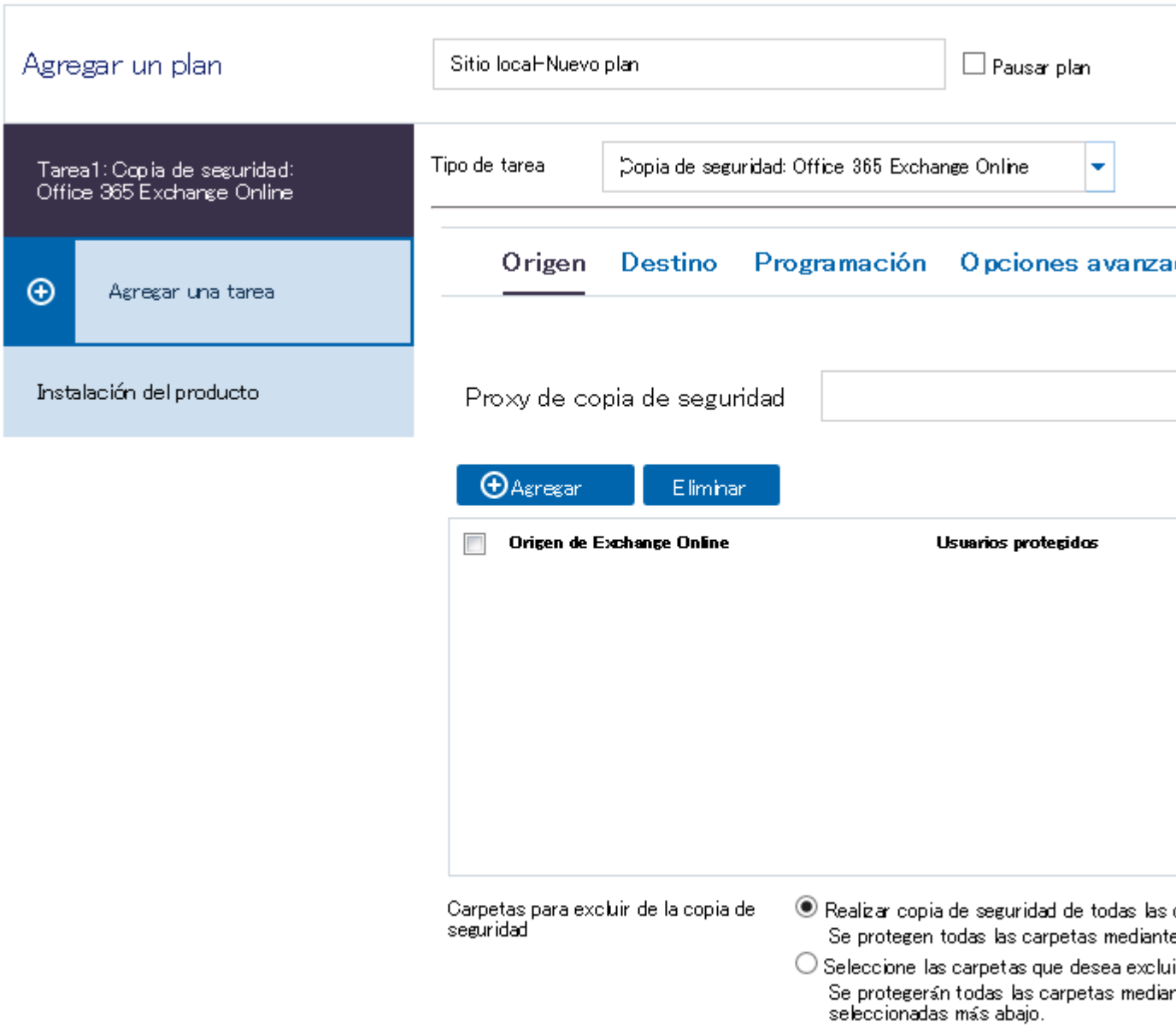
1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre el cuadro de diálogo **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecuta hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable Tipo de tarea seleccione **Copia de Seguridad: Office 365 Exchange Online**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

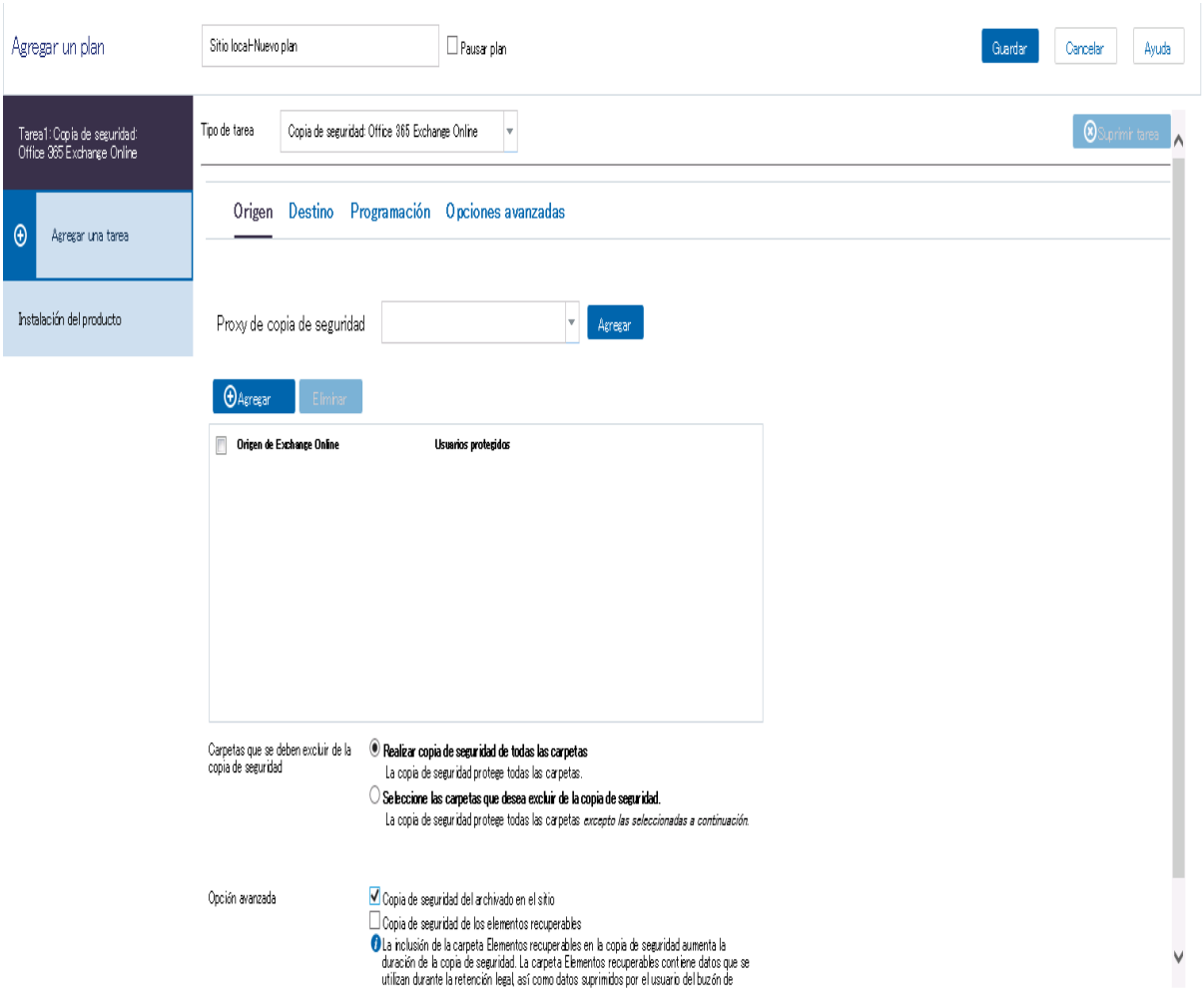
La página Origen le permite especificar los nodos de origen de Exchange Online que se desean proteger. Se puede seleccionar más de un nodo de origen de Exchange Online en el plan. Si no se han agregado nodos a la Consola, se pueden agregar nodos de origen de Exchange Online desde la página Origen.

Nota: Se puede guardar un plan sin agregar nodos de origen pero el plan no se muestra a menos que se agreguen nodos.

También se pueden gestionar los nodos de Exchange Online utilizando Compatibilidad con el buzón de correo de la carpeta pública para la protección de Exchange Online.

Siga estos pasos:

1. Haga clic en la ficha **Origen**.



2. Para el servidor proxy de la copia de seguridad, realice una de las siguientes acciones:
   - En la lista desplegable, seleccione un servidor proxy de la copia de seguridad existente.
   - Para agregar un nuevo servidor proxy de la copia de seguridad, haga clic en **Agregar** junto a la lista desplegable.
3. Agregue el nodo de Exchange Online utilizando una de las siguientes opciones:

   Método 1

   a. Haga clic en **Agregar** y, a continuación, haga clic en **Seleccionar nodos para proteger en Arcserve UDP**.

      Se muestra el cuadro de diálogo Agregar nodos al plan.

   b. Seleccione un nodo y haga clic en **Conectar**.

      Nota: También se pueden buscar los nodos de origen de Exchange Online que se desean proteger en **Buscar**.

   c. Seleccione la casilla de verificación **Proteger todo el origen de Office 365 Exchange** para proteger todas las cuentas de Exchange Online en todas las páginas.

      Nota: Para agregar todas las cuentas de Exchange Online a la lista protegida, se puede hacer clic en la flecha hacia la derecha (>).

      Se agregan las cuentas de Exchange Online que se han seleccionado.

   Método 2

   - Haga clic en **Agregar** y, a continuación, haga clic en **Agregar origen de Exchange Online**.

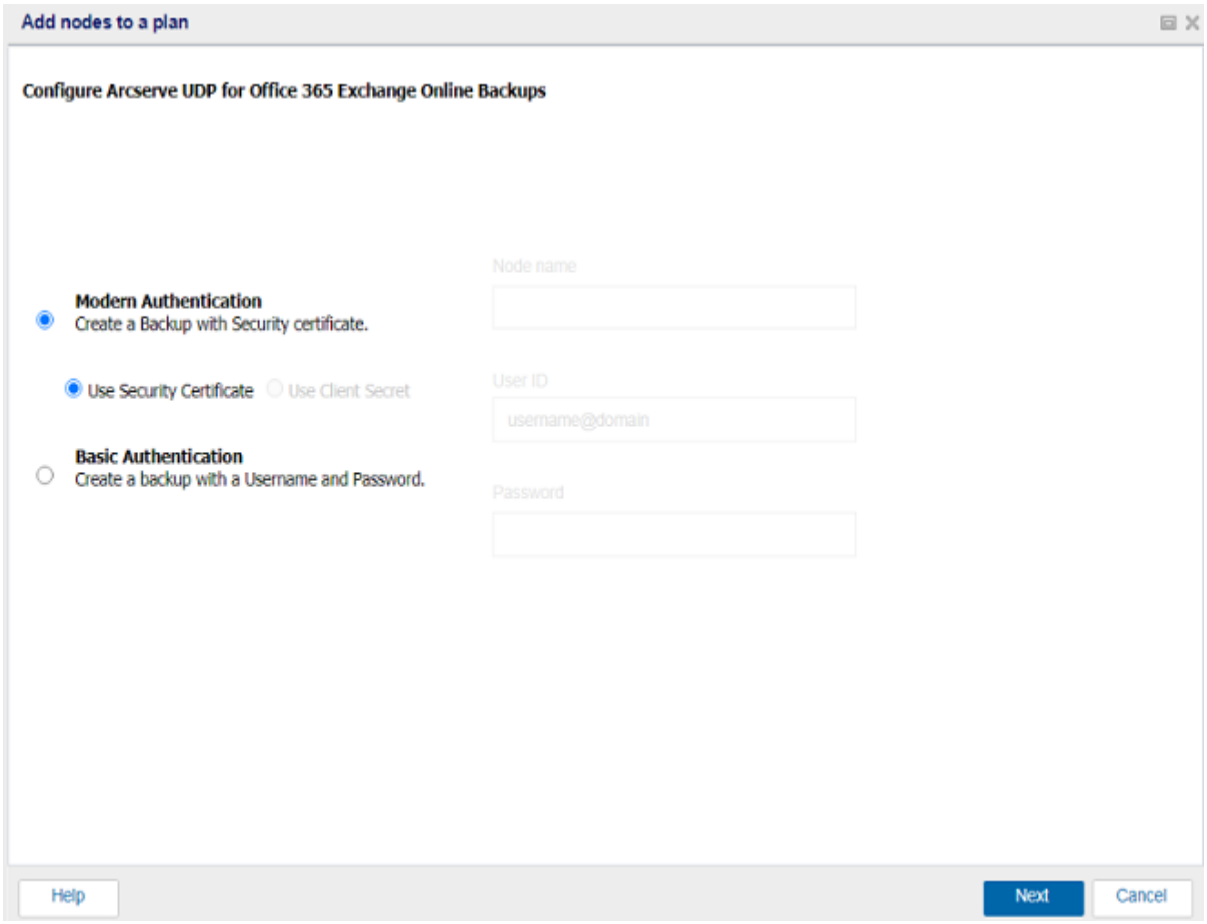
     Aparece el cuadro de diálogo Agregar nodos a un plan.

     Nota: A diferencia de otros nodos, no se puede agregar el nodo de Exchange Online desde la página **Todos los nodos**. Solo se puede agregar un nodo de Exchange Online a un plan o cuando se modifica un plan.

     Varios nodos de Exchange Online pueden utilizar la misma cuenta de usuario (cuenta de servicio) de Exchange Online.
4. Para aplicar la autenticación, realice una de las siguientes acciones:

Autenticación moderna

Para la autenticación moderna, se puede ejecutar una copia de seguridad con un certificado de seguridad.



Utilizar certificado de seguridad

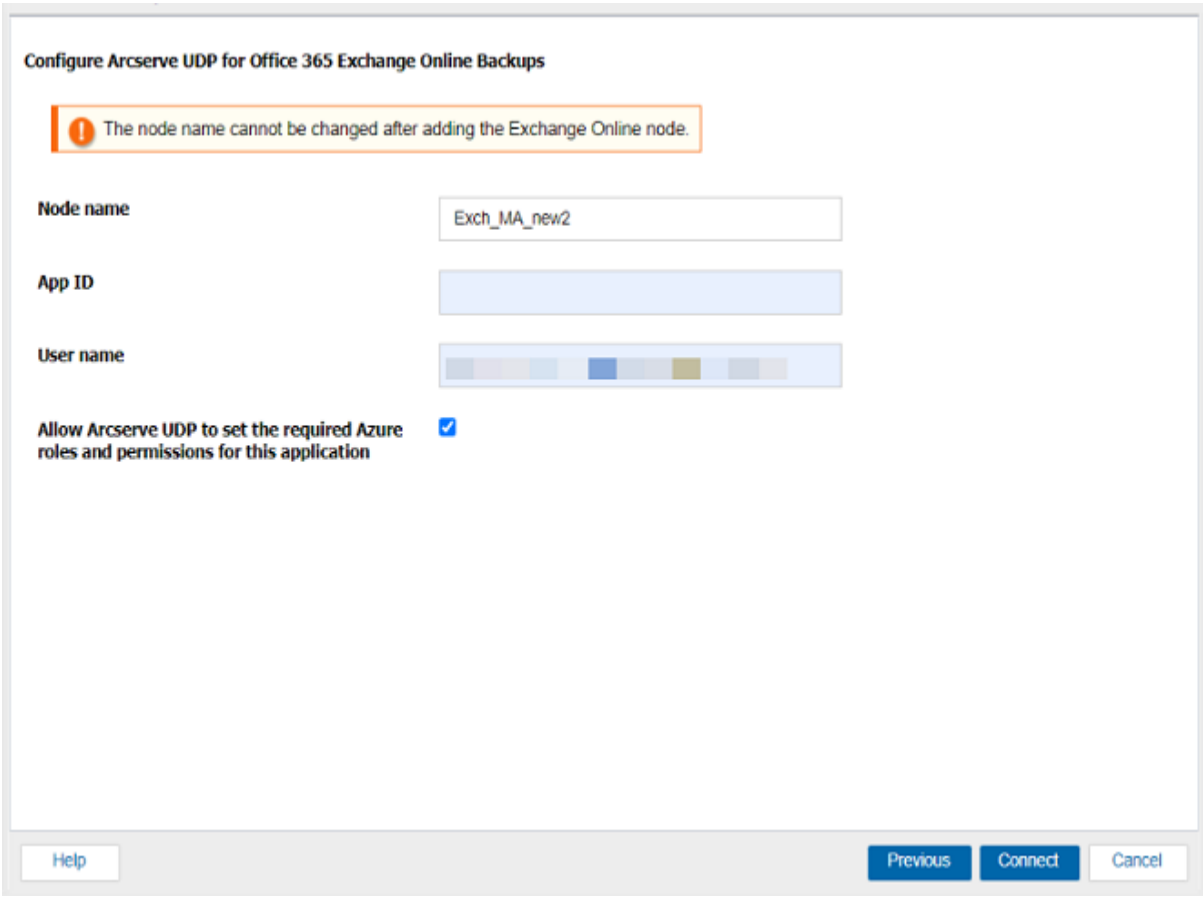
Nota: De forma predeterminada, el plan de copia de seguridad selecciona **Utilizar certificado de seguridad** para la autenticación moderna.

Siga estos pasos:

a. Para autenticar la aplicación de UDP con certificados de seguridad, consulte Descarga del certificado de UDP y carga del certificado en Azure.

b. Introduzca los siguientes detalles:

- Nombre de nodo
- ID de aplicación
- Nombre de usuario



c. Para aplicar los permisos de API automáticamente, seleccione la casilla de verificación **Permitir que Arcserve UDP establezca los permisos de la API necesarios para esta aplicación**.

   Nota: Para aplicar los permisos manualmente sin utilizar el rol de administrador global o de la compañía, consulte Configuración de los permisos de la API manualmente sin utilizar el rol de administrador global o de la compañía.

d. Haga clic en **Conectar**.

Notas:

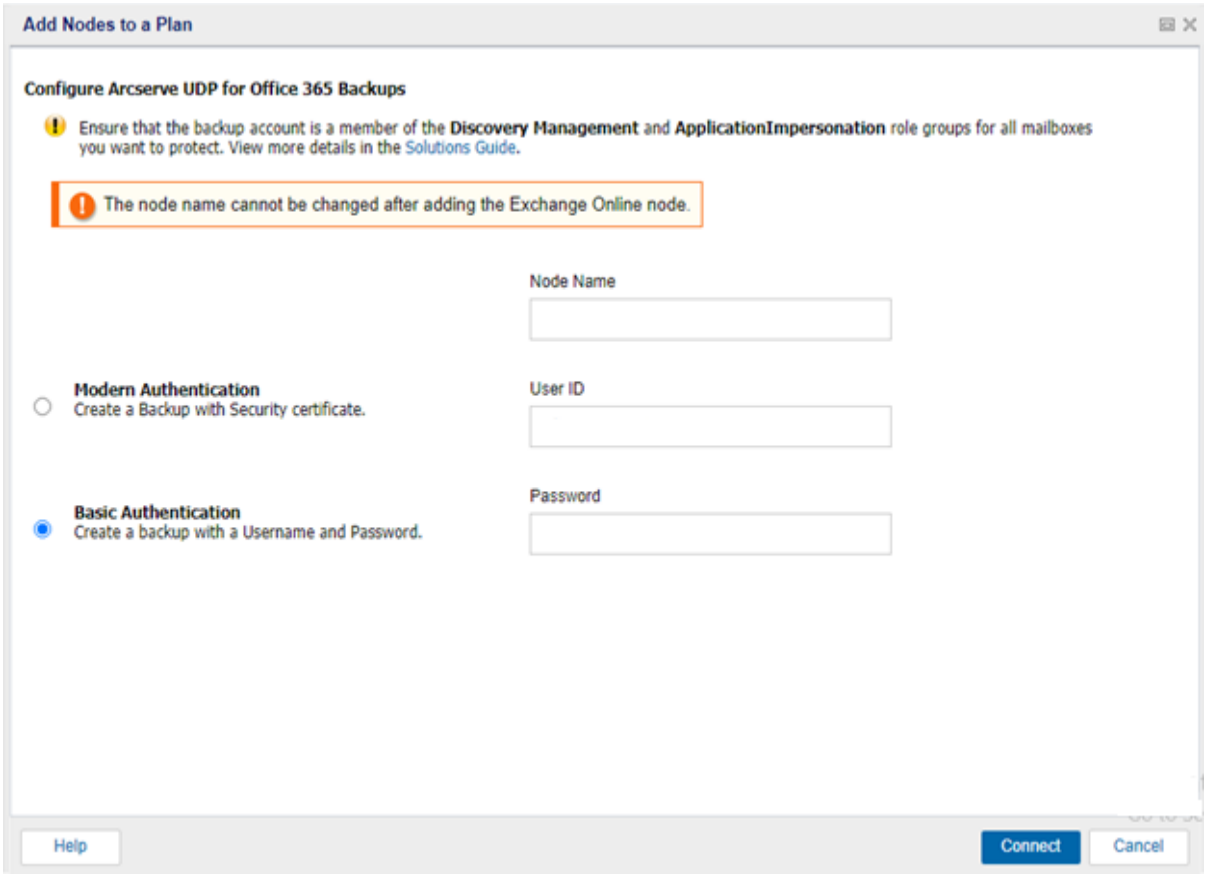
- El nombre del nodo de Exchange Online no se puede cambiar después de agregar el nodo.
- Introduzca el nombre de usuario de la cuenta de copia de seguridad de Exchange Online que cumpla los requisitos previos en **Nombre de usuario del administrador**.
- La autenticación moderna no se aplica a lo siguiente:

- Los clientes que utilizan Microsoft 365 (Office 365) para sus instancias de Arcserve Cloud Hybrid o Arcserve Cloud Backup para Office 365, que se creó antes del 18 de octubre de 2020, no permiten la autenticación moderna.
- Los clientes que continúan utilizando la autenticación básica.

Autenticación básica

Para la autenticación básica, para continuar con la copia de seguridad, proporcione la siguiente información y, a continuación, haga clic en **Conectar**:

- Nombre de nodo
- ID de usuario
- Contraseña



Nota: Es posible que al realizar una actualización o cambio en la cuenta de usuario se pueda cambiar el número de buzones de correo protegidos. Se debe comprobar que las cuentas de servicio nuevas o actualizadas tienen derechos de suplantación para que los buzones puedan estar protegidos.

5. Para proteger los buzones de correo de Exchange Online, realice una de las siguientes acciones:

   - Para proteger todos los grupos y buzones de correo de Exchange Online, seleccione la casilla de verificación **Proteger todo el origen de Office 365 Exchange**.

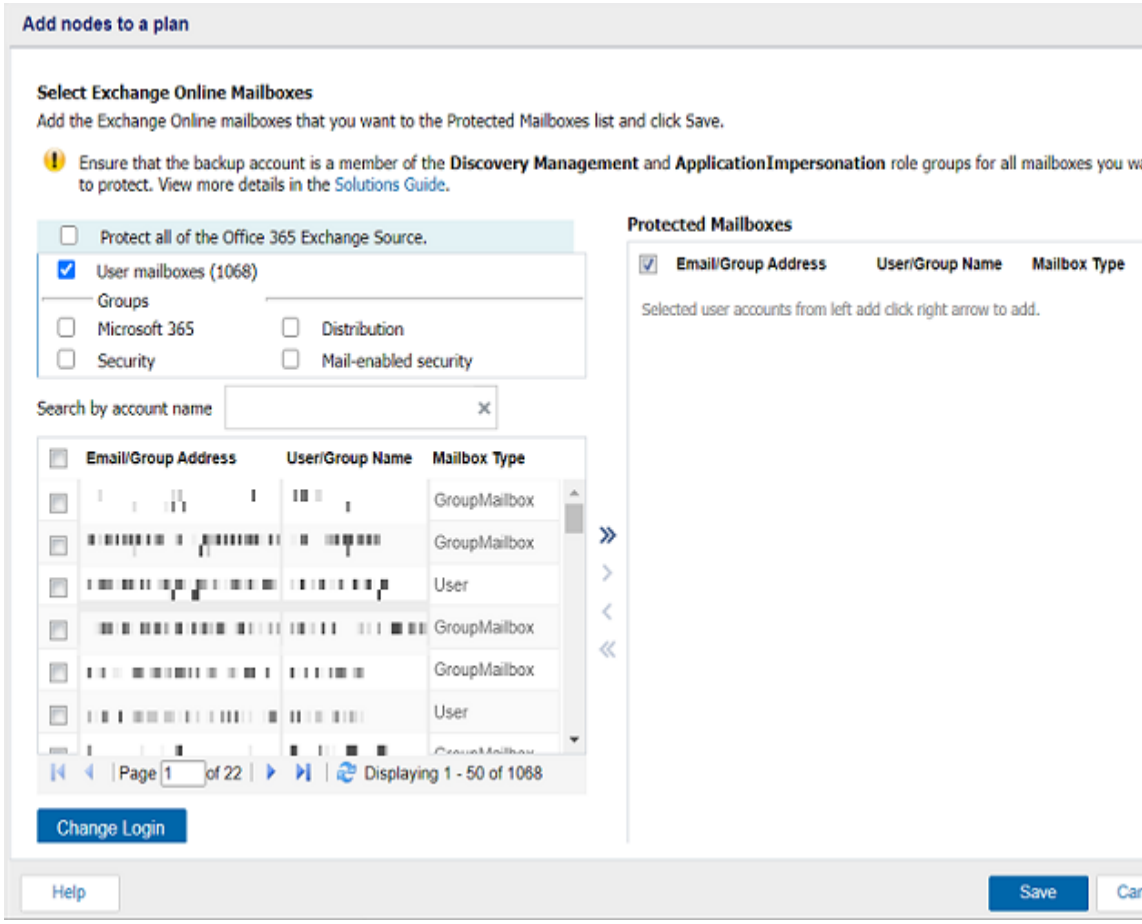
     Nota: Esta opción se selecciona automáticamente de forma pre-determinada cuando aparece la pantalla Seleccionar buzones de correo de Exchange Online.

   - Para obtener los buzones de correo del usuario, siga estos pasos:

     a. Seleccione la casilla de verificación **Buzones de correo del usuario**.

        Aparecerá una lista de los buzones de correo del usuario.

     b. (Opcional) Para buscar una cuenta en la lista, en el campo Buscar por nombre de cuenta escriba el nombre de la cuenta.



c. En la lista de buzones de correo del usuario, seleccione los buzones de correo que se desean proteger.

d. Haga clic en la flecha hacia la derecha (>) para mover los buzones de correo seleccionados a la lista de buzones de correo protegidos.

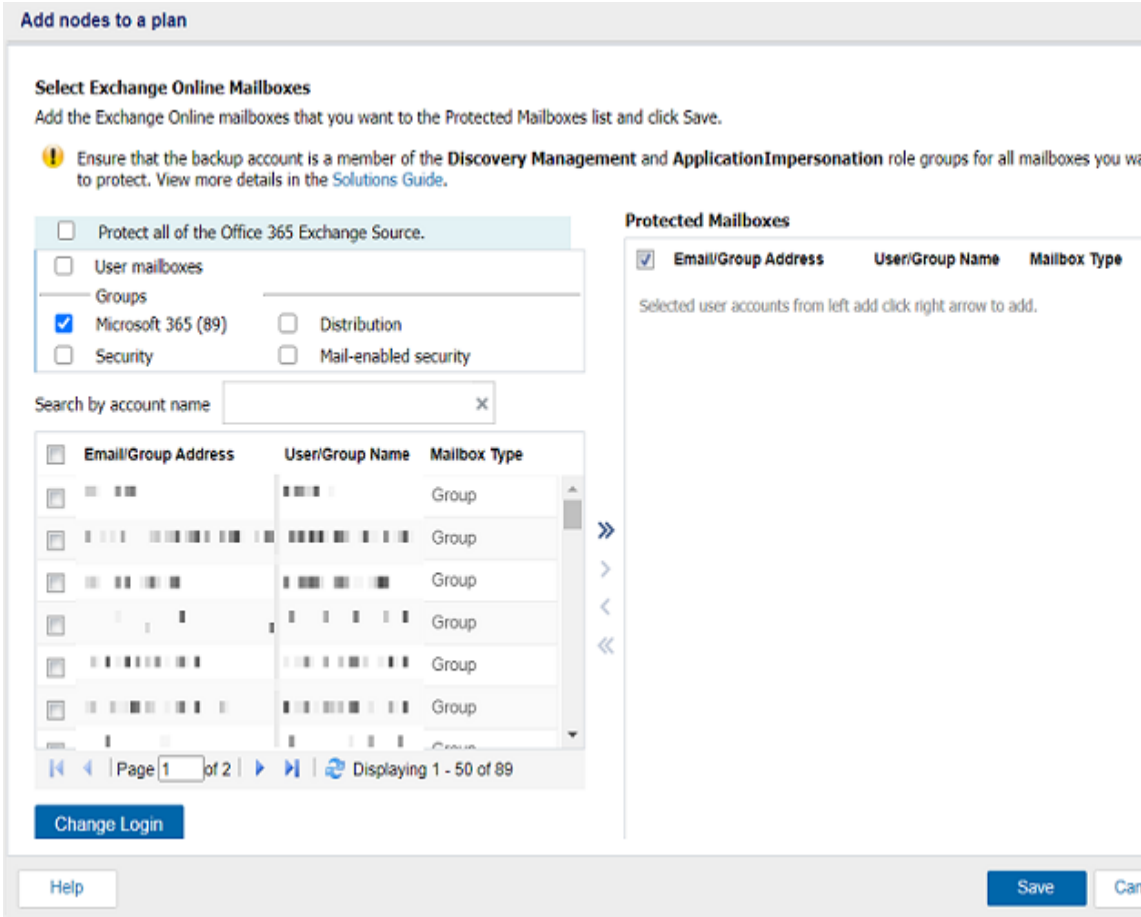
- Para obtener los grupos, siga estos pasos:

a. Seleccione la casilla de verificación **Microsoft 365**.

Aparece una lista de grupos.

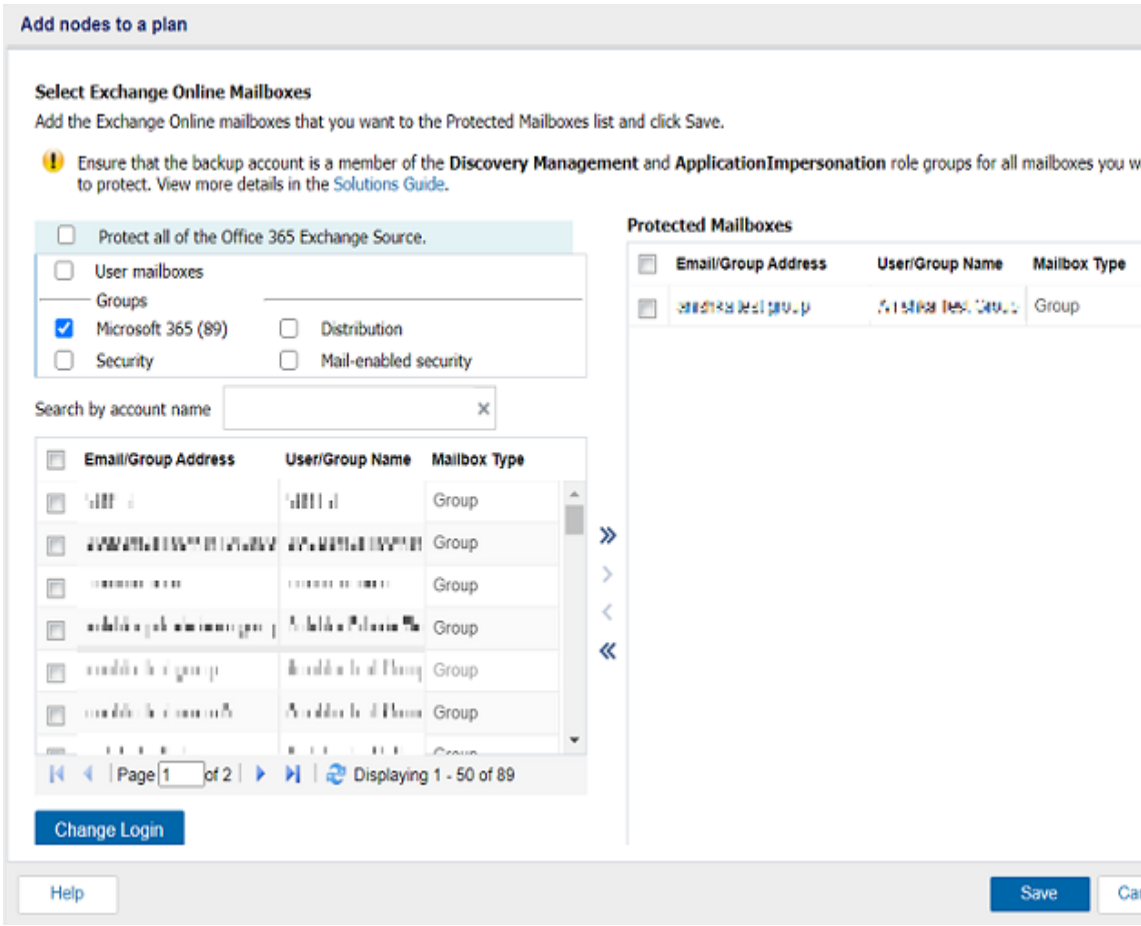
Nota: Si desea seleccionar grupos junto con subgrupos como, por ejemplo, **Distribución**, **Seguridad** o **Seguridad activada para el correo**, seleccione la casilla de verificación **Microsoft 365** y, a continuación, seleccione una casilla de verificación del subgrupo según sea necesario.

b. (Opcional) Para buscar una cuenta en la lista, en el campo Buscar por nombre de cuenta escriba el nombre de la cuenta.



c. En la lista de grupos, seleccione los grupos que desea proteger.

d. Haga clic en la flecha hacia la derecha (>) para mover los grupos seleccionados a la lista de buzones de correo protegidos.



6. Haga clic en **Guardar**.
7. En la ficha Orígenes, vaya a **Carpetas que se deben excluir de la copia de seguridad** y, a continuación, seleccione la casilla de verificación deseada.
8. En Opción avanzada, seleccione la casilla de verificación deseada.
   - Para permitir que la protección de Exchange Online sea compatible con el Buzón archivado, active la casilla de verificación **Backup up In-Place Archiving**.

     Nota: Para obtener más información sobre el archivado de buzones, consulte el vínculo.
   - Active la casilla de verificación **Backup up Recoverable items** para activar la protección del buzón que se activa la función Conservación local o Suspensión por litigio.

Nota: Para la Conservación local o la Suspensión por litigio del archivado para Exchange Online, consulte este vínculo.

Nota: Para activar las características en el buzón al mismo tiempo para hacer la copia de seguridad de los elementos recuperables en el buzón archivado, seleccione tanto la opción **Backup up In-Place Archiving** como la opción **Backup up Recoverable items**

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Haga clic en la ficha **Destino**.
2. Seleccione la opción **Servidor de puntos de recuperación de Arcserve UDP. Servidor de puntos de recuperación de Arcserve UDP** especifica que el destino de la copia de seguridad es un servidor de puntos de recuperación. Si se selecciona esta opción, los datos se almacenan como puntos de recuperación. No se pueden almacenar los datos como conjuntos de recuperación.
3. Proporcione los siguientes detalles:
   a. Seleccione un servidor de puntos de recuperación.
   b. Seleccione un almacén de datos sin deduplicación o de deduplicación. La lista muestra todos los almacenes de datos que se han creado en el servidor de puntos de recuperación especificado.
   c. Proporcione una contraseña de la sesión. La contraseña de sesión es opcional cuando el destino de copia de seguridad es un almacén de datos del servidor de puntos de recuperación no cifrado.
   d. Confirme la contraseña de la sesión.

   Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y se pueden proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

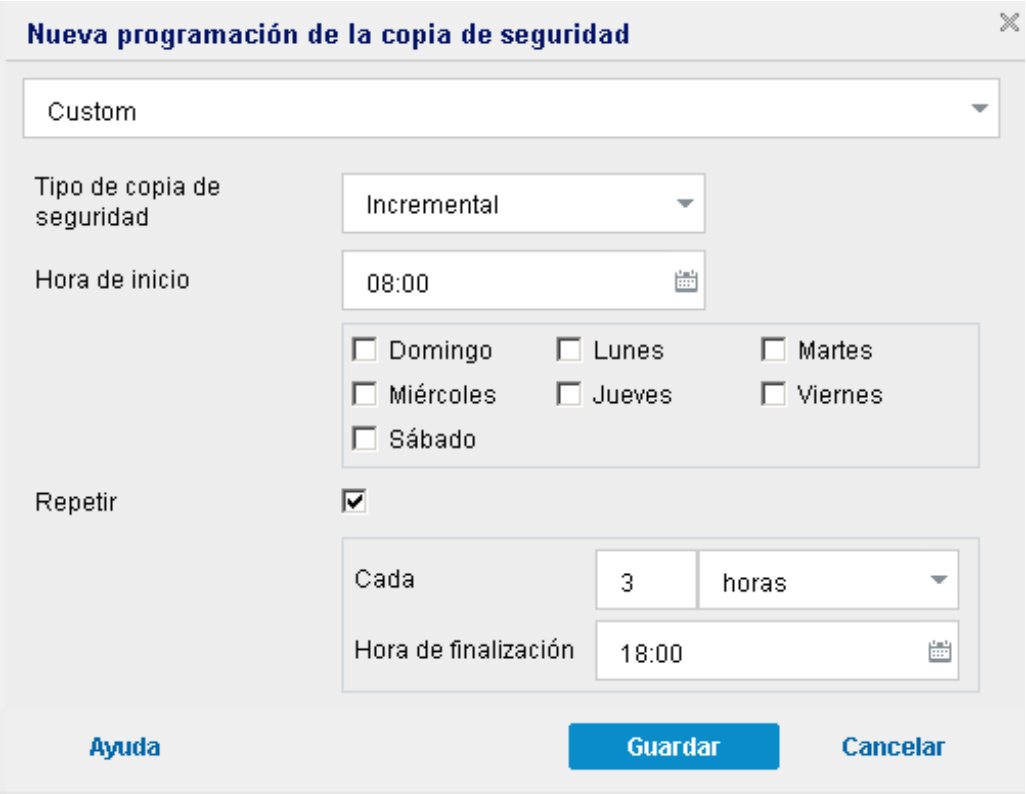
Siga estos pasos:

1. Agregue las programaciones de la copia de seguridad, de la combinación y del regulador.

   Agregar programación de la copia de seguridad

   a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

      Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

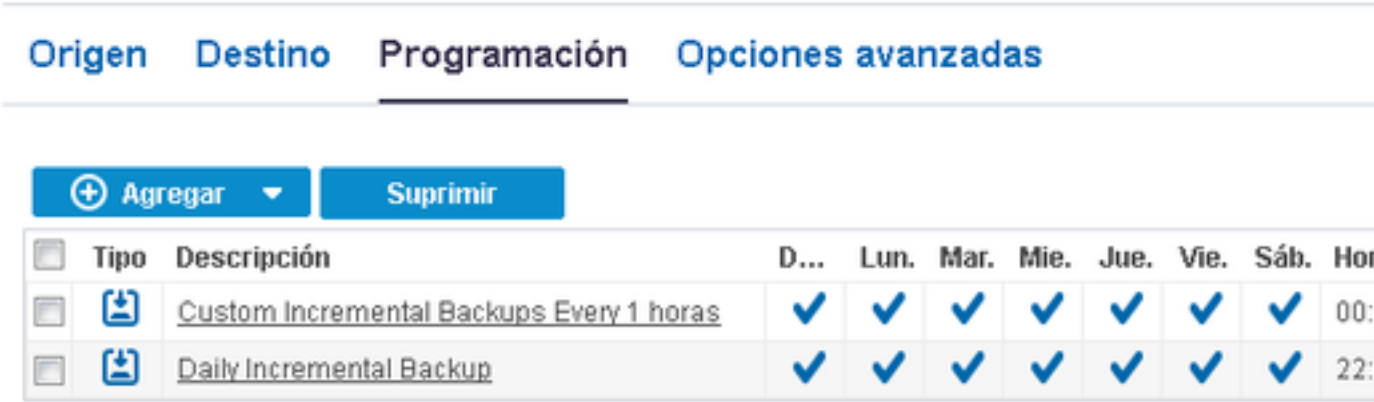
Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de las copias de seguridad incrementales consisten en que la copia de seguridad es rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en **Agregar** y seleccione **Agregar programación de la combinación**.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

b. Especifique la hora de inicio para iniciar la tarea de combinación.

c. Especifique **Hasta** para especificar una hora de finalización para la tarea de combinación.

d. Haga clic en **Guardar**.

La programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

Se abre el cuadro de diálogo **Agregar nueva programación del limitador.**

b. Especifique el límite de rendimiento en MB por minuto.

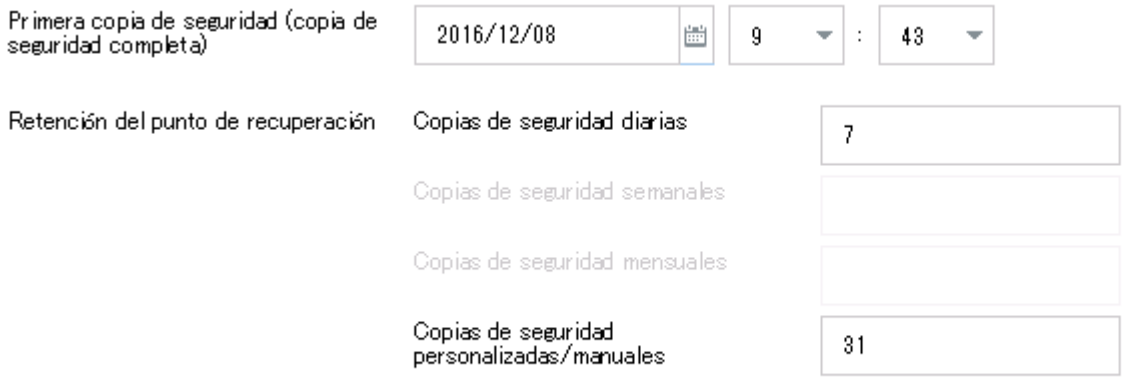
c. Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para especificar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

La programación del limitador se especifica y se muestra en la página **Programación**.

2. Especifique la hora de inicio para la copia de seguridad programada.



3. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo **Programación de la copia de seguridad**.

Se especifica la programación.

Funcionamiento de la programación avanzada y de la retención

La opción de programación le permite especificar una programación personalizada, una programación diaria/semanal/mensual o ambas. En la programación personalizada, se puede configurar la programación de la copia de seguridad durante cada día de la semana y se pueden agregar hasta cuatro programaciones de copia de seguridad cada día. Se puede seleccionar un día específico de una semana y crear un período de tiempo para definir cuando se desea ejecutar la copia de seguridad y con qué frecuencia.

Programación	Tarea compatible	Comentarios
Copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para ejecutar las tareas de copia de seguridad.
Regulación de la copia de seguridad	Tarea de copia de seguridad	Defina los períodos de tiempo para controlar la velocidad de la copia de seguridad.
Combinar	Tarea de combinación	Defina cuando se deben ejecutar las tareas de combinación.
Programación diaria	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad diarias.
Programación semanal	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad semanales.
Programación mensual	Tarea de copia de seguridad	Defina cuando se deben ejecutar las tareas de copia de seguridad mensuales.

Se pueden especificar también los valores de configuración de retención para los puntos de recuperación.

Nota: Establezca la configuración de la retención en cada plan para controlar cómo se retienen los datos para los nodos asignados a ese plan en el almacén de datos de destino.

Las programaciones para las copias de seguridad diarias/semanales/mensuales son independientes de la programación personalizada y de las unas a las otras. Se puede configurar solamente ejecutar una copia de seguridad diaria, una copia de seguridad semanal o una copia de seguridad mensual sin configurar la programación personalizada.

Programación de la tarea de copia de seguridad

Se pueden agregar cuatro períodos de tiempo por día en la programación de la copia de seguridad. Un período de tiempo válido es desde las 12:00 horas hasta las 23:59 horas. No se puede especificar un período de tiempo como, por

ejemplo, de las 18:00 horas a las 06:00 horas. En tales casos, se debe especificar manualmente dos períodos de tiempo diferentes.

Para cada período de tiempo, la hora de inicio está incluida y, en cambio, no se incluye la hora de finalización. Por ejemplo, se ha configurado ejecutar una copia de seguridad incremental ejecutada todas las horas entre las 06:00 horas y las 09:00 horas y la copia de seguridad se iniciará a las 06:00 horas. Esto significa que la copia de seguridad se ejecuta a las 06:00 horas, a las 07:00 horas y a las 08:00 horas, pero NO a las 09:00 horas.

Nota: Si desea ejecutar la tarea de copia de seguridad reiteradamente hasta el final del día, configure la programación hasta las 12:00 horas. Por ejemplo, para ejecutar la tarea de copia de seguridad cada 15 minutos durante todo el día, configure la programación de las 12:00 a las 12:00, cada 15 minutos.

Programación del regulador de la copia de seguridad

La programación del regulador de la copia de seguridad le permite controlar la velocidad del rendimiento de la copia de seguridad, que a su vez controla el uso de recursos (E/S del disco, CPU, ancho de banda de la red) del servidor del que se está realizando la copia de seguridad. Esto es útil si no se desea afectar al rendimiento del servidor durante el horario comercial. Se pueden agregar cuatro períodos de tiempo por día en la programación del regulador de la copia de seguridad. Para cada período de tiempo, se puede especificar un valor en MB por minuto. Este valor se utiliza para controlar el rendimiento de la copia de seguridad. Los valores válidos van desde 1 MB/minuto a 99999 MB/minuto.

Si una tarea de copia de seguridad excede el tiempo especificado, el límite del regulador se ajusta según el período de tiempo especificado. Por ejemplo, se ha definido el límite del regulador de la copia de seguridad en 500 MB/minuto desde las 08:00 horas a las 20:00 horas y en 2500 MB/minuto de las 20:00 horas a las 22:00 horas. Si una tarea de copia de seguridad se inicia a las 19:00 horas y se ejecuta durante tres horas, el límite del regulador es de 500 MB/minuto de las 19:00 horas a las 20:00 horas y de 2500 MB/minuto de las 20:00 horas a las 22:00 horas.

Si no se define ninguna programación de la copia de seguridad ni ninguna programación del rendimiento de la copia de seguridad, la copia de seguridad se ejecuta tan deprisa como pueda.

Programación de la combinación

Le permite combinar puntos de recuperación basándose en la programación proporcionada.

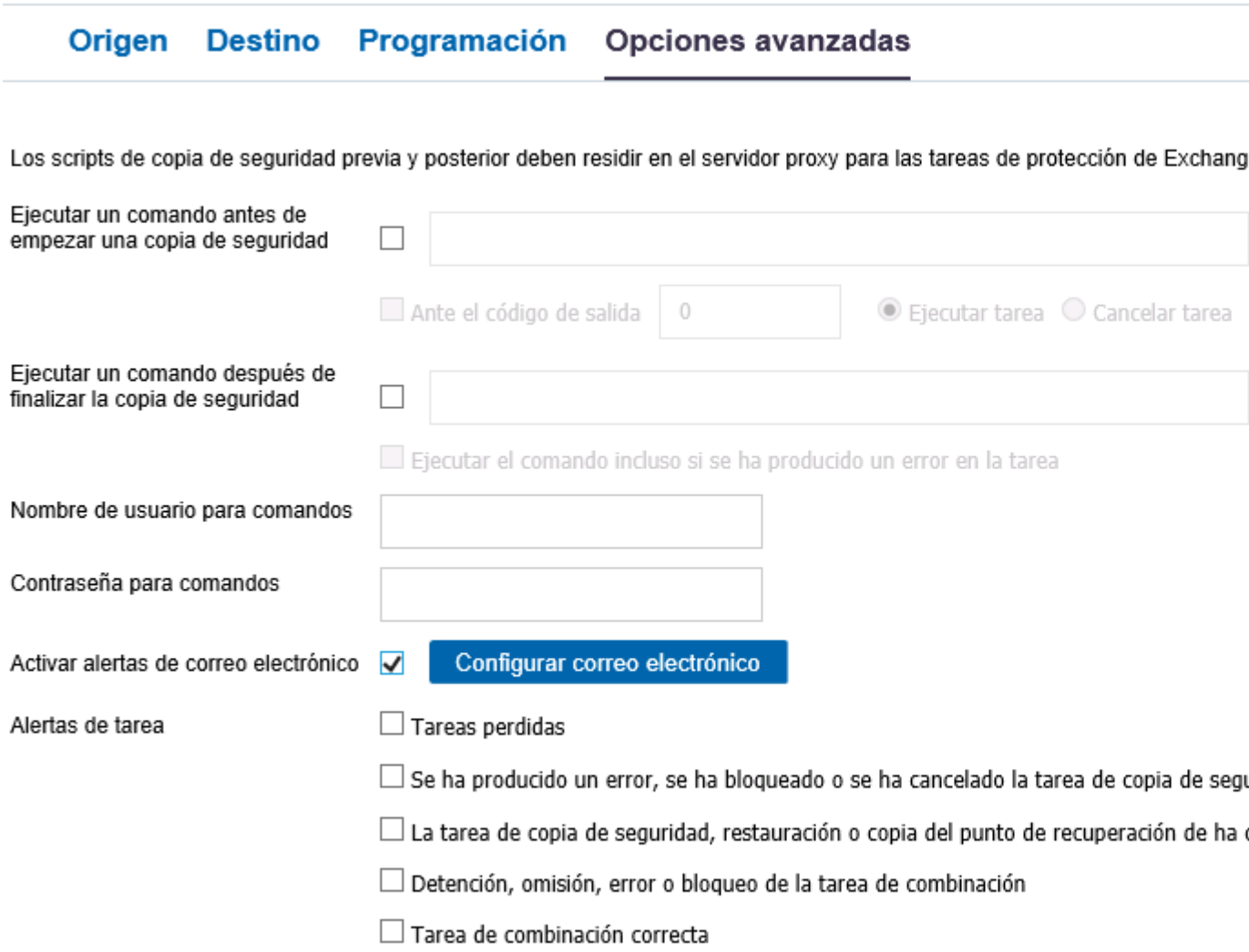
Tenga en cuenta los puntos siguientes para la tarea de combinación:

- Solamente una tarea de combinación puede ejecutarse para un nodo en cualquier momento proporcionado.
- Si se inicia una tarea de combinación, se tiene que completar antes de que la siguiente tarea de combinación se pueda iniciar. Esto no significa que, si uno o más conjuntos de puntos de recuperación se combinan, no se pueda agregar un punto de recuperación nuevo a este proceso de combinación hasta que el proceso de combinación del conjunto actual de puntos de recuperación se complete.
- Si una tarea de combinación está procesando más de un conjunto de puntos de recuperación (por ejemplo, el conjunto [1~4], el conjunto [5~11] y el conjunto [12~14] son tres conjuntos), el servidor de puntos de recuperación procesará estos conjuntos uno a uno.
- Si una tarea de combinación se reanuda después de una pausa, la tarea detecta en qué punto se ha pausado y reanuda la combinación a partir del punto de pausa.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye proporcionar la ubicación de algunos scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha **Avanzada**:



Siga estos pasos:

1. Especifique los siguientes detalles:

   Ejecutar un comando antes de empezar una copia de seguridad

   Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde está almacenado el script en el nodo del proxy. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de

seguridad continúa cuando el script devuelve el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detiene cuando el script devuelve el código de salida.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta completa donde está almacenado el script.

Ejecutar el comando incluso si se ha producido un error en la tarea

Si se selecciona esta casilla de verificación, el script especificado en **Ejecutar un comando después de finalizar una copia de seguridad** se ejecuta incluso cuando se produce un error en la tarea de copia de seguridad. De lo contrario, este script se ejecuta solamente cuando la tarea de copia de seguridad finaliza correctamente.

Nombre de usuario para comandos

Permite especificar el nombre de usuario para ejecutar los comandos.

Contraseña para comandos

Permite especificar la contraseña para ejecutar los comandos.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy. Para obtener más información sobre cómo configurar el correo electrónico, consulte la sección Configuración del correo electrónico y alertas.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de alerta de las tareas que se desean recibir.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo del servidor proxy y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera

todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en **Guardar**.

Los cambios se guardan y aparecerá una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar. Se pueden agregar las tareas **Copiar punto de recuperación**, **Copia en cinta**, **Replicar** y **Replicar desde un servidor de puntos de recuperación** como tareas de seguimiento.

El plan se implementa automáticamente en el nodo del servidor proxy.

Se crea el plan de copia de seguridad de Exchange Online para el servidor proxy. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

(Opcional) Realización de una copia de seguridad manual

Normalmente se realizan copias de seguridad automáticamente y las controlan los valores de configuración de programación. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario. Por ejemplo, si tiene una programación de repetición para las copias de seguridad completas e incrementales y desea hacer cambios importantes en el equipo, debe realizar una copia de seguridad manual inmediata sin necesidad de esperar a la siguiente copia de seguridad programada.

Para realizar una copia de seguridad manual de los nodos de Exchange Online, siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Los nodos de Exchange Online se muestran en el panel central.
3. Seleccione los nodos de Exchange Online (por ejemplo, Mailbox@<nombreorganización.com) de los que se desea realizar la copia de seguridad y que tienen un plan asignado. El nombre del nodo es la cuenta que se utiliza cuando se agrega el nodo de Exchange Online y se conecta.
4. Haga clic con el botón derecho en el nodo y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
5. Seleccione el tipo de copia de seguridad que desea realizar y, a continuación, haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.
6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.
7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   La copia de seguridad manual se realiza correctamente.

   Para realizar una copia de seguridad manual de un plan de Exchange Online, siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Los planes de copia de seguridad de Exchange Online se muestran en el panel central.
3. Seleccione el plan del que se desea realizar la copia de seguridad y que tiene un plan asignado.
4. Haga clic con el botón secundario del ratón en el plan y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
5. Seleccione el tipo de copia de seguridad que desea realizar y, a continuación, haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.
6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.
7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   La copia de seguridad manual se realiza correctamente.

Verificación de la copia de seguridad.

Para verificar la copia de seguridad, confirme que se ha creado correctamente el plan de copia de seguridad. Después de verificar que el plan se ha creado correctamente, confirme si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Se puede verificar el estado de las tareas de copia de seguridad en la ficha **Tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga uno de estos métodos para verificar las tareas de copia de seguridad:

Método 1

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Método 2

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Tareas correctas**.

   La lista de tareas de copia de seguridad completadas aparecerá en el panel central.
3. Haga clic en la tarea que desea verificar.

   Se actualiza el panel derecho.
4. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
5. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Restauración de los mensajes (chats) de Microsoft Teams utilizando Exchange Online

Se pueden restaurar mensajes (chats) de Microsoft Teams utilizando Exchange Online desde la nube de Microsoft mediante cualquier equipo. Se pueden restaurar datos desde el punto de recuperación a la ubicación original o a una ubicación alternativa.

Realice las tareas siguientes para restaurar los datos del buzón de correo de Exchange Online:

1. Selección de los elementos del buzón de correo Exchange Online que se deben restaurar
2. Definición de las opciones de restauración
3. Restauración de los elementos recuperables
4. Restauración del contenido del punto de recuperación
5. Verificación de que se ha restaurado el contenido

Selección de los elementos de correo de Exchange Online que se deben restaurar

Se pueden restaurar los datos de correo de Exchange Online desde un punto de recuperación. Cuando se selecciona una fecha de recuperación y, a continuación, se especifica el tiempo, se muestran todos los puntos de recuperación asociados para esa duración. Tiene la opción de explorar y seleccionar el contenido de la copia de seguridad (incluyendo las aplicaciones) que se debe restaurar.

Siga estos pasos:

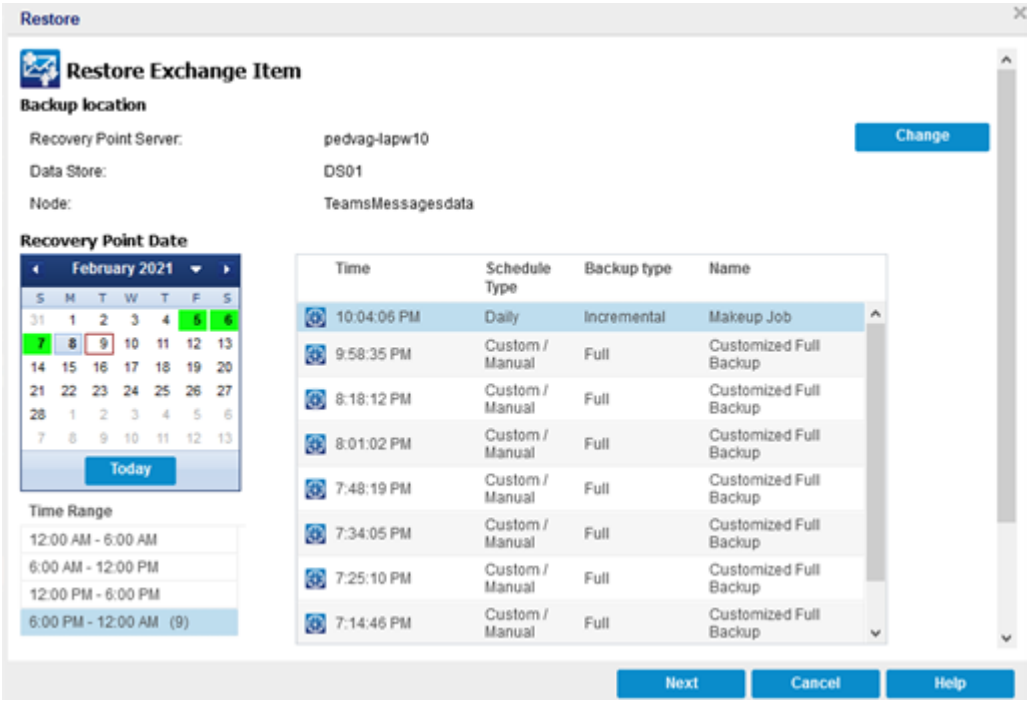
1. Inicie sesión en Arcserve UDP.
2. Haga clic en la ficha **recursos**.
3. Seleccione **Todos los nodos** en el panel izquierdo.

   Se muestran todos los nodos de agregados en el panel central.
4. En el panel central, seleccione el nodo Exchange Online y, a continuación, haga clic en **Acciones**.
5. Haga clic en **Restaurar** en la lista desplegable Acciones.

   Se abre el cuadro de diálogo Restaurar elemento de Exchange.

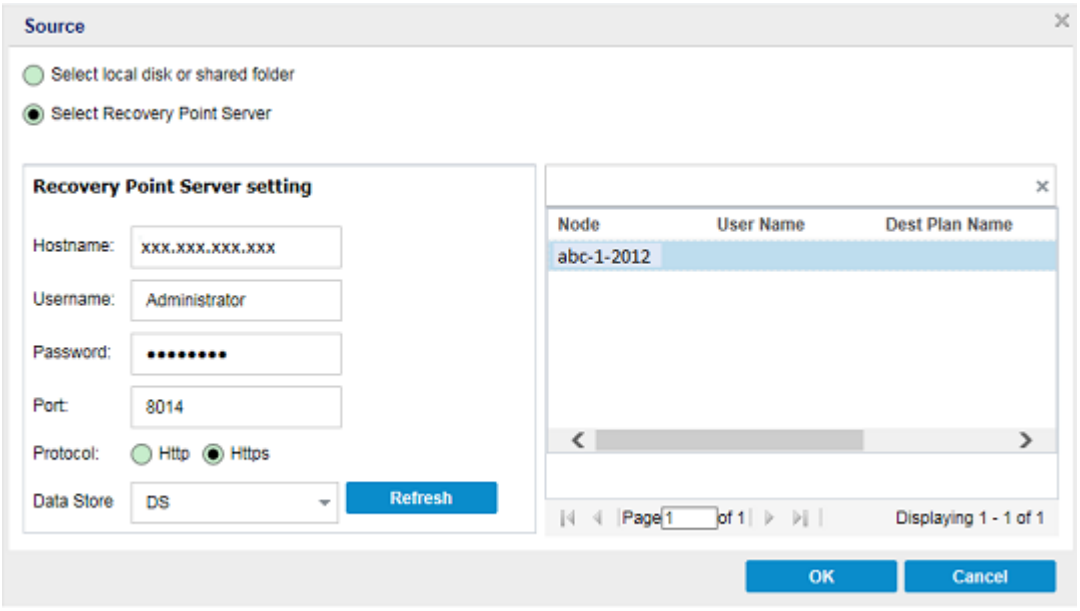
   Nota: Se inicia sesión automáticamente en el nodo del agente y se abre el cuadro de diálogo **Restaurar elemento de Exchange**.

   Se pueden ver los detalles del Servidor de puntos de recuperación en la Ubicación de la copia de seguridad.



6. (Opcional) Para modificar la ubicación de la copia de seguridad, haga clic en **Cambiar** .

   Se abrirá el cuadro de diálogo Origen. Se puede seleccionar la ubicación de la copia de seguridad en este cuadro de diálogo.



Nota: Cuando se agrega una tarea de copia en cinta al plan y ahora se desea restaurar el punto de recuperación de la copia de seguridad de la copia en cinta, seleccione el punto de recuperación en la copia de seguridad de la copia en cinta. Para

obtener más información, consulte Exploración del punto de recuperación de la copia en cinta para la restauración.

7. Para especificar el origen, seleccione una de las siguientes opciones y, a continuación, haga clic en **Aceptar**:

   Seleccionar disco local o carpeta compartida

   Nota: En Arcserve UDP, no se recomienda seleccionar la opción **Seleccionar disco local o carpeta compartida**.

   Seleccionar servidor de puntos de recuperación

   a. Especifique los detalles del valor de configuración del servidor de puntos de recuperación y, a continuación, haga clic en **Actualizar**.

      Todos los agentes se muestran en la columna Agente de protección de datos en el cuadro de diálogo Origen.

   b. Seleccione el agente en la lista mostrada y, a continuación, haga clic en **Aceptar**.

      Los puntos de recuperación se enumeran en el cuadro de diálogo Restaurar elemento de Exchange.

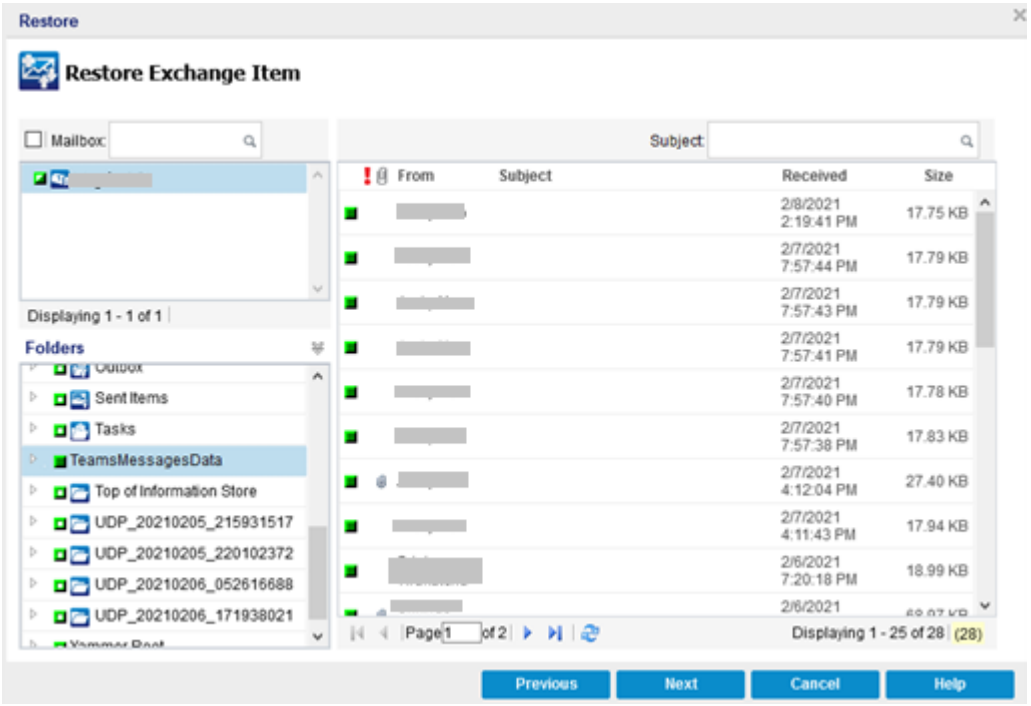
      Nota: Desde el punto de recuperación **Carpeta**, se pueden ver muchas carpetas con el mismo nombre junto con los nodos de Exchange Online. Esto sucede debido a que el GUID del nodo cambia y se crea una nueva carpeta del punto de recuperación cuando se suprime un nodo y se vuelve a agregar al plan de prueba.

8. Seleccione la fecha de calendario para restaurar la imagen de la copia de seguridad y, a continuación, haga clic en **Siguiente**.

   Todas las fechas que contienen puntos de recuperación para el origen de la copia de seguridad especificado se resaltan en verde.

   Aparecerán los puntos de recuperación correspondientes para la fecha, junto con la hora de la copia de seguridad, el tipo de copia de seguridad que se realiza (completa, incremental o de verificación) y el nombre de la copia de seguridad.

9. En el panel **Buzón de correo**, haga clic en el buzón de correo que se desea restaurar.



Se muestran todos los elementos de correo relacionados con el buzón de correo en el panel Carpetas.

10. Seleccione la carpeta **TeamsMessagesData** y, a continuación, haga clic en **Siguiente**.

    Notas:

    - Se puede seleccionar todo el contenido o el contenido parcial del objeto de Exchange para restaurar. Para seleccionar parte del contenido, expanda el objeto y haga clic en la casilla de verificación de dicho contenido.
    - Se pueden seleccionar objetos de Exchange múltiples para restaurar.

    Se abrirá el cuadro de diálogo Opciones de restauración.

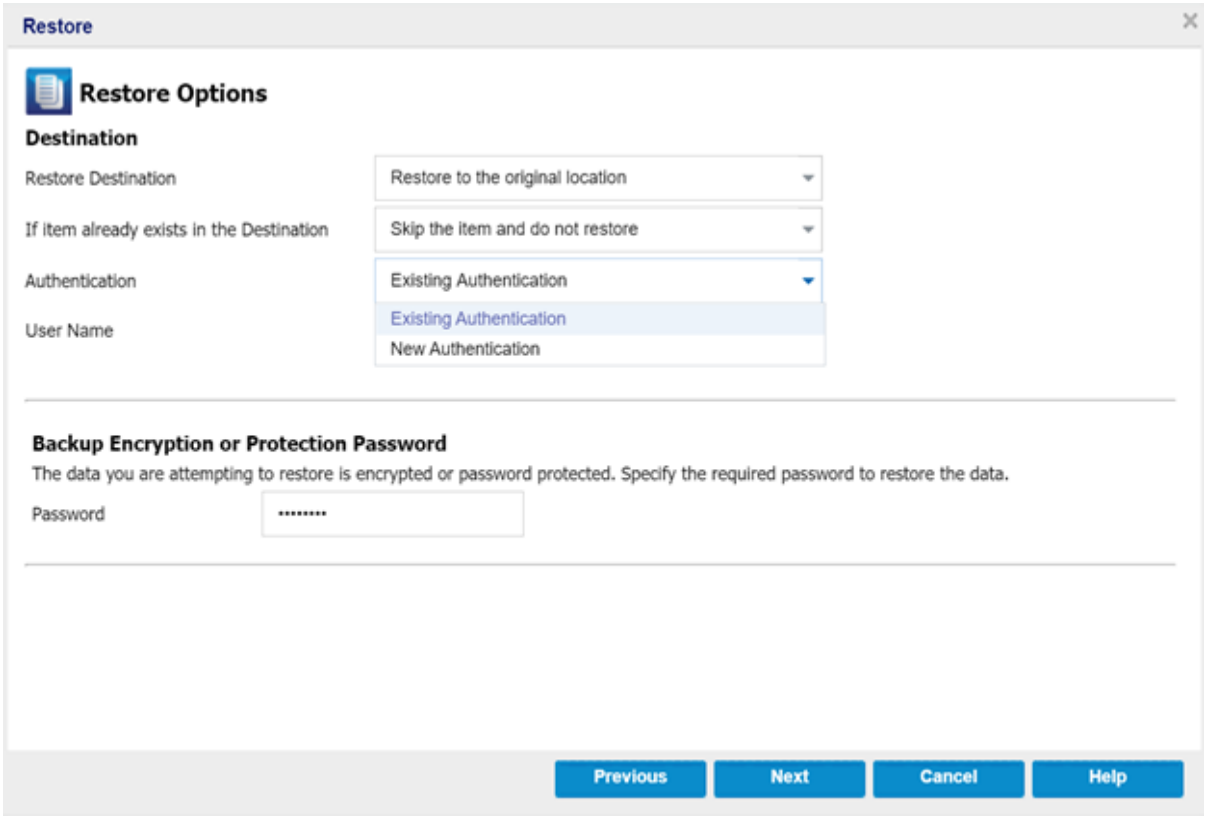
    Se han seleccionado los elementos de correo de Exchange Online que se deben restaurar. Ahora, se pueden definir las opciones de restauración.

Definición de las opciones de restauración

Después de especificar la información de Exchange Online que se debe restaurar, defina las opciones de restauración para el contenido seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo Opciones de restauración, seleccione el destino para la restauración.



A continuación se especifican las opciones de destino disponibles:

Restauración en la ubicación original

Restaura los datos del correo en la misma ubicación desde donde se ha realizado una copia de seguridad.

Notas:

- Si se restaura en la ubicación original, los datos no se reflejarán en los mensajes de Teams. Esta no es una restauración completa a la ubicación original ya que no se puede realizar la restauración de la carpeta raíz.

- Si se restaura dos veces un mismo elemento de correo en la ubicación original mediante la opción Sobrescribir, tras la segunda restauración, el primer elemento de correo restaurado no se sobrescribe. De este modo, aparecen dos elementos de correo similares en la ubicación original.
- Si se restaura un elemento de correo en la ubicación original mediante la opción Omitir y en la carpeta original ya existe un elemento similar al elemento restaurado, la tarea de copia de seguridad muestra un resultado incompleto.

Restaurar en una ubicación alternativa

Restaura los datos del correo a otro buzón de correo o a otra carpeta del buzón de correo original. Cuando se selecciona esta opción, se puede examinar y seleccionar el destino.

2. Especifique una de las siguientes opciones del menú desplegable **Si el elemento ya existe en el destino**:

Omitir el elemento y no restaurar

Se omiten los elementos y no se restaurará.

Valor predeterminado: La opción Omitir el elemento y no restaurar.

Sobrescribir el elemento en el destino

Sobrescribe el elemento en el destino.

Nota: La lista desplegable Si el elemento ya existe en el destino está disponible si se selecciona la opción **Restaurar en la ubicación original** en la lista desplegable Destino de la restauración.

Autentificación

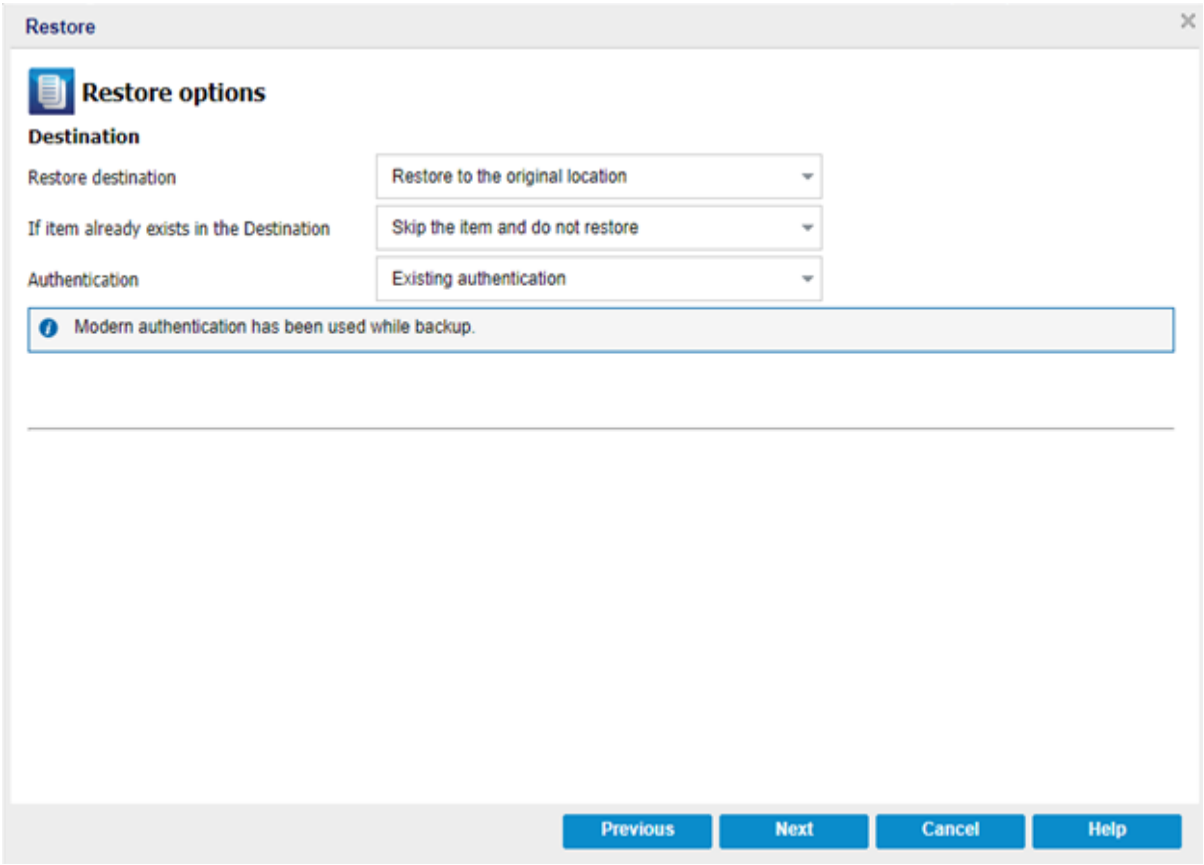
Valida e identifica la cuenta de usuario. Seleccione una de las opciones siguientes:

- **Autenticación existente**

  Cuando se selecciona Autenticación existente, se utiliza el tipo de autenticación que se ha seleccionado durante la creación del nodo.

  - Si la autenticación del nodo es básica, se cargan automáticamente parámetros como Nombre de usuario, Contraseña y Cifrado de la copia de seguridad o Contraseña de protección [Si está cifrada] para continuar con la restauración.

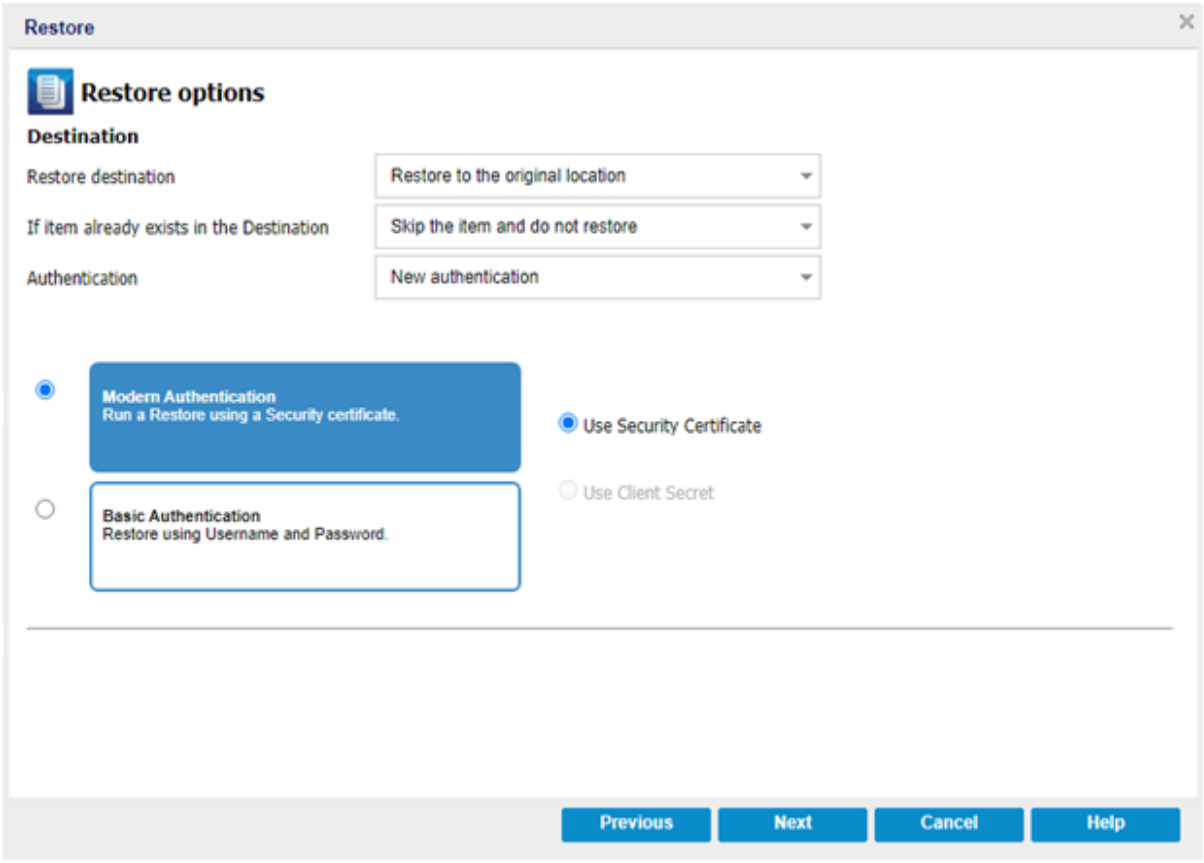
- Si la autenticación del nodo es moderna, se cargan automáticamente parámetros como Nombre de usuario y Cifrado de la copia de seguridad o Contraseña de protección [Si está cifrada] para continuar con la restauración.



- **Nueva autenticación**

  Durante la restauración, se puede seleccionar una de las siguientes opciones para cambiar el tipo de autenticación:

  - Autenticación moderna
  - Autenticación básica



3. Para aplicar la autenticación, realice una de las siguientes acciones:

   Autenticación moderna

   Para la autenticación moderna, se puede ejecutar una restauración utilizando un certificado de seguridad.

   Utilizar certificado de seguridad

   Nota: De forma predeterminada, el plan de copia de seguridad selecciona **Utilizar certificado de seguridad** para la autenticación moderna.

   Siga estos pasos:

   a. Para autenticarse mediante un certificado autofirmado, consulte Descarga del certificado desde UDP y carga del certificado en Azure.

   b. Introduzca el ID de la aplicación y el Nombre de usuario.

   c. Para aplicar los roles y permisos necesarios, seleccione la casilla de verificación **Permitir a Arcserve UDP establecer los roles y permisos de Azure necesarios para esta aplicación** y, a continuación, haga clic en **Siguiente**.

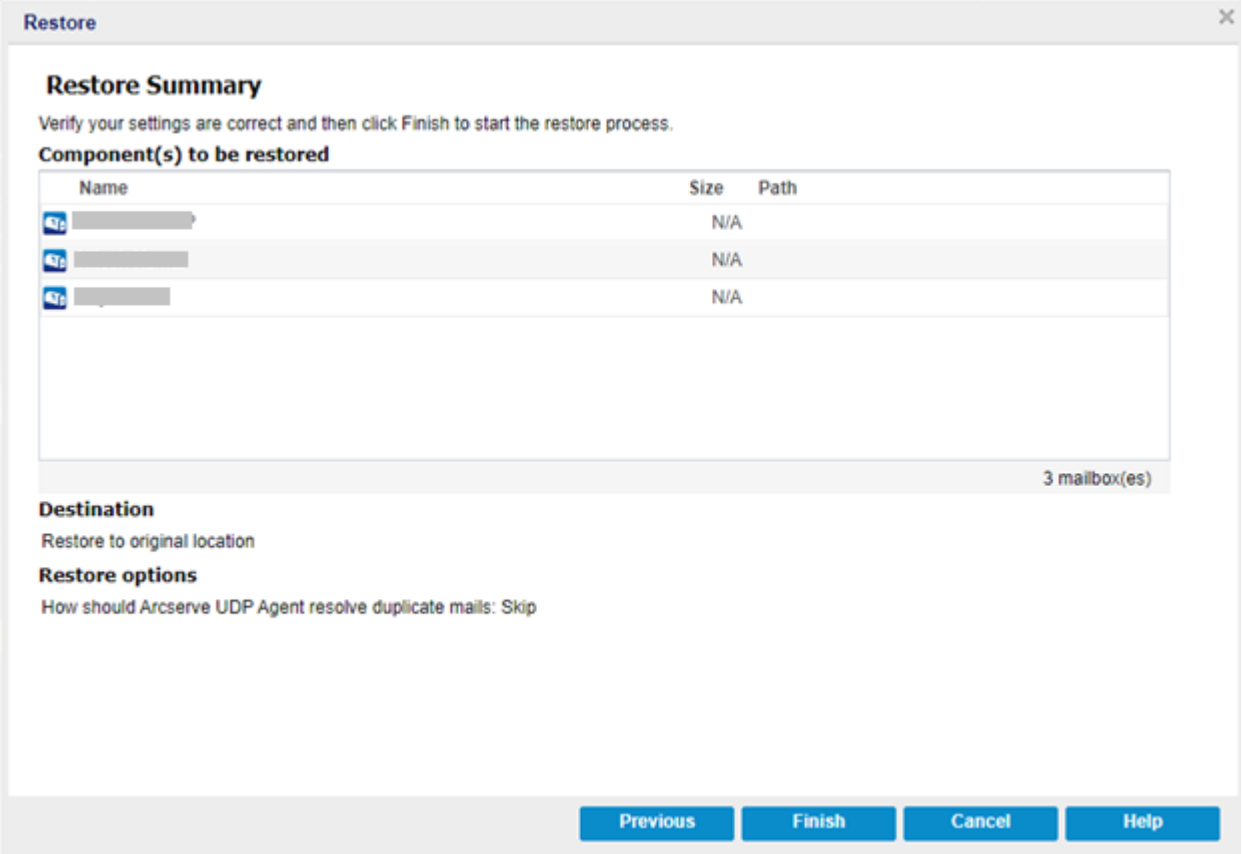
Autenticación básica

Para la Autenticación básica, introduzca el Nombre de usuario y la Contraseña para continuar con la restauración.

Nota: Esta opción produce un error si tiene activada la autenticación moderna en el inquilino o en la cuenta.

4. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo Resumen de la restauración.



5. En la ventana Resumen de la restauración, verifique la configuración y, a continuación, haga clic en **Finalizar**.

Las opciones de restauración se han definido para restaurar la información de Exchange Online.

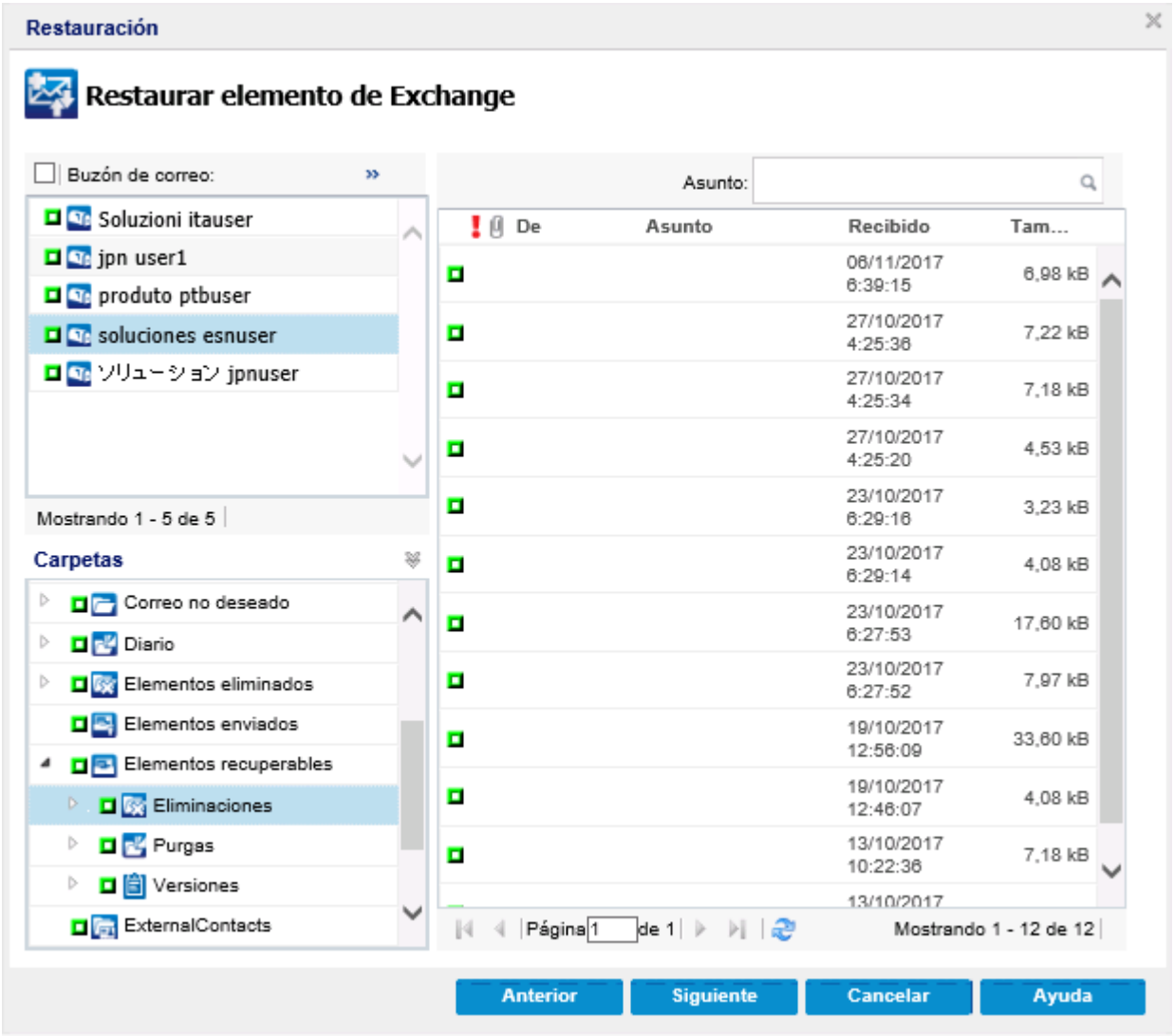
Restauración de los elementos recuperables

Se pueden restaurar los elementos recuperables del buzón que permite la característica In-Place Hold or Litigation Hold desde la interfaz de usuario del nodo de Exchange Online para examinar la sesión de copia de seguridad. Para activar esta característica, consulte Especificación del origen.

Después de activar la característica, se podrán restaurar los elementos recuperables utilizando el asistente de la restauración.

Siga estos pasos:

1. En el cuadro de diálogo Restaurar elemento de Exchange, seleccione las carpetas necesarias bajo **Elementos recuperables** y, a continuación, haga clic en **Siguiente**.



Aparecerá el cuadro de diálogo Opción de restauración.

2. En la pantalla Opción de restauración, realice los siguientes detalles y, a continuación, haga clic en **Siguiente**:
   - Seleccione el destino de la restauración.
   - Omita o sobrescriba si el elemento ya existe en el destino.

     Se puede realizar la restauración original o alternativa.

     Restauración original

     Los elementos que se encuentran bajo Elementos recuperables se restauran en la carpeta *UDP_RecoverableItems_aaaaMMdd_HHmmssfff* creada en el buzón de correo de destino. Las opciones Omitir y Sobrescribir para la restauración no se aplican a estos elementos.

     Restauración alternativa

     De la misma manera que con el buzón del usuario, restaura los elementos seleccionados en la ruta de destino en una carpeta con la marca de tiempo única como, por ejemplo, *titulado/restore_aaaaMMdd-mmssff*.
   - Proporcione el ID de usuario y la contraseña del destino donde se desea restaurar.

   Se restauran los elementos recuperables seleccionados.

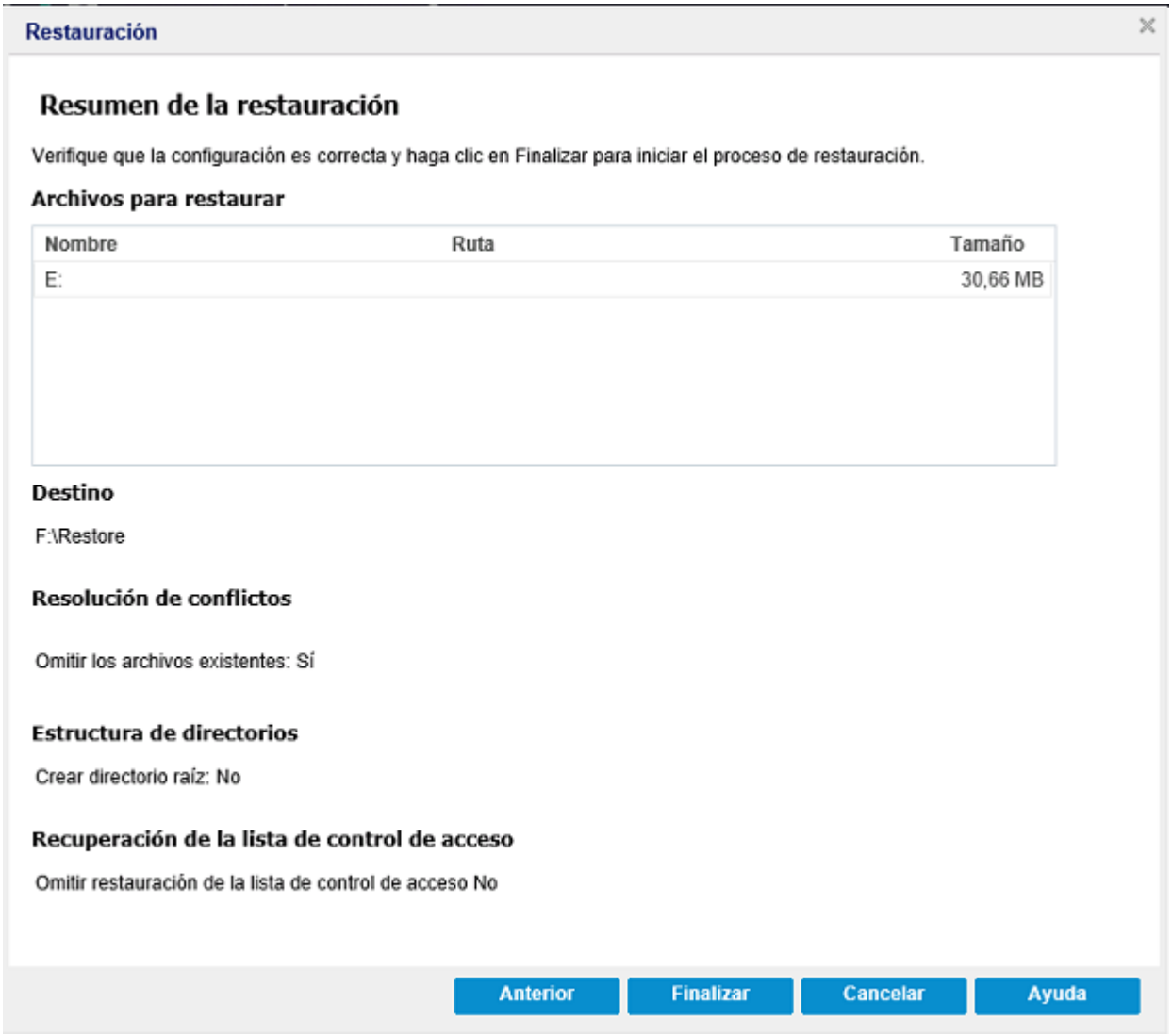
   El contenido del punto de recuperación se restaura.

Restauración del contenido del punto de recuperación

Después de definir las opciones de restauración, verifique que los valores de configuración sean correctos y confirme el proceso de restauración. El **Resumen de la restauración** le ayuda a revisar todas las opciones de la restauración definidas y a modificarlas si es necesario.

Siga estos pasos:

1. En el cuadro de diálogo Resumen de la restauración, revise la información que aparece en pantalla para verificar que todas las opciones de restauración y los valores de configuración sean correctos.



- Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para cambiar el valor de configuración incorrecto.

- Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar la tarea de restauración.

El contenido del punto de recuperación se restaura.

Verificación de que se ha restaurado el contenido

Después de la terminación del proceso de restauración, verifique que el contenido se ha restaurado en el destino especificado.

Siga estos pasos:

1. Inicie sesión en el buzón de correo de destino.
2. Compruebe que existe el elemento del buzón de correo que se ha restaurado.
3. Verifique el contenido restaurado.

   El contenido restaurado se ha verificado correctamente.

Cómo realizar copias de seguridad y restauraciones de archivos de Microsoft Teams utilizando SharePoint Online

Siempre que se crea un canal de grupo, público o privado en Microsoft Teams, se crea automáticamente un sitio de SharePoint Online. Este sitio de SharePoint Online tiene una carpeta de biblioteca de documentos predeterminada, en la que se guardan automáticamente todos los archivos compartidos en todas las conversaciones. También se pueden personalizar los permisos y las opciones de seguridad para proteger la información confidencial.

Cuando se crea cualquier grupo en Microsoft Teams, se crea automáticamente un sitio de SharePoint Online con el nombre **Team - Nombre_grupo**. Todos los archivos compartidos en los canales públicos se guardan en este sitio.

Cuando se crea un canal privado en el grupo de Microsoft Teams, se crea otro sitio de SharePoint Online con el nombre **Nombre_grupo_Teams - Nombre_canal_privado** para ese canal privado, aparte del sitio creado para el grupo de equipo.

Esta sección proporciona información sobre cómo restaurar y realizar copias de seguridad de archivos de Microsoft Teams utilizando SharePoint Online.

Esta sección incluye los siguientes temas:

Copia de seguridad de los archivos de Microsoft Teams utilizando SharePoint Online

Esta sección proporciona información sobre cómo realizar una copia de seguridad de los archivos de Microsoft Teams utilizando SharePoint Online.

Esta sección incluye los siguientes temas:

Cómo crear un plan de copia de seguridad de SharePoint Online

La protección de SharePoint se utiliza para la copia de seguridad y la restauración de los elementos de lista y el sitio de Microsoft SharePoint Online. SharePoint Online es uno de los productos principales de Microsoft Office 365. Para proteger el contenido de SharePoint, es necesario crear un plan.

Esta sección incluye los siguientes temas:

Revisión de los requisitos previos

Revise los siguientes requisitos previos antes de crear un plan de copia de seguridad de SharePoint Online.

Creación de un plan de copia de seguridad de SharePoint Online:

Requisitos previos:

La cuenta de la copia de seguridad es miembro de los grupos de Administradores de la colección de sitios o se ha asignado con el rol *Administrador de SharePoint*.

Para agregar una cuenta al grupo Administradores de la colección de sitios, consulte el vínculo.

Creación de un plan de copia de seguridad de SharePoint Online utilizando la autenticación básica:

Revise los siguientes requisitos previos:

- Instale PowerShell versión 5.1 o posterior (forma parte de Windows Management Framework (WMF)) en el servidor proxy (equipo de 64 bits).
- Instale los siguientes módulos de PowerShell en el servidor proxy mediante la ventana PowerShell:
  - Para instalar el módulo Azure, ejecute el siguiente comando:

    Install-Module -Name AzureAD -Force
  - Para instalar el módulo ExchangeOnlineManagement, ejecute el siguiente comando:

    Install-Module -Name ExchangeOnlineManagement -Force

  Nota: Cuando se instalan módulos de PowerShell utilizando los comandos anteriores, es posible que se instale una versión más nueva de los módulos en función de la versión de disponibilidad general del componente disponible en el repositorio de Microsoft.

Creación de un plan de copia de seguridad de SharePoint Online utilizando la autenticación moderna:

Revise los requisitos previos antes de crear un plan utilizando la autenticación moderna.

Creación de un plan de copia de seguridad de SharePoint Online

Un plan de copia de seguridad incluye la tarea **copia de seguridad: Office 365 SharePoint Online** que realiza una copia de seguridad de los elementos de SharePoint Online (listas, bibliotecas, documentos, etc.) y almacena los datos en un almacén de datos de deduplicación o sin deduplicación. Además, este plan de copia de seguridad permite a UDP detectar y especificar los grupos de SharePoint Online para los que se realiza una tarea de copia de seguridad. Cada tarea está formada por parámetros que definen el origen, destino, programación y otros detalles de la copia de seguridad.

Siga estos pasos:

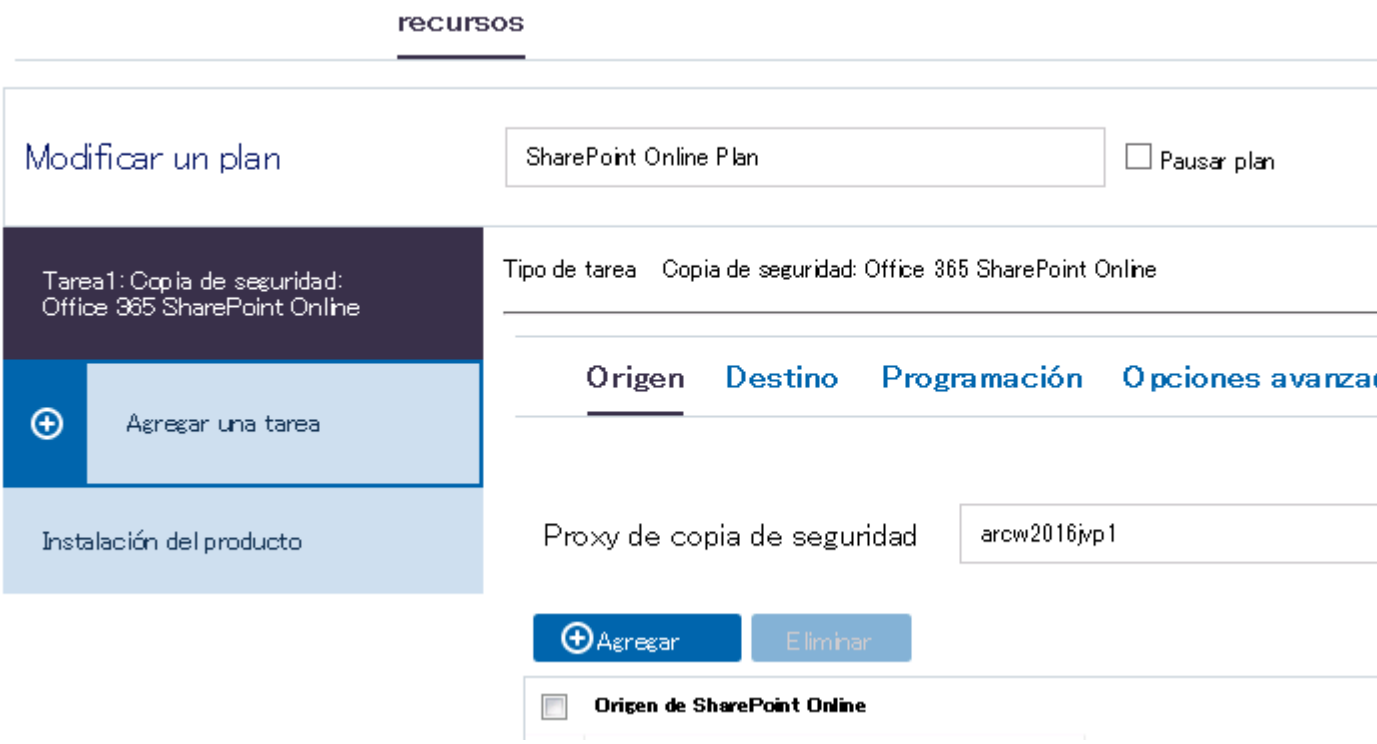
1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y, a continuación, haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre el cuadro de diálogo Agregar un plan.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecuta hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable Tipo de tarea seleccione **Copia de Seguridad: Office 365 SharePoint Online**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Especificación del origen

La página Origen le permite especificar los nodos de origen de SharePoint Online que se desean proteger. Se puede seleccionar más de un nodo de origen de SharePoint Online en el plan.

Nota: Se puede guardar un plan sin agregar nodos de origen pero el plan no se muestra a menos que se agregue un nodo.

Siga estos pasos:

1. Haga clic en la ficha **Origen**.
2. Seleccione **Servidor proxy de copia de seguridad** en la lista desplegable.
3. Agregue el nodo de SharePoint Online utilizando uno de los siguientes métodos:

   Método 1:

   a. Haga clic en **Agregar** y, a continuación, haga clic en **Seleccionar nodos para proteger en Arcserve UDP**.

      Se muestra el cuadro de diálogo Agregar nodos al plan.

      Nota: Utilice esta opción solamente cuando ya se haya agregado el nodo de SharePoint.

   b. Seleccione un nodo y haga clic en **Conectar**.

      Nota: Para buscar los nodos de SharePoint Online que se desean proteger, utilice **Búsqueda**.

   Método 2:

   - Haga clic en **Agregar** y, a continuación, haga clic en **Agregar origen de SharePoint Online**.

     Aparece el cuadro de diálogo Agregar nodos a un plan.

     Nota:

     - Utilice esta opción para detectar y especificar elementos en línea para el origen de SharePoint Online.
     - A diferencia de otros nodos, no se puede agregar el nodo de SharePoint Online desde la página Todos los nodos. Solo se puede agregar un nodo de SharePoint Online a un plan al crear o modificar un plan.
4. Para aplicar la autenticación, realice una de las siguientes acciones:

Autenticación moderna

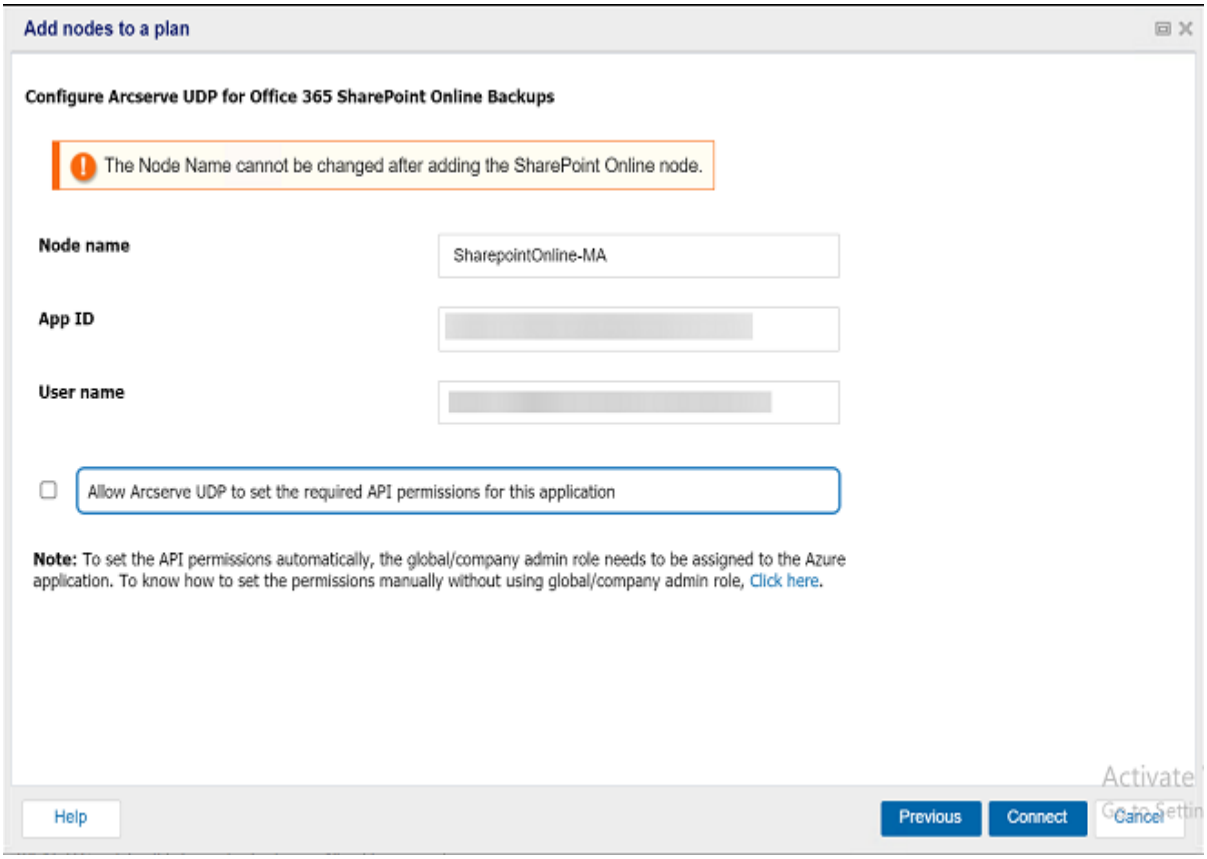
Para la autenticación moderna, se puede ejecutar una copia de seguridad con un certificado de seguridad.

Utilizar certificado de seguridad

Nota: De forma predeterminada, el plan de copia de seguridad selecciona **Utilizar certificado de seguridad** para la autenticación moderna.

Siga estos pasos:

1. Para autenticar la aplicación de UDP con certificados de seguridad, consulte Descarga del certificado de UDP y carga del certificado en Azure.
2. Introduzca los siguientes detalles:
   - Nombre de nodo
   - ID de aplicación
   - Nombre de usuario



c. Para aplicar los permisos de API automáticamente, seleccione la casilla de verificación **Permitir que Arcserve UDP establezca los permisos de la API necesarios para esta aplicación**.

Nota: Para aplicar los permisos manualmente sin utilizar el rol de administrador global o de la compañía, consulte Configuración de los permisos de la API manualmente sin utilizar el rol de administrador global o de la compañía.

d. Haga clic en **Conectar**.

Notas:

- Los nombres del nodo de origen de SharePoint Online no se pueden cambiar después de crear el nodo.
- Se puede utilizar una única cuenta para proteger varios nodos de SharePoint Online.
- Rellene la contraseña de la aplicación si la autenticación multifactor está activada y el inquilino está configurado para utilizar la autenticación básica.

Autenticación básica

Para la autenticación básica, para continuar con la copia de seguridad, proporcione la siguiente información y, a continuación, haga clic en **Conectar**:

- Nombre de nodo
- Dirección URL de la recopilación de sitios
- ID de usuario
- Contraseña

5. Para proteger los elementos de SharePoint Online, haga lo siguiente:
   - En la lista desplegable Tipo de sitio, seleccione el tipo de sitio que desea proteger como, por ejemplo, Sitios de SharePoint o Sitios personales.
   - Para Proteger todos los sitios y subsitios, realice lo siguiente:

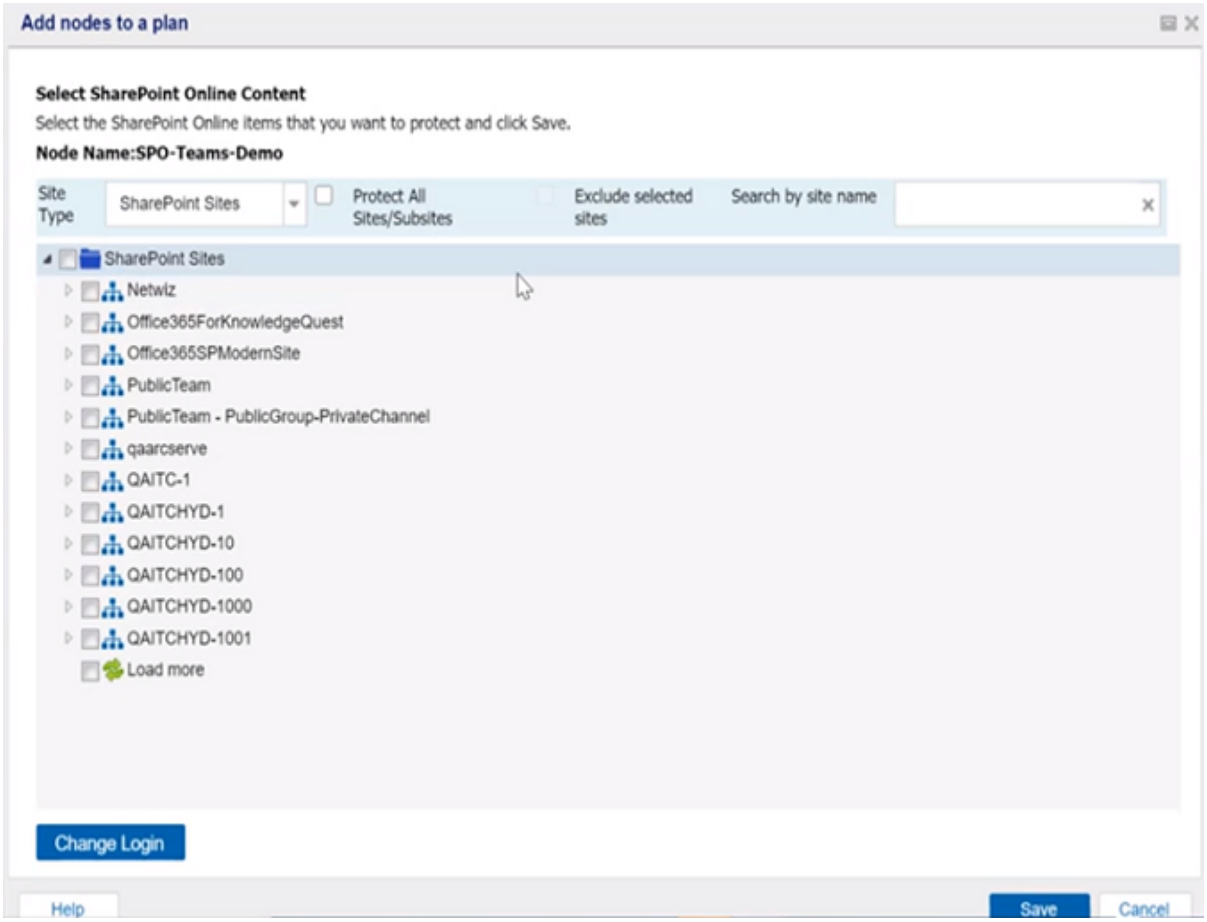
     Notas:

     - Esta opción se selecciona automáticamente de forma predeterminada cuando aparece la pantalla Seleccionar contenido de SharePoint Online.

- Para proteger todos los elementos del tipo de sitio seleccionado, seleccione la casilla de verificación **Proteger todos los sitios y subsitios**.
- Para proteger elementos específicos en el tipo de sitio seleccionado, desactive la casilla de verificación **Proteger todos los sitios y subsitios** y, a continuación, seleccione los elementos específicos que desea proteger.

- Al configurar el plan de SharePoint Online existente, si se han seleccionado sitios manualmente para la protección y ahora se desea seleccionar la casilla de verificación **Proteger todos los sitios y subsitios**, siga estos pasos:
  a. Modifique el plan de SharePoint Online existente.
  b. Borre los sitios de SharePoint que se seleccionan manualmente para la protección.
  c. Seleccione la casilla de verificación **Proteger todos los sitios y subsitios** y, a continuación, guarde el plan.

- Para excluir elementos específicos de la protección, seleccione la casilla de verificación **Excluir sitios seleccionados** y, a continuación, seleccione elementos específicos en el tipo de sitio seleccionado.



6. Haga clic en **Guardar**.

   Los orígenes de SharePoint Online que desea proteger se agregan al plan.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Haga clic en la ficha **Destino**.

   La opción Servidor de puntos de recuperación de Arcserve UDP especifica que el destino de la copia de seguridad es un servidor de puntos de recuperación.

   No se pueden almacenar los datos como conjuntos de recuperación.

2. Realice los pasos siguientes:

   a. Seleccione un servidor de puntos de recuperación.

   b. Seleccione un almacén de datos sin deduplicación o de deduplicación.

      La lista muestra todos los almacenes de datos que se han creado en el servidor de puntos de recuperación especificado.

   c. Proporcione una contraseña de la sesión.

      La contraseña de sesión es opcional cuando el destino de copia de seguridad es un almacén de datos del servidor de puntos de recuperación no cifrado.

   d. Confirme la contraseña de la sesión.

   Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y proporcionar valores de configuración de retención.

Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Nota: Para obtener más información sobre los valores de configuración de programación y retención, consulte Funcionamiento de la programación avanzada y de la retención.

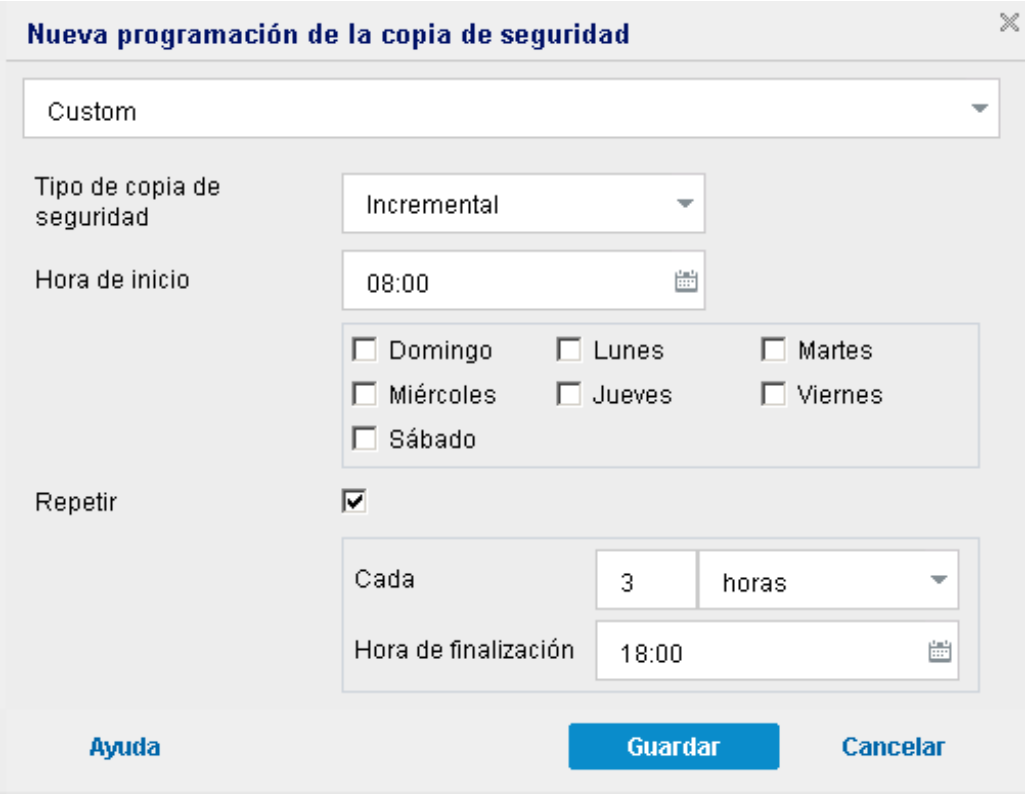
Siga estos pasos:

1. Agregue las programaciones de la copia de seguridad, de la combinación y del regulador.

   Agregar programación de la copia de seguridad

   a. Haga clic en **Agregar** y seleccione **Agregar programación de la copia de seguridad**.

      Se abrirá el cuadro de diálogo **Nueva programación de la copia de seguridad**.



b. Seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

c. Seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas. Tal y como está previsto, Arcserve UDP realizará una copia de seguridad completa de todos los bloques utilizados desde el equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

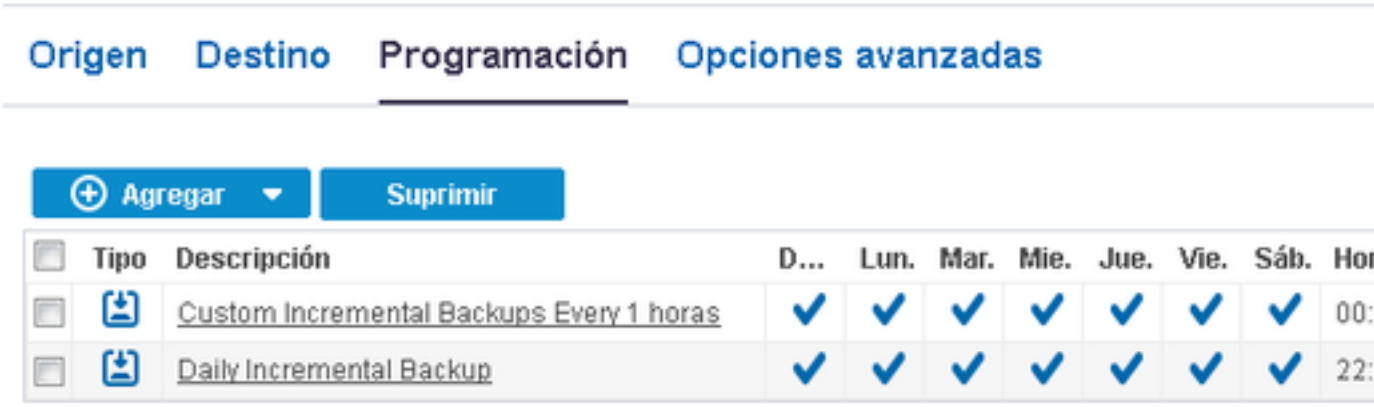
Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad incremental solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de las copias de seguridad incrementales consisten en que la copia de seguridad es rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

d. Especifique la hora de inicio de la copia de seguridad.

e. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página **Programación**.



Adición de la programación de la combinación

a. Haga clic en **Agregar** y seleccione **Agregar programación de la combinación**.

Se abrirá el cuadro de diálogo **Agregar nueva programación de la combinación**.

b. Especifique la hora de inicio de la tarea de combinación.

c. Especifique **Hasta** para proporcionar una hora de finalización para la tarea de combinación.

d. Haga clic en **Guardar**.

La programación de la combinación se especifica y se muestra en la página **Programación**.

Agregar programación del regulador

a. Haga clic en **Agregar** y seleccione **Agregar nueva programación del regulador**.

Se abre el cuadro de diálogo **Agregar nueva programación del limitador.**

b. Especifique el límite de rendimiento en MB por minuto.

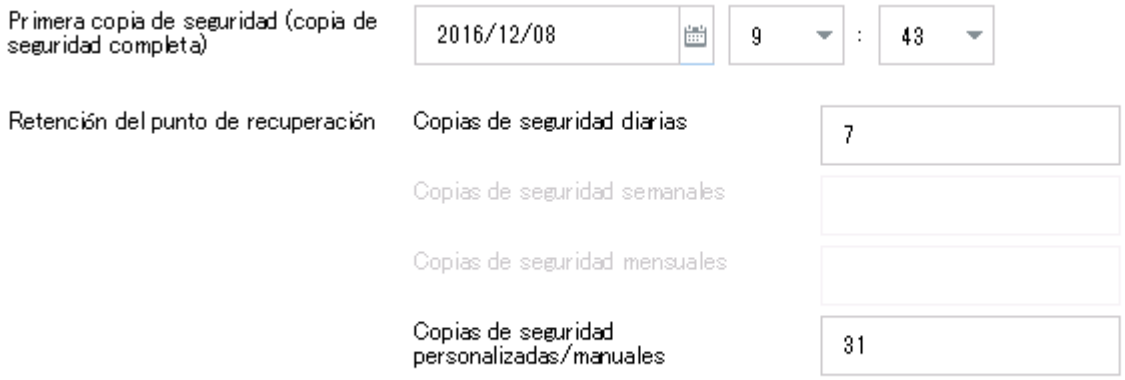
c. Especifique la hora de inicio de la tarea de rendimiento de la copia de seguridad.

d. Especifique **Hasta** para proporcionar una hora de finalización para la tarea de rendimiento.

e. Haga clic en **Guardar**.

La programación del limitador se especifica y se muestra en la página **Programación**.

2. Especifique la hora de inicio para la copia de seguridad programada.



3. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

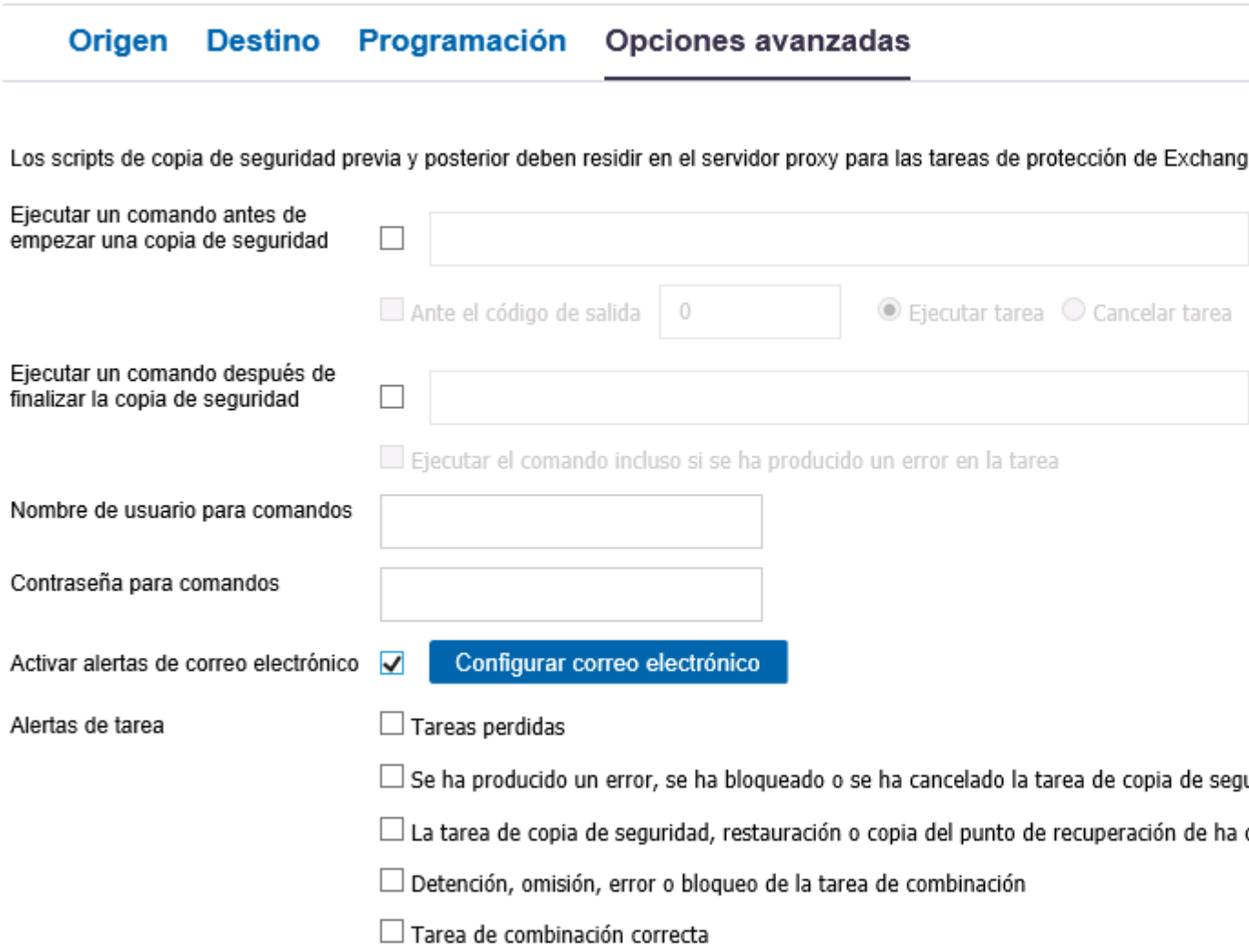
Las opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo **Programación de la copia de seguridad**.

Se especifica la programación.

Especificación de la configuración avanzada

La ficha **Avanzada** le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad. La configuración avanzada incluye proporcionar la ubicación de algunos scripts y la configuración del correo electrónico.

La imagen siguiente se muestra en la ficha **Avanzada**:



Siga estos pasos:

1. Especifique los siguientes detalles:

   Ejecutar un comando antes de empezar una copia de seguridad

   Le permite ejecutar un script antes de que la tarea de copia de seguridad se inicie. Especifique la ruta donde está almacenado el script en el nodo del proxy. Haga clic en **Ante el código de salida** y especifique el código de salida para **Ejecutar tarea** o **Cancelar tarea**. **Ejecutar tarea** indica que la tarea de copia de

seguridad continúa cuando el script devuelve el código de salida. **Cancelar tarea** indica que la tarea de copia de seguridad se detiene cuando el script devuelve el código de salida.

Ejecutar un comando después de finalizar una copia de seguridad

Le permite ejecutar un script después de completar la tarea de copia de seguridad. Especifique la ruta completa donde está almacenado el script.

Ejecutar el comando incluso si se ha producido un error en la tarea

Si se selecciona esta casilla de verificación, el script especificado en **Ejecutar un comando después de finalizar una copia de seguridad** se ejecuta incluso cuando se produce un error en la tarea de copia de seguridad. De lo contrario, este script se ejecuta solamente cuando la tarea de copia de seguridad finaliza correctamente.

Nombre de usuario para comandos

Permite especificar el nombre de usuario para ejecutar los comandos.

Contraseña para comandos

Permite especificar la contraseña para ejecutar los comandos.

Activar Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico. Haga clic en **Configuraciones del correo electrónico** y configure el servidor de correo electrónico y los detalles del servidor proxy. Para obtener más información sobre cómo configurar el correo electrónico, consulte la sección Configuración del correo electrónico y alertas.

Alertas de tarea

Le permite seleccionar los tipos de correos electrónicos de alerta de las tareas que se desean recibir.

2. Haga clic en **Guardar**.

Nota: Cuando se selecciona un nodo como origen de la copia de seguridad o como proxy de la copia de seguridad, Arcserve UDP comprueba si el Agente está instalado en el nodo del servidor proxy y si la versión del Agente es la más reciente. Arcserve UDP muestra, a continuación, un cuadro de diálogo de verificación que enumera

todos los nodos que, o bien tienen una versión anticuada del agente, o bien no lo tienen instalado. Para instalar/actualizar el agente en estos nodos, seleccione el método de instalación y haga clic en **Guardar**.

Los cambios se guardan y aparecerá una marca de verificación verde al lado del nombre de la tarea. Se cierra la página del plan.

Nota: Si se tiene que agregar otra tarea, se debe seleccionar el plan en la ficha **recursos** y modificar el plan. Para modificar el plan, haga clic en el plan en el panel central. El plan se abre y se puede modificar. Se pueden agregar las tareas **Copiar punto de recuperación**, **Copia en cinta**, **Replicar** y **Replicar desde un servidor de puntos de recuperación** como tareas de seguimiento.

El plan se implementa automáticamente en el nodo del servidor proxy.

Se crea el plan de copia de seguridad de SharePoint Online para el servidor proxy. La copia de seguridad se ejecuta según la programación configurada en la ficha **Programación.** Se puede realizar también una copia de seguridad manual en cualquier momento.

(Opcional) Realización de una copia de seguridad manual

Normalmente, en función de la configuración de la programación aplicada, las copias de seguridad se realizan automáticamente. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario. Por ejemplo, si tiene una programación de repetición para las copias de seguridad completas e incrementales y desea hacer cambios importantes en el equipo, puede realizar una copia de seguridad manual inmediata sin necesidad de esperar a la siguiente copia de seguridad programada.

Para realizar una copia de seguridad manual de los nodos de SharePoint Online, siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Los nodos de SharePoint Online se muestran en el panel central.
3. Seleccione los nodos de SharePoint Online (por ejemplo, Mailbox@<nombreorganización.com) de los que se desea realizar la copia de seguridad y que tienen un plan asignado. El nombre del nodo es la cuenta que se utiliza cuando se agrega el nodo de SharePoint Online y se conecta.
4. Haga clic con el botón derecho en el nodo y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
5. Seleccione el tipo de copia de seguridad que desea realizar y, a continuación, haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.
6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.
7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   La copia de seguridad manual se realiza correctamente.

   Para realizar una copia de seguridad manual del plan de SharePoint Online, siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Planes** y, a continuación, haga clic en **Todos los planes**.

   Los planes de copia de seguridad de SharePoint Online se muestran en el panel central.
3. Seleccione el plan del que desea realizar la copia de seguridad y asegúrese de que tiene un plan asignado.
4. Haga clic con el botón secundario del ratón en el plan y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
5. Seleccione el tipo de copia de seguridad que desea realizar y, a continuación, haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.
6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.
7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   La copia de seguridad manual se realiza correctamente.

Verificación de la copia de seguridad.

Para verificar la tarea de copia de seguridad, confirme que se ha creado correctamente el plan de copia de seguridad. Después de verificar que el plan se ha creado correctamente, confirme si la tarea de copia de seguridad se está ejecutando tal y como estaba programado. Se puede verificar el estado de las tareas de copia de seguridad en la ficha **Tareas**.

Siga estos pasos para verificar los planes:

1. Haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Nodos** y, a continuación, haga clic en **Todos los nodos**.

   Una lista de todos los nodos se muestra en el panel central.
3. Verifique que los planes están asignados a nodos.

Siga uno de estos métodos para verificar las tareas de copia de seguridad:

Método 1

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Todas las tareas finalizadas**.

   El estado de cada tarea se muestra en el panel central.
3. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Método 2

1. Haga clic en la ficha **tareas**.
2. En el panel izquierdo, haga clic en **Tareas correctas**.

   La lista de tareas de copia de seguridad completadas aparecerá en el panel central.
3. Haga clic en la tarea que desea verificar.

   Se actualiza el panel derecho.
4. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
5. Verifique que la tarea de copia de seguridad ha sido correcta.

   Se verifica la tarea de copia de seguridad.

Restauración de los datos de recopilación de sitios de SharePoint Online

Se puede restaurar la lista o la biblioteca de SharePoint Online, así como los elementos de lista en el sitio. La recopilación de sitios y el sitio todavía no se admiten en Arcserve UDP 8.0. Se pueden restaurar los datos en el sitio original con un nuevo nombre, restaurar los datos en la ubicación original y exportar al disco desde los puntos de recuperación.

Realice las tareas siguientes para restaurar el elemento de lista de SharePoint Online:

1. Selección de los elementos de lista del sitio de SharePoint Online que se van a restaurar
2. Definición de las opciones de restauración
3. Verificación de que se ha restaurado el contenido

Selección de los elementos de lista del sitio de SharePoint Online que se van a restaurar

Se pueden restaurar los datos de los elementos de lista de SharePoint Online desde un punto de recuperación. Cuando se selecciona una fecha de recuperación y, a continuación, se especifica el tiempo, se muestran todos los puntos de recuperación asociados para esa duración. Tiene la opción de explorar y seleccionar el contenido de la copia de seguridad (incluyendo las aplicaciones) que se debe restaurar.

Siga estos pasos:

1. Iniciar sesión en Arcserve UDP.
2. Haga clic en la ficha **recursos**.
3. Seleccione **Todos los nodos** en el panel izquierdo.

   Se muestran todos los nodos de agregados en el panel central.

   O

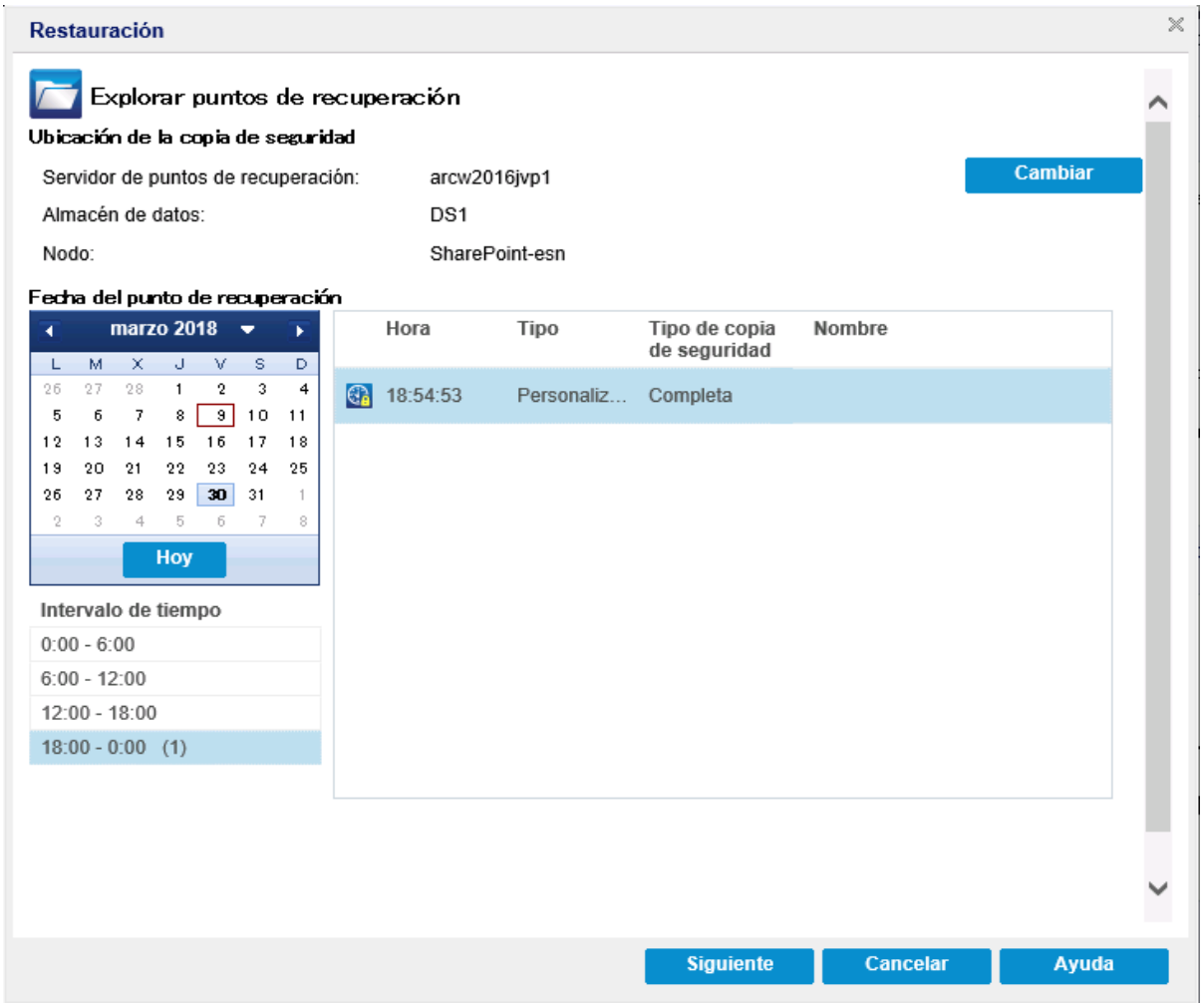
   Seleccione el grupo **Nodos de SharePoint Online**.

   Se muestran todos los nodos de SharePoint agregados en el panel central.
4. En el panel central, seleccione el nodo SharePoint Online y, a continuación, haga clic en **Acciones**.
5. Haga clic en **Restaurar** del menú desplegable Acción.

   Se abre el cuadro de diálogo Restaurar elemento de SharePoint.

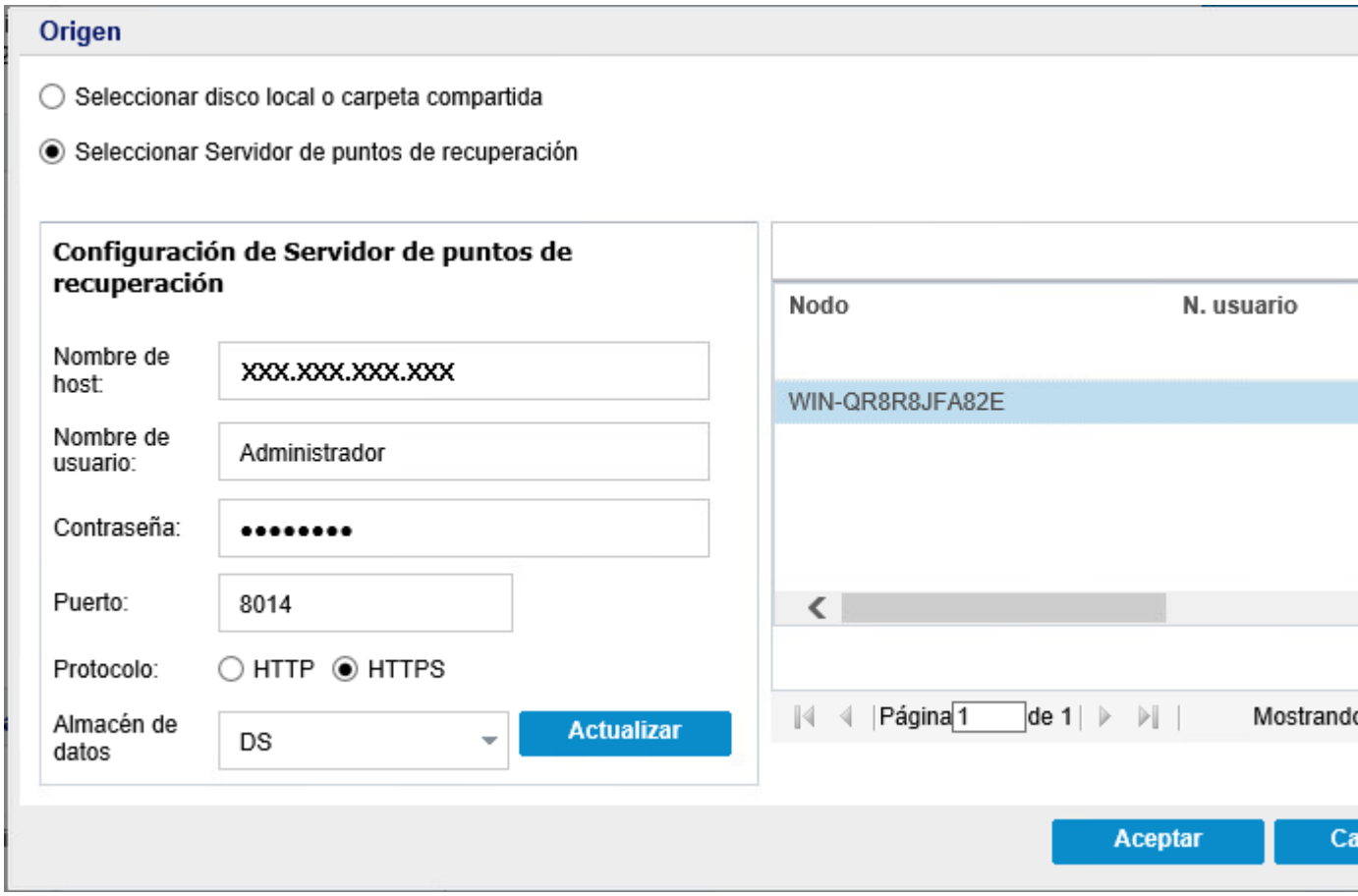
   Nota: Se inicia sesión automáticamente en el nodo del agente y se abre el cuadro de diálogo Restaurar elemento de SharePoint.

   La opción Ubicación de la copia de seguridad muestra los detalles del Servidor de puntos de recuperación.



6. (Opcional) Haga clic en **Cambiar** para modificar la ubicación de la copia de seguridad.

   Se abrirá el cuadro de diálogo Origen. Se puede seleccionar la ubicación de la copia de seguridad en este cuadro de diálogo.



Nota: Cuando se agrega una tarea de copia en cinta al plan y ahora se desea restaurar el punto de recuperación de la copia de seguridad de la copia en cinta, seleccione el punto de recuperación en la copia de seguridad de la copia en cinta. Para obtener más información, consulte Exploración del punto de recuperación de la copia en cinta para la restauración.

7. Para especificar el origen, seleccione una de las siguientes opciones y, a continuación, haga clic en **Aceptar**:

   Seleccionar disco local o carpeta compartida

   Nota: En Arcserve UDP, no se recomienda seleccionar la opción **Seleccionar disco local o carpeta compartida**.

   Seleccionar servidor de puntos de recuperación

   a. Especifique los detalles del valor de configuración del servidor de puntos de recuperación y, a continuación, haga clic en **Actualizar**.

      Todos los agentes se muestran en la columna Agente de protección de datos en el cuadro de diálogo Origen.

b. Seleccione el agente en la lista o biblioteca mostrada y, a continuación, haga clic en **Aceptar**.

   Los puntos de recuperación se enumeran en el cuadro de diálogo Restaurar elemento de SharePoint.

8. Seleccione la fecha de calendario para restaurar la imagen de la copia de seguridad y, a continuación, haga clic en **Siguiente**.

   Todas las fechas que contienen puntos de recuperación para el origen de la copia de seguridad especificado se resaltan en verde.

   Aparecerán los puntos de recuperación correspondientes para la fecha, junto con la hora de la copia de seguridad, el tipo de copia de seguridad que se realiza (completa o incremental) y el nombre de la copia de seguridad.

9. En el cuadro de diálogo Restaurar los elementos de SharePoint Online, expanda la recopilación de sitios.

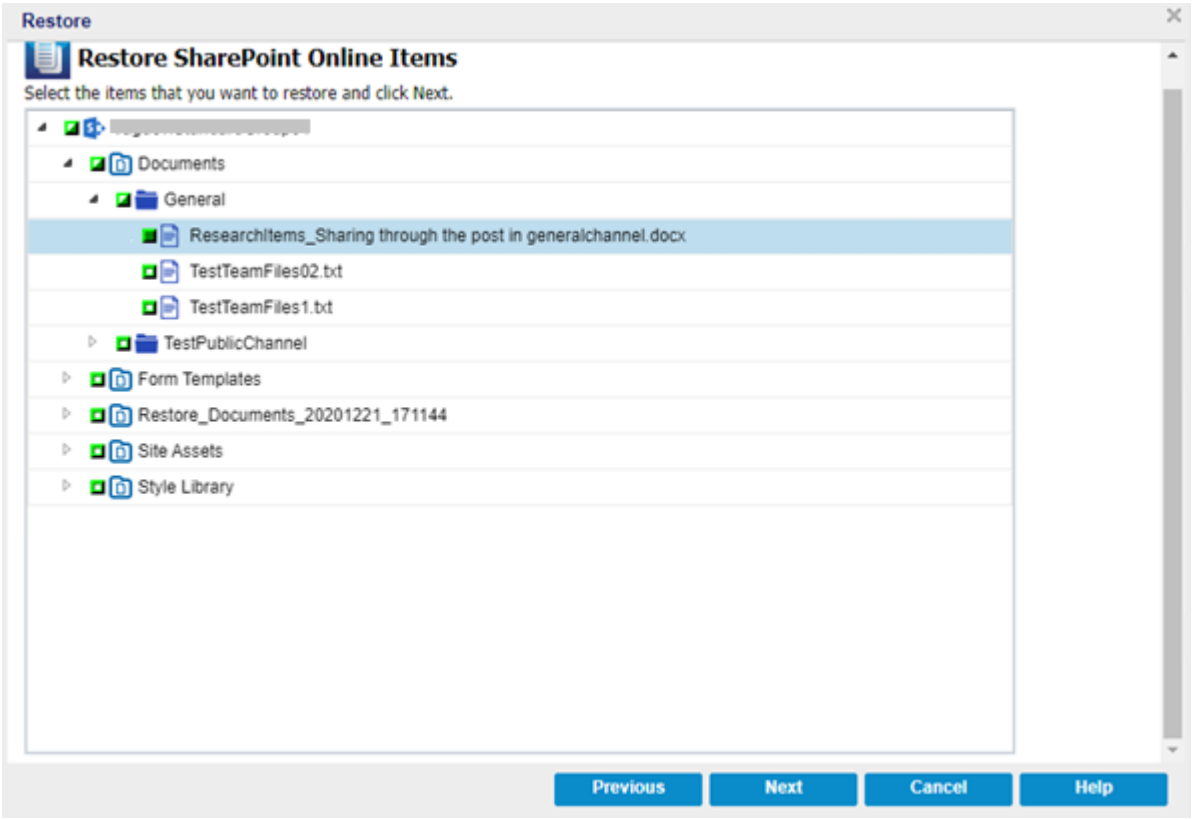
   Se muestran todas las listas o bibliotecas, así como los elementos de lista.

10. Seleccione el sitio o el canal específico disponible en la recopilación de sitios que desea restaurar desde la recopilación de sitios de SharePoint y haga clic en **Siguiente**.

    Notas:

    - Se puede seleccionar todo el contenido o el contenido parcial del objeto de SharePoint que se va a restaurar. Para seleccionar parte del contenido, expanda el objeto y, a continuación, haga clic en la casilla de verificación de dicho contenido.
    - Puede seleccionar varias listas o bibliotecas de SharePoint, o los elementos de lista que desea restaurar.

    Se abrirá el cuadro de diálogo Opciones de restauración.



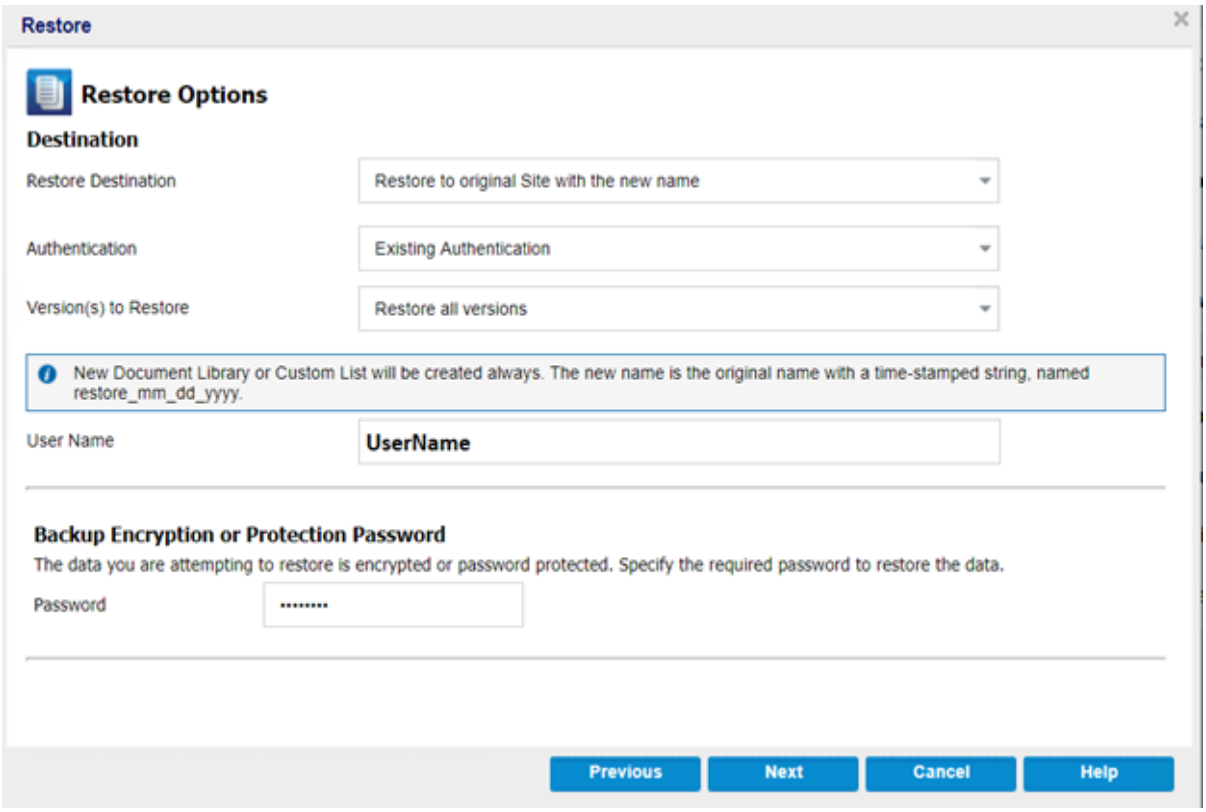
Las listas o bibliotecas de SharePoint Online, así como los elementos de lista que se van a restaurar, están seleccionados. Ahora, se pueden definir las opciones de restauración.

Definición de las opciones de restauración

Después de especificar la información de SharePoint Online que se debe restaurar, defina las opciones de restauración para el contenido seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo Opciones de restauración, seleccione el destino para la restauración.



A continuación se especifican las opciones de destino disponibles:

Restaurar al sitio original con el nombre nuevo

Restaura los datos de la lista o de la biblioteca, así como de los elementos de lista, en el mismo sitio con un nuevo nombre de lista desde donde se ha realizado una copia de seguridad.

Restaurar en la ubicación original

Restaura los datos de la lista o de la biblioteca, así como de los elementos de lista, en la misma ubicación desde donde se ha realizado una copia de seguridad.

2. Especifique una de las siguientes opciones del menú desplegable Si el elemento ya existe en la lista desplegable Destino:

Añadir como nueva versión si está activado el control de versiones

Esta opción funciona cuando está activada la configuración de la versión en la configuración de la biblioteca en el sitio de SharePoint. Una vez que se selecciona esta opción, la nueva versión se agrega a las versiones actuales de los elementos de lista si existen elementos de lista.

Omitir el elemento y no restaurar

Se omiten los elementos y no se restaurará.

Sobrescribir el elemento en el destino

Sobrescribe el elemento en el destino.

Exportar a disco

Restaura las listas y las bibliotecas, así como los elementos de lista de la recopilación de sitios, a la carpeta o a la carpeta del recurso compartido del disco.

Nota: Para la restauración de las listas cuando se selecciona la opción de restauración de la opción Exportar a disco, solo se exportan los datos adjuntos de la lista al disco.

Autentificación

Valida e identifica la cuenta de usuario. Seleccione una de las opciones siguientes:

- **Autenticación existente**

  Cuando se selecciona Autenticación existente, se utiliza el tipo de autenticación que se ha seleccionado durante la creación del nodo.

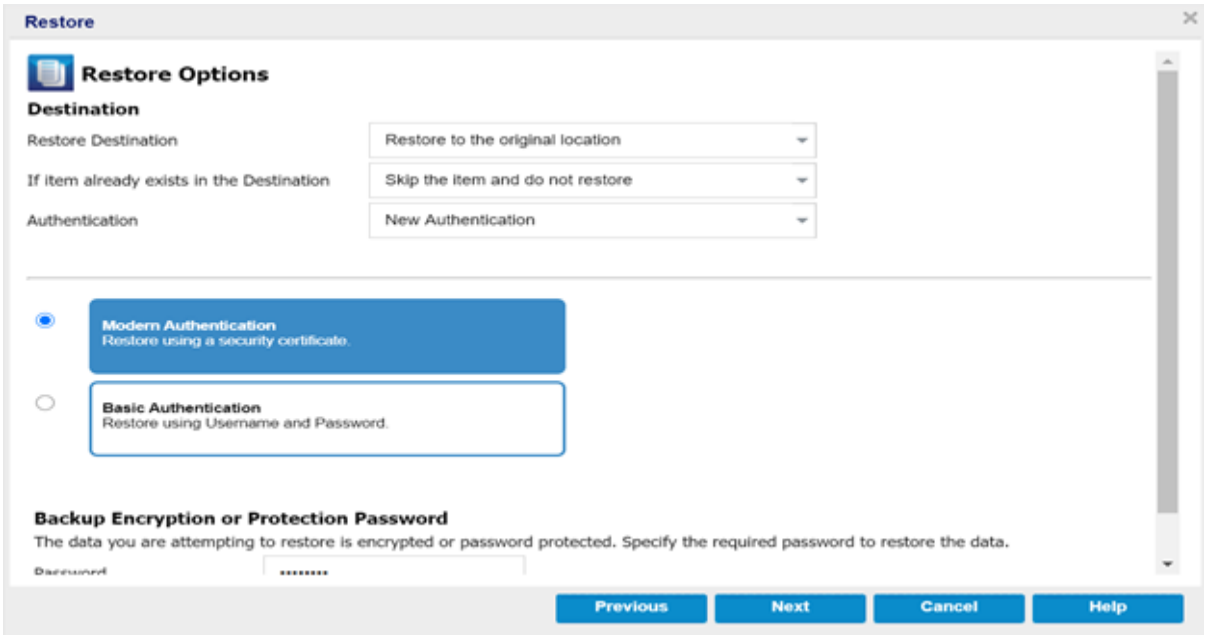
  - Si la autenticación del nodo es básica, se cargan automáticamente parámetros como Nombre de usuario, Contraseña y Cifrado de la copia de seguridad o Contraseña de protección [Si está cifrada] para continuar con la restauración.
  - Si la autenticación del nodo es moderna, se cargan automáticamente parámetros como Nombre de usuario y Cifrado de la copia de seguridad o Contraseña de protección [Si está cifrada] para continuar con la restauración.

- **Nueva autenticación**

  Durante la restauración, se puede seleccionar una de las siguientes opciones para cambiar el tipo de autenticación:

  - Autenticación moderna

- Autenticación básica



3. Para aplicar la autenticación, realice una de las siguientes acciones:

Autenticación moderna

Para la autenticación moderna, se puede ejecutar una restauración utilizando un certificado de seguridad.

Utilizar certificado de seguridad

Nota: De forma predeterminada, el plan de copia de seguridad selecciona **Utilizar certificado de seguridad** para la autenticación moderna.

Siga estos pasos:

a. Para autenticarse mediante un certificado autofirmado, consulte Descarga del certificado desde UDP y carga del certificado en Azure.

b. Introduzca el ID de la aplicación y el Nombre de usuario.

c. Para aplicar los roles y permisos necesarios, seleccione la casilla de verificación **Permitir a Arcserve UDP establecer los roles y permisos de Azure necesarios para esta aplicación** y, a continuación, haga clic en **Siguiente**.

Autenticación básica

Para la Autenticación básica, introduzca el nombre de usuario y la contraseña para continuar con la restauración.

Nota: Esta opción produce un error si tiene activada la autenticación moderna en el inquilino o en la cuenta.

4. Especifique las versiones del elemento de lista que se van a restaurar cuando se active la configuración de la versión desde la configuración de la biblioteca en el sitio de SharePoint.

   Restaurar todas las versiones

   Restaura todas las versiones durante la copia de seguridad.

   Restaurar solo la versión más reciente

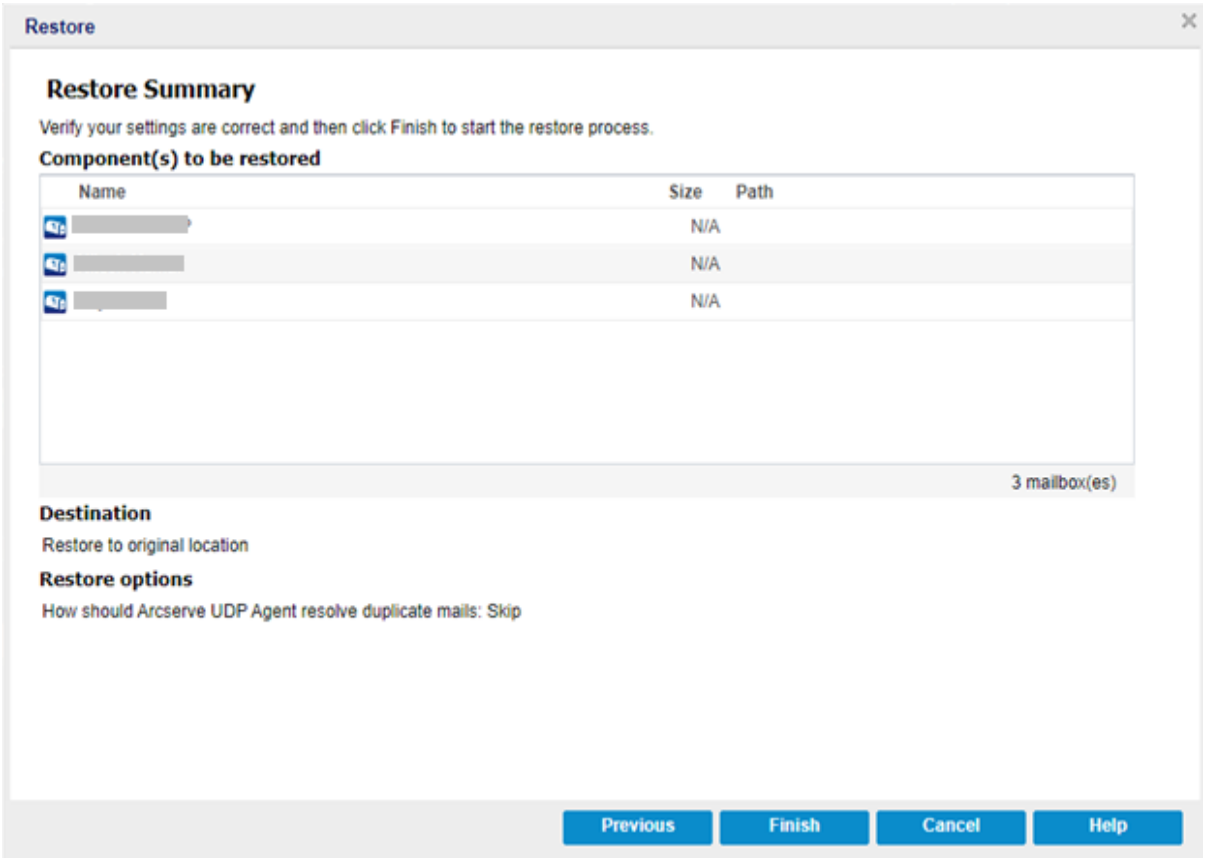
   Restaura solo la versión más reciente durante la copia de seguridad.

   Restaurar solo la última versión principal

   Restaura solo la última versión principal durante la copia de seguridad.

5. Especifique la contraseña de la sesión si la tiene.
6. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo Resumen de la restauración.



Se puede verificar la información sobre la restauración en el cuadro de diálogo Resumen de la restauración.

7. Haga clic en **Finalizar** para enviar la tarea de restauración.

   Las opciones de restauración se han definido para restaurar la información de SharePoint Online.

Verificación de que se ha restaurado el contenido

Después de la terminación del proceso de restauración, verifique que el contenido se ha restaurado en el destino especificado.

Siga estos pasos:

1. Inicie sesión en la Colección de sitios de SharePoint.
2. Verifique la lista y la biblioteca, así como los elementos de lista.
3. Verifique el contenido restaurado.

   El contenido restaurado se ha verificado correctamente.

Mapa de protección de datos para Microsoft Teams

Importante: Los datos de Teams para toda una organización se protegen automáticamente si las tareas de Exchange, SharePoint y OneDrive se configuran para usar la opción *proteger todo* para cuentas y sitios.

La tabla siguiente describe el mapa de protección de datos para Microsoft Teams:

Elemento de Teams	De qué se debe realizar una copia de seguridad en UDP	Desde dónde restaurar
Grabaciones de reuniones programadas	Cuenta de OneDrive del usuario que realiza las grabaciones	Interfaz de usuario del agente para la cuenta de OneDrive del usuario
Chats, publicaciones y conversaciones privados y personales	Buzón de correo de Exchange del usuario	Interfaz de usuario del agente para Exchange
Archivos enviados a través de un chat personal	Buzón de Exchange o cuenta de OneDrive del usuario	Interfaz de usuario del agente para el usuario de Exchange y para la cuenta de OneDrive del usuario
Elementos en el canal estándar de Teams		
Chats, publicaciones y conversaciones	Buzón de correo de grupo del canal estándar	Interfaz de usuario del agente para el buzón de correo de grupo
Calendario de equipos para el canal	Buzón de correo de grupo del canal estándar	Interfaz de usuario del agente para el buzón de correo de grupo
Archivos enviados a través de las conversaciones de	Seleccionar el sitio de SharePoint de los sitios del	Interfaz de usuario del

los chats	canal/*Proteger todos* o el buzón de correo del grupo del canal	agente de SharePoint > Sitio para el canal estándar > Biblioteca de documentos O interfaz de usuario del agente de Exchange > Buzón de correo de grupo
Archivos o carpetas cargados utilizando la ficha Archivos	Seleccionar el sitio de SharePoint de los sitios del canal/*Proteger todos*	Interfaz de usuario del agente de SharePoint > Sitio para el canal estándar > Biblioteca de documentos
Elementos en el canal privado de Teams		
Chats, publicaciones y conversaciones	Buzón de correo de Exchange del usuario	Interfaz de usuario del agente para el buzón de correo del usuario
Archivos enviados a través de las conversaciones de los chats	Seleccionar el sitio de SharePoint de los sitios del canal/*Proteger todos* o el buzón de correo del usuario	Interfaz de usuario del agente de SharePoint > Sitio para el canal estándar > Biblioteca de documentos O interfaz de usuario del agente de Exchange > Buzón de correo del usuario
Archivos o carpetas cargados utilizando la ficha Archivos	Seleccionar el sitio de SharePoint de los sitios del canal/*Proteger todos*	Interfaz de usuario del agente de SharePoint > Sitio para el canal estándar > Biblioteca de documentos

Cómo crear y configurar máquinas virtuales instantáneas simultáneas en varios hipervisores

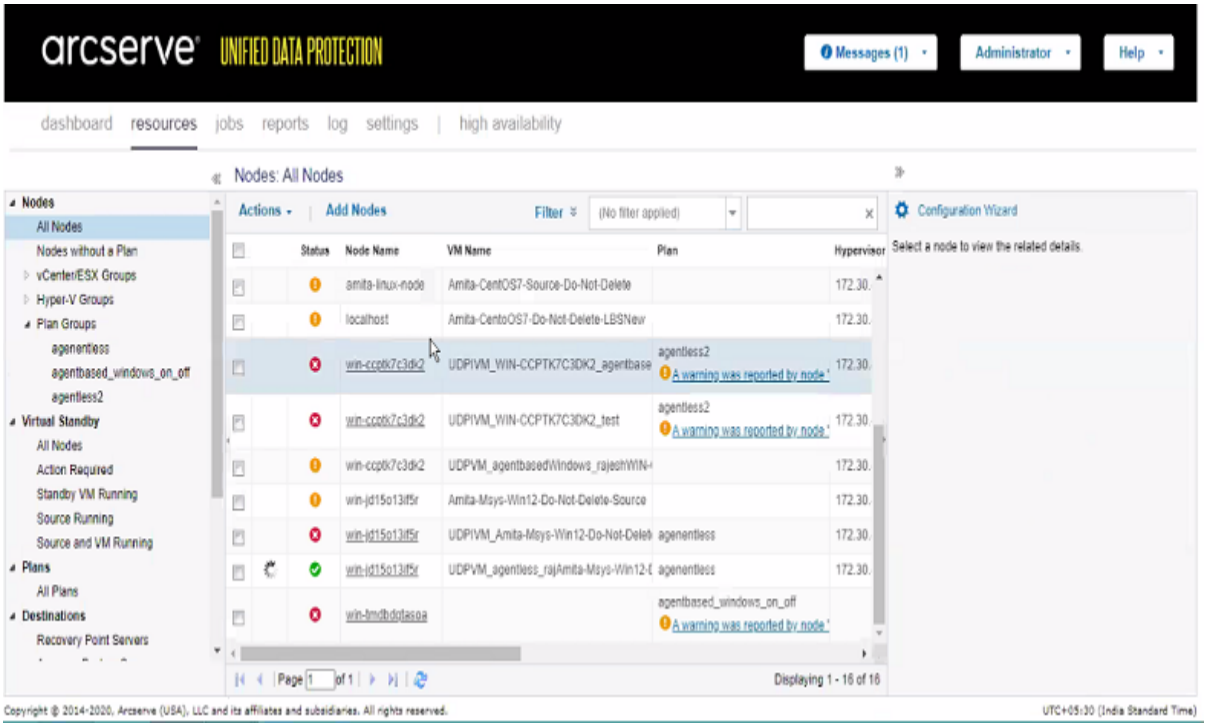
Esta sección proporciona información sobre cómo crear y configurar máquinas virtuales instantáneas simultáneas en varios hipervisores como, por ejemplo, Hyper-V, VMware, Nutanix AHV, Amazon EC2 y Microsoft Azure.

Se pueden crear máquinas virtuales instantáneas simultáneas desde la Consola de Arcserve UDP mediante el Asistente para la creación de una máquina virtual instantánea.

Para abrir el Asistente para la creación de una máquina virtual instantánea, siga estos pasos:

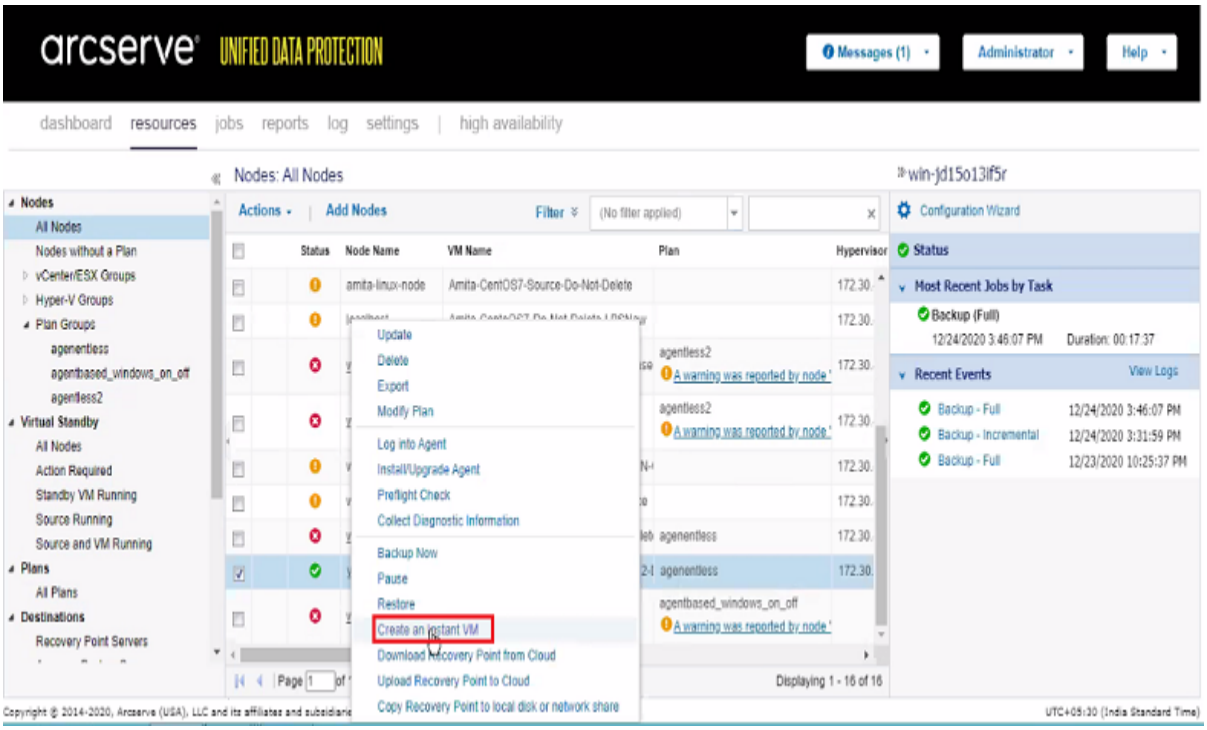
1. Inicie sesión en la cuenta de la Consola de UDP.
2. En la página de la Consola de UDP, haga clic en la ficha **recursos**.
3. En el panel izquierdo, vaya a **Nodos** > **Todos los nodos**.

   La lista de nodos existentes aparece en el panel central.



4. Seleccione uno o más nodos que ya estén asociados a un plan.

   Nota: Si un nodo no está asociado a ningún plan, no aparecerá la opción Crear una máquina virtual instantánea.



5. Haga clic con el botón secundario del ratón en los nodos seleccionados y, a continuación, seleccione la opción **Crear una máquina virtual instantánea**.

Se abre el asistente de creación de una máquina virtual instantánea. En el asistente, se pueden configurar máquinas virtuales instantáneas simultáneas.

Para configurar las máquinas virtuales instantáneas simultáneas, siga estos pasos:

1. Selección de un servidor de punto de recuperación de origen
2. Selección de la ubicación de las máquinas virtuales
3. Selección de servidores de recuperación
4. Configuración de las máquinas virtuales
5. Verificación del resumen

Selección de un servidor de puntos de recuperación de origen

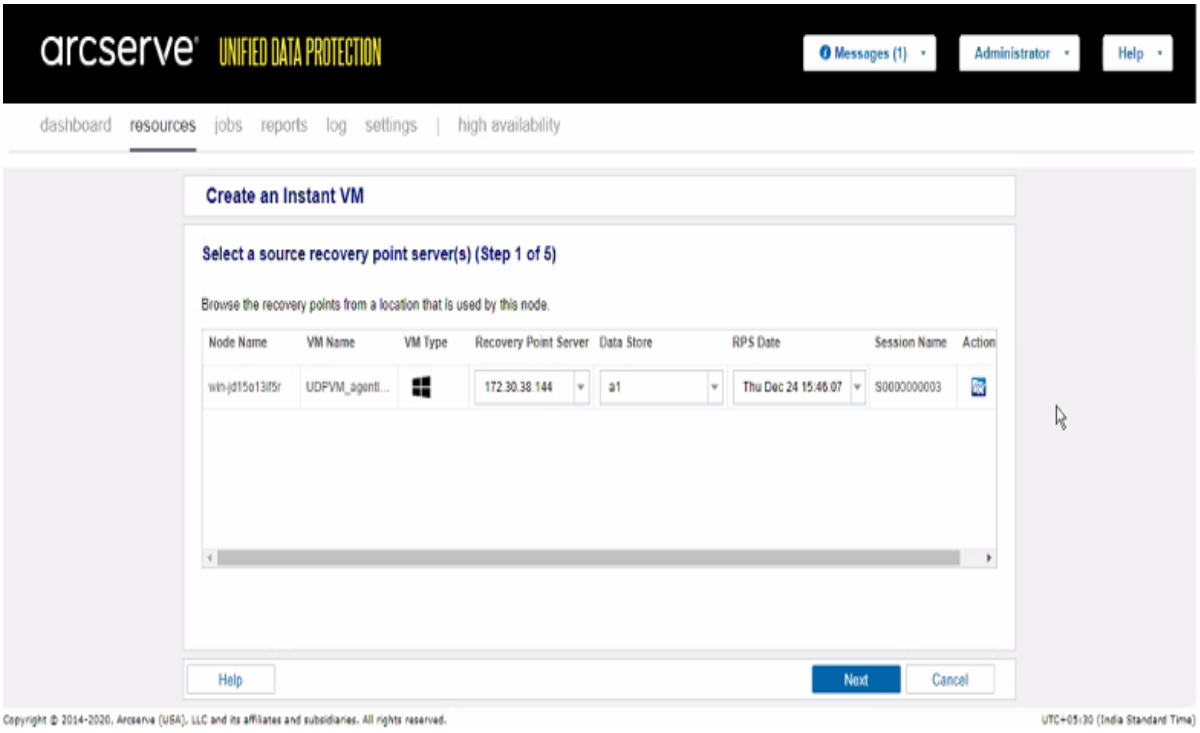
Esta sección proporciona información sobre cómo realizar el primer paso para seleccionar un punto de recuperación de origen.

La pantalla Selección de un servidor de puntos de recuperación de origen muestra la lista de nodos seleccionados con detalles como Nombre de nodo, Nombre de máquina virtual, Tipo de máquina virtual, Servidor de puntos de recuperación,

Almacén de datos, Fecha del servidor de puntos de recuperación, Nombre de sesión y Acción. Para cada nodo de la lista, la consola selecciona automáticamente los detalles de las opciones Servidor de puntos de recuperación, Almacén de datos y Fecha del servidor de puntos de recuperación. También se pueden cambiar estos detalles si hay varios servidores de puntos de recuperación disponibles en cada nodo.

Siga estos pasos:

1. En la pantalla Selección de un servidor de puntos de recuperación de origen, en cada nodo, realice lo siguiente:



   - Para Servidor de puntos de recuperación, en la lista desplegable, seleccione el servidor de puntos de recuperación requerido.
   - Para Almacén de datos, seleccione el almacén de datos necesario en la lista desplegable.
   - Para Fecha del servidor de puntos de recuperación, seleccione la fecha del servidor de puntos de recuperación en la lista desplegable.
2. Haga clic en **Siguiente**.
3. (Opcional) Si la sesión de la copia de seguridad está cifrada para cualquiera de los nodos seleccionados, introduzca la contraseña.

   Aparecerá la pantalla Ubicación de las máquinas virtuales.

Complete el siguiente paso: Selección de la ubicación de las máquinas virtuales

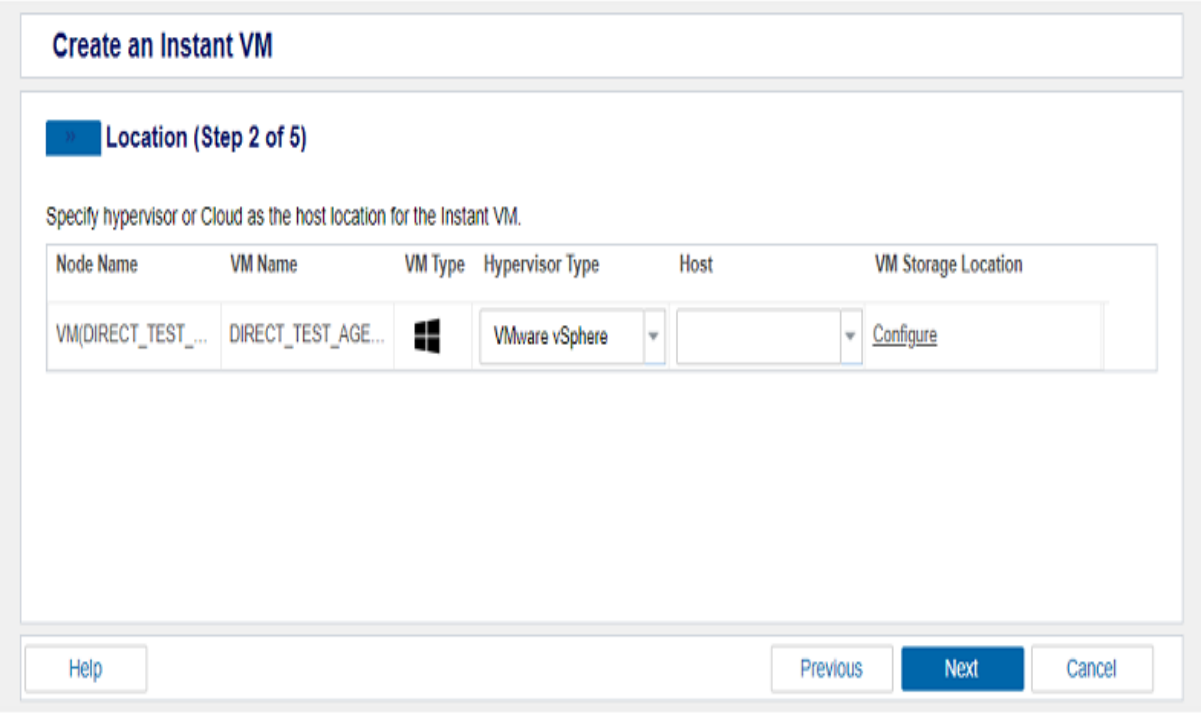
Selección de la ubicación de las máquinas virtuales

Esta sección proporciona información sobre cómo realizar el segundo paso de la selección de una ubicación de la máquina virtual para alojar la máquina virtual instantánea.

La pantalla Ubicación de las máquinas virtuales muestra la lista de nodos seleccionados con detalles como Nombre de máquina virtual, Tipo de máquina virtual, Tipo de hipervisor y Host. Para cada nodo de la lista, se puede seleccionar el tipo de hipervisor y la ubicación de la máquina virtual para alojar la máquina virtual instantánea.

Siga estos pasos:

1. En la pantalla Ubicación de las máquinas virtuales, en cada nodo, realice lo siguiente:



Nodo de Windows

- Para Tipo de hipervisor, en la lista desplegable, seleccione el tipo de hipervisor.

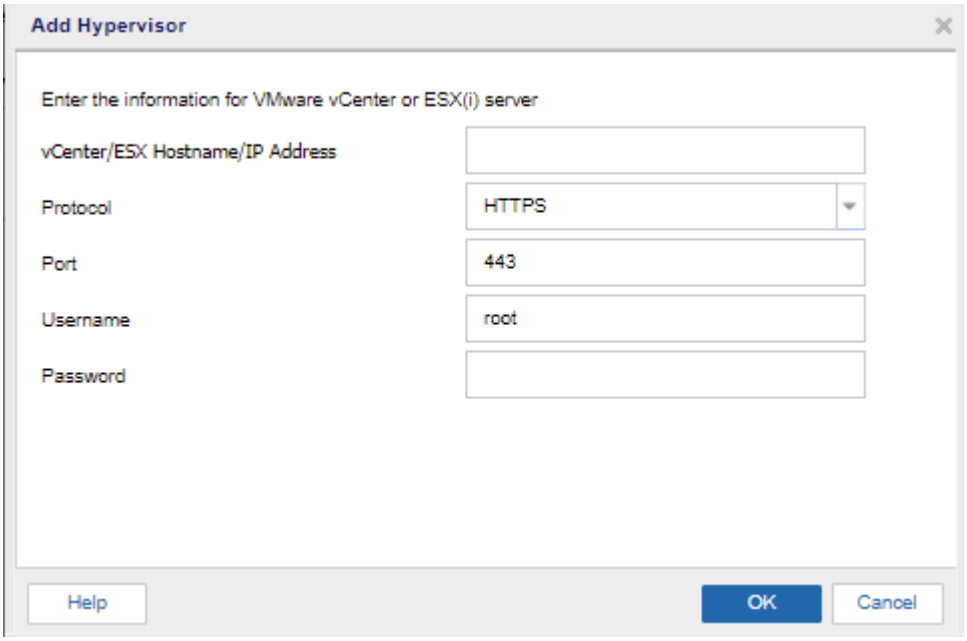
  Nota: Arcserve UDP es compatible con VMware y Hyper-V para alojar los nodos de la máquina virtual instantánea para Windows.

- Para Host, en la lista desplegable, seleccione el hipervisor existente o agregue un hipervisor nuevo.

  Para agregar un nuevo hipervisor, siga estos pasos:

  a. En la lista desplegable Host, haga clic en **+ Agregar nuevo hipervisor**.

     Aparecerá el cuadro de diálogo Agregar hipervisor.



  b. En el cuadro de diálogo Agregar hipervisor, proporcione los detalles siguientes según sea necesario:

     - **Nombre de host/dirección IP de ESX/vCenter:** Especifique el nombre de host o la dirección IP de vCenter.
     - **Protocolo:** Seleccione el protocolo como HTTP o HTTPS.
     - **Puerto**: Introduzca el número de puerto.
     - **Nombre de usuario**: Especifique el nombre de usuario.
     - **Contraseña:** Introduzca la contraseña.

  c. Haga clic en **Aceptar**.

     Se agrega el nuevo hipervisor.

- Para Ubicación del almacenamiento de la máquina virtual, para configurar la selección de la ubicación del almacenamiento de VMware, haga clic en **Configurado**.

Nodo de Linux

- Para Tipo de hipervisor, en la lista desplegable, seleccione el tipo de hipervisor.

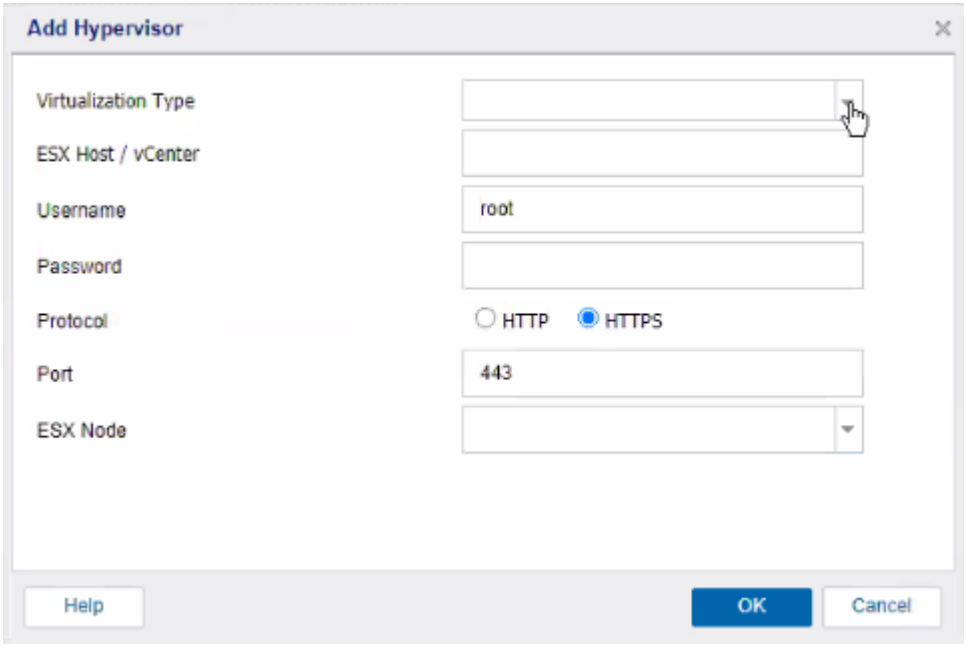
  Nota: Arcserve UDP es compatible con VMware, Hyper-V, Nutanix AHV, Amazon EC2 y Microsoft Azure para alojar la máquina virtual instantánea para los nodos de Linux.

- Para Host, en la lista desplegable, seleccione el hipervisor existente o agregue un hipervisor nuevo.

  Para agregar un nuevo hipervisor, siga estos pasos:

  a. En la lista desplegable Host, haga clic en **+ Agregar nuevo hipervisor**.

     Aparecerá el cuadro de diálogo Agregar hipervisor.



  b. En el cuadro de diálogo Agregar hipervisor, en la lista desplegable Tipo de virtualización, seleccione una de las siguientes opciones:

     VMware

     Proporcione los siguientes detalles según sea necesario:

- **Host de ESX/vCenter:** Especifique el nombre de host o la dirección IP de vCenter.
- **Nombre de usuario**: Especifique el nombre de usuario.
- **Contraseña:** Introduzca la contraseña.
- **Protocolo:** Seleccione el protocolo como HTTP o HTTPS.
- **Puerto**: Introduzca el número de puerto.
- **Nodo de ESX:** En el menú desplegable, seleccione uno de los nodos disponibles.

Hyper-V

Proporcione los siguientes detalles según sea necesario:

- **Nombre de host de Hyper-V:** Especifique el nombre de host para el hipervisor de Hyper-V.
- **Nombre de usuario**: Especifique el nombre de usuario.
- **Contraseña:** Introduzca la contraseña.

Nutanix AHV

Proporcione los siguientes detalles según sea necesario:

- **Dirección IP virtual del clúster de Nutanix AHV:** Especifique la dirección IP.
- **Nombre de usuario**: Especifique el nombre de usuario.
- **Contraseña:** Introduzca la contraseña.
- **Puerto**: Introduzca el número de puerto.

EC2

Proporcione los siguientes detalles según sea necesario:

- **Nombre de cuenta:** Especifique el nombre de la cuenta de la nube. Si no se agrega la cuenta de la nube, haga clic en Agregar. Para obtener más información, consulte Adición de una

cuenta de la nube.

- **Región:** En el menú desplegable, seleccione la región disponible.

Azure

Proporcione los siguientes detalles según sea necesario:

- **Nombre de cuenta:** Especifique el nombre de la cuenta de la nube. Si no se agrega la cuenta de la nube, haga clic en Agregar. Para obtener más información, consulte Adición de una cuenta de la nube.
- **Grupo de recursos:** En el menú desplegable, seleccione el grupo de recursos disponible.
- **Región:** En el menú desplegable, seleccione la región disponible.

c. Haga clic en **Aceptar**.

Se agrega el nuevo hipervisor.

- Para Ubicación del almacenamiento de la máquina virtual, para configurar la selección de la ubicación del almacenamiento de VMware, haga clic en **Configurado**.

2. Haga clic en **Siguiente**.

Aparece la pantalla Servidores de recuperación.

Complete el siguiente paso: Selección de servidores de recuperación

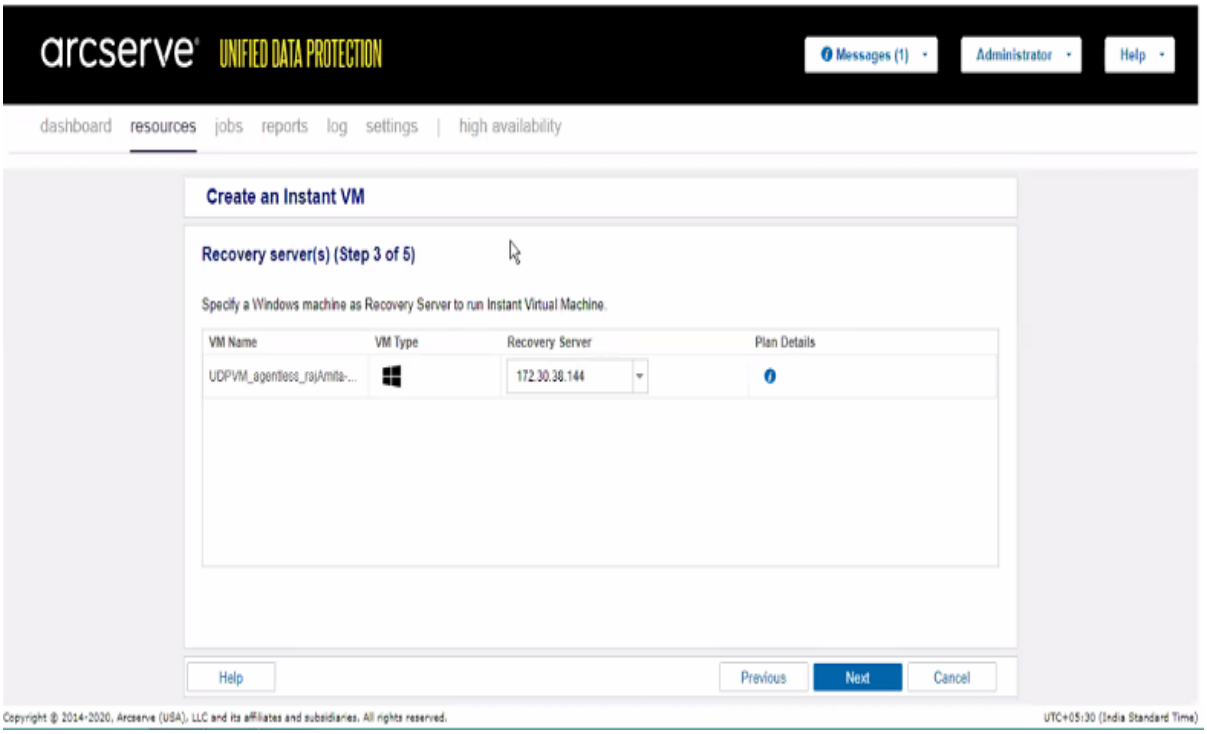
Selección de servidores de recuperación

Esta sección proporciona información sobre cómo realizar el tercer paso de la selección de un servidor de recuperación para ejecutar la máquina virtual instantánea.

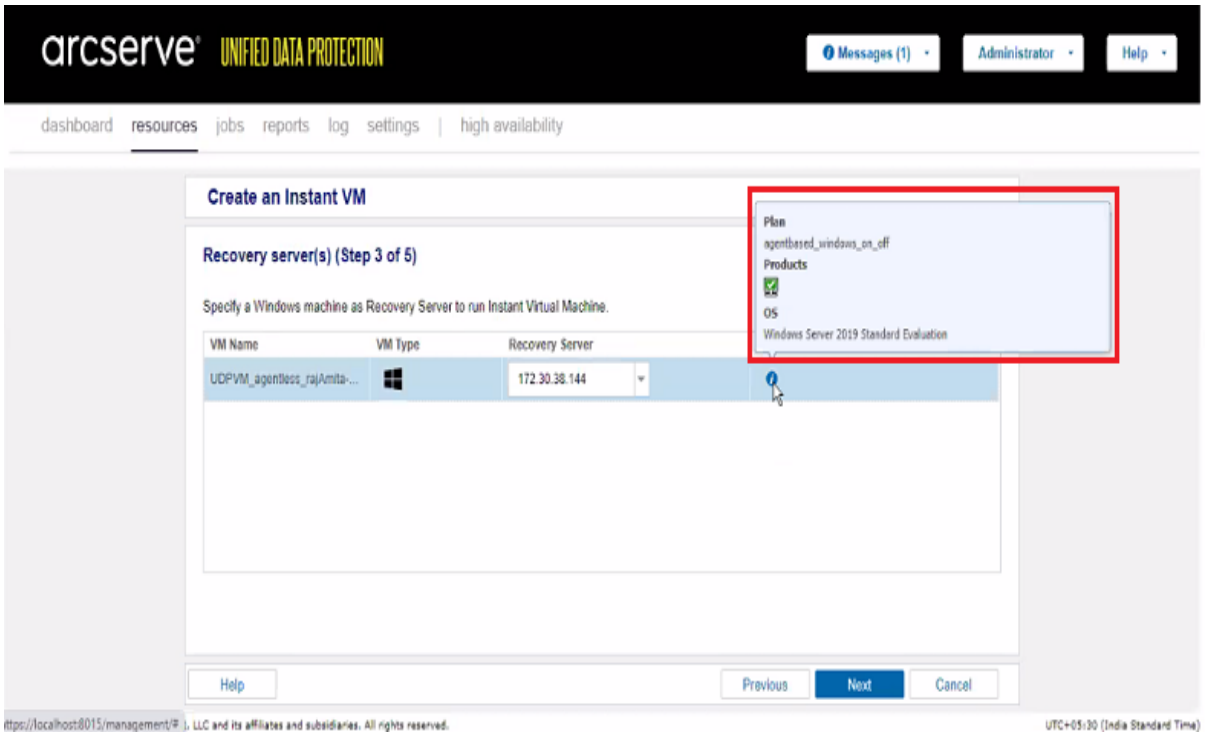
La pantalla Servidores de recuperación muestra la lista de nodos seleccionados con detalles como Nombre de máquina virtual, Tipo de máquina virtual, Servidor de recuperación y Detalles del plan. Para cada nodo de la lista, se puede seleccionar el servidor de recuperación para ejecutar la máquina virtual instantánea.

Siga estos pasos:

1. En la pantalla Servidores de recuperación, en cada nodo, realice lo siguiente:



   - Para Servidor de recuperación, en la lista desplegable, seleccione el servidor de recuperación requerido.
   - Para Detalles del plan, coloque el cursor sobre el icono de información para verificar los detalles del plan.



Notas:

- Para las sesiones de copia de seguridad de Linux, el servidor de recuperación es un servidor de copia de seguridad de Linux.
- En estos casos, debe instalarse el rol de Network File System (NFS) de Windows en el servidor de puntos de recuperación. Se instala automáticamente durante el proceso de la máquina virtual instantánea. Para instalarlo de forma manual, consulte Cómo instalar el sistema de archivos de red en Windows Server.

2. Haga clic en **Siguiente**.

   Aparecerá la pantalla Configuración de las máquinas virtuales.

Complete el siguiente paso: Configuración de las máquinas virtuales

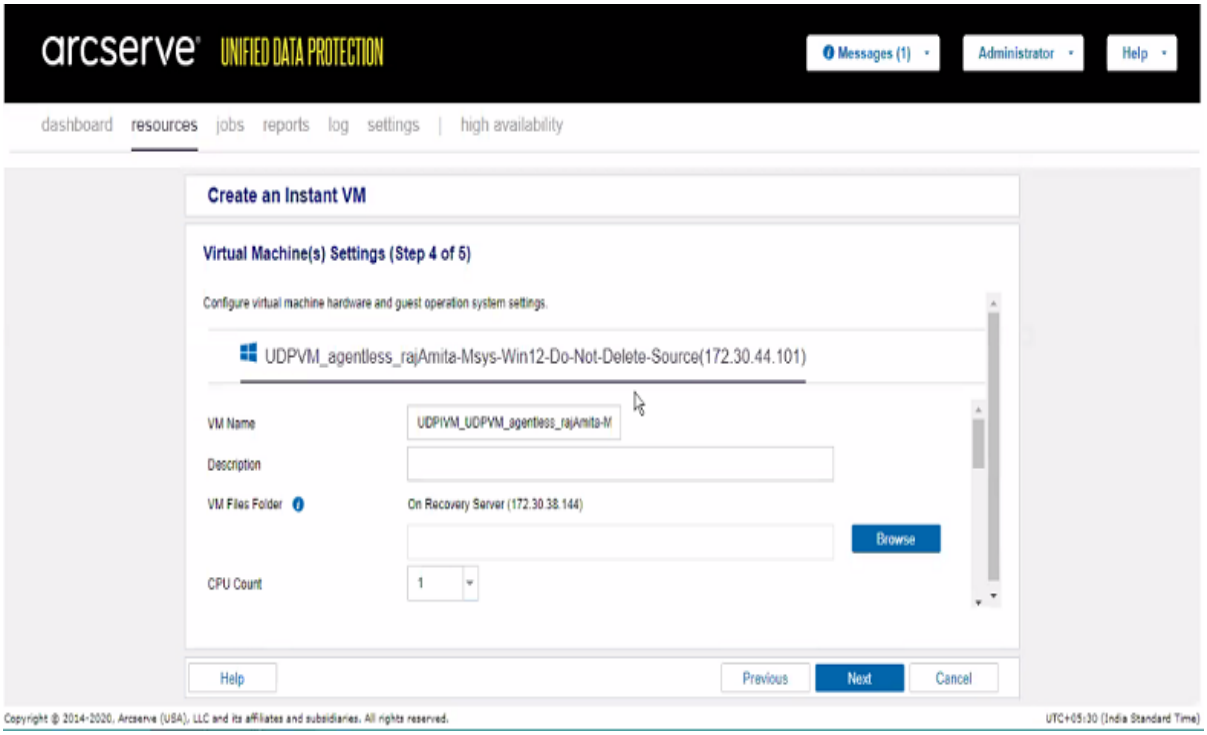
Configuración de las máquinas virtuales

Esta sección proporciona información sobre cómo configurar los valores de configuración de la máquina virtual para crear una máquina virtual instantánea.

La pantalla Configuración de las máquinas virtuales muestra secciones individuales para cada nodo seleccionado con los detalles de configuración. En cada sección, se pueden proporcionar los detalles según sea necesario para crear la máquina virtual instantánea.

Siga estos pasos:

1. En la pantalla Configuración de las máquinas virtuales, haga clic en el nodo de la máquina virtual que desea configurar.



2. En el nodo de la máquina virtual seleccionada, realice lo siguiente:
   - En Nombre de máquina virtual, escriba el nombre de la máquina virtual instantánea. El nombre del nodo de origen con un prefijo es el nombre predeterminado de la máquina virtual instantánea.
   - (Opcional) En Descripción, escriba la descripción necesaria para la máquina virtual instantánea.
   - Para Carpeta de los archivos de la máquina virtual, haga clic en el botón **Examinar** para seleccionar la ubicación de la carpeta en el servidor de recuperación para la máquina virtual instantánea. También se puede crear una nueva carpeta desde el cuadro de diálogo Carpeta de los archivos de la máquina virtual.

     Nota: La opción Carpeta de los archivos de la máquina virtual solo está disponible para los nodos de la máquina virtual de Windows. Para el nodo de la máquina virtual de Linux, se puede seleccionar el almacén de datos disponible en la lista desplegable del almacén de datos de archivos de máquina virtual.
   - En Número de CPU, seleccione el número de CPU para la máquina virtual instantánea.

- En Tamaño de memoria, escriba el tamaño de memoria para la máquina virtual instantánea.

  Nota: También se puede utilizar el control deslizante para proporcionar el tamaño de memoria para la máquina virtual instantánea.

- Para Adaptadores de red, haga lo siguiente:

  Agregar un adaptador

  Se pueden agregar varios adaptadores de red. Después de agregar un adaptador de red, se puede modificar y suprimir el adaptador de red en la columna Acciones.

  Nota: Para una máquina virtual instantánea de Linux, se puede utilizar al menos una tarjeta NIC virtual para conectarse al servidor de copia de seguridad de Linux.

  Para agregar un adaptador de red, siga estos pasos:

  a. En la sección Adaptador de red, haga clic en **Agregar un adaptador**.

     Aparecerá el cuadro de diálogo Agregar adaptador de red.

  b. En el cuadro de diálogo Agregar adaptador de red, introduzca los siguientes detalles y, a continuación, haga clic en **Aceptar**.

     - **Red virtual:** En la lista desplegable Red virtual, seleccione la red virtual necesaria.
     - **Tipo de adaptador:** En la lista desplegable Tipo de adaptador, seleccione el tipo de adaptador.
     - **Configuración de TCP/IP:** En la lista desplegable Configuración de TCP/IP, seleccione **Origen (automático)** o **Configuración personalizada de IP/puerta de enlace/DNS/WINS** según sea necesario.

       Nota: Si selecciona la opción Configuración personalizada de IP/puerta de enlace/DNS/WINS, haga clic en Agregar una dirección para proporcionar los detalles de TCP/IP manualmente.

  Se agrega el adaptador de red.

  Actualizar DNS

  Si ya se ha proporcionado una dirección IP y una dirección DNS en el adaptador de red y el equipo de origen de un dominio, se

puede actualizar el DNS mediante los siguientes pasos:

Nota: Esta función solo está disponible para la máquina virtual instantánea de Windows.

a. En la sección Adaptador de red, haga clic en **Actualizar DNS**.

b. Para agregar un registro de actualización de DNS, haga clic en **Agregar una dirección de DNS**.

Notas:

- Se puede eliminar el registro de actualización de DNS. Para eliminar, haga clic en **Eliminar**.
- Para ajustar la secuencia de los registros, haga clic en los botones Arriba y Abajo.

c. Seleccione una dirección de DNS y una dirección IP en la lista desplegable y, a continuación, haga clic en **Aceptar**.

d. Especifique el Período de vida (TTL).

e. Especifique la Autenticación de DNS.

Para Microsoft DNS Server, introduzca el nombre de usuario y la contraseña. Para Servidor BIND, es necesario especificar la ruta completa, incluido el nombre de archivo del archivo de claves en el servidor de recuperación.

- Para la configuración avanzada, haga lo siguiente:
  - Compruebe el espacio libre en disco de la capacidad de la carpeta de archivos de la máquina virtual.

    Nota: La casilla de verificación **Controlar espacio libre en disco de la capacidad de la carpeta de archivos de la máquina virtual** está activada de forma predeterminada. La barra de capacidad aparece en amarillo en la página de las máquinas virtuales instantáneas si el espacio libre de la capacidad de la carpeta de archivos de la máquina virtual es menor que el valor del umbral. El valor predeterminado del umbral es 3 %. Se puede cambiar el valor según sea necesario.
  - Seleccione la casilla de verificación **Especificar el tipo de controlador de disco para la máquina virtual** y, a continuación, seleccione en la lista desplegable, el tipo de controlador de disco para la máquina virtual.

Nota: La casilla de verificación **Especificar el tipo de controlador de disco para la máquina virtual** está disponible si se ha seleccionado la casilla de verificación **VMware vSphere** como la ubicación de la máquina virtual. Se crea la máquina virtual instantánea aplicando el controlador de disco especificado en VMware.

- Para volver a dirigir las actualizaciones del disco virtual al almacén de datos de VMware, siga estos pasos:

  a. Seleccione la casilla de verificación **Redirigir las actualizaciones del disco virtual al almacén de datos de VMware**.

     Nota: La casilla de verificación **Redirigir las actualizaciones del disco virtual al almacén de datos de VMware** solo está disponible cuando se selecciona VMware vSphere como ubicación de la máquina virtual.

  b. En el menú desplegable, seleccione el almacén de datos de VMware requerido.

  Las actualizaciones del disco virtual se redirigen al almacén de datos seleccionado de VMware.

- Para cambiar el nombre de host de la máquina virtual instantánea, siga estos pasos:

  a. Haga clic en la casilla de verificación **Cambiar nombre de host**.

     La pantalla se actualiza con los nuevos campos.

  b. En el campo Nuevo nombre de host, escriba el nuevo nombre de host según sea necesario.

  c. Si el equipo de origen está en un dominio, proporcione los detalles siguientes según sea necesario:

     - **Cuenta de usuario:** Escriba la cuenta de usuario.
     - **Contraseña:** Introduzca la contraseña.
     - **Confirmar contraseña:** Vuelva a escribir la contraseña para confirmarla.

     Nota: Si el equipo de origen está en un dominio, se debe disponer de los permisos de cuenta para cambiar el nombre de host en el dominio.

- (Opcional) Para la máquina virtual instantánea de Linux, seleccione la casilla de verificación **Recuperar los datos automáticamente después de iniciar la máquina virtual instantánea** para activar la recuperación automática de los datos cuando se inicia el destino de la máquina virtual instantánea.

  El comportamiento predeterminado de la máquina virtual instantánea de Linux es recuperar primero los datos necesarios e iniciar la máquina virtual. Si no se selecciona la opción, cuando se inicia la máquina virtual los datos restantes no se recuperarán incluso si se utiliza una máquina virtual normal. Si la opción está activada, los datos restantes se recuperan en el servidor backend cuando se utiliza la máquina virtual. También puede preservar el destino de la máquina virtual instantánea de forma permanente cuando haya finalizado la recuperación de datos.

  Nota: Cuando el estado del destino de la máquina virtual instantánea de Linux es Apagado, se produce un error en la tarea de máquina virtual instantánea. Si ese punto de recuperación se combina, se produce un error en la máquina virtual instantánea de Linux al encenderse.

3. Haga clic en **Siguiente**.

   Aparecerá la pantalla Resumen.

Complete el último paso: Verificación del resumen

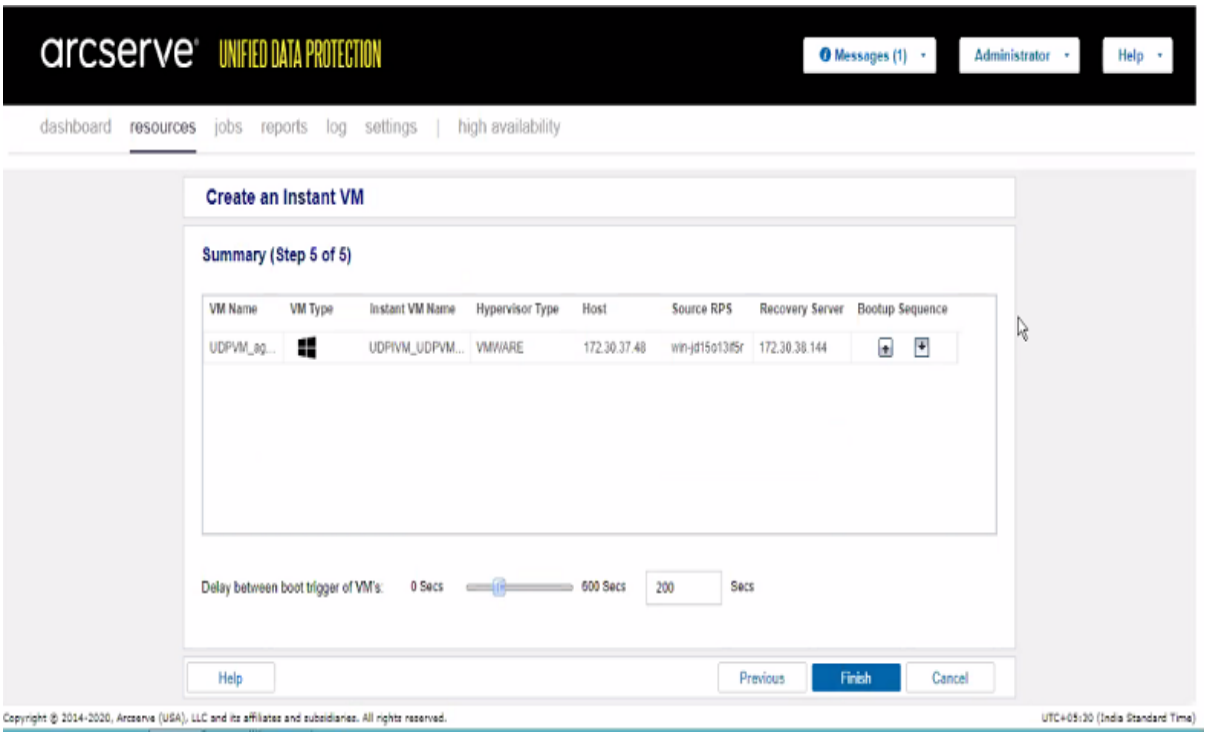
Verificación del resumen

Este es el paso final para crear máquinas virtuales instantáneas simultáneas. Esta sección proporciona información sobre cómo verificar el resumen, ajustar la secuencia de arranque y proporcionar un retraso entre el desencadenador de arranque de las máquinas virtuales.

La pantalla Resumen muestra la lista de nodos seleccionados con detalles como el Nombre de máquina virtual, el Tipo de máquina virtual, el Nombre de la máquina virtual instantánea, el Tipo de hipervisor, el Host, el Servidor de puntos de recuperación de origen, el Servidor de recuperación y la Secuencia de arranque. Se pueden verificar los detalles y dar prioridad a las máquinas virtuales en el orden en el que se desee iniciarlas.

Siga estos pasos:

1. En la pantalla Resumen, realice lo siguiente:



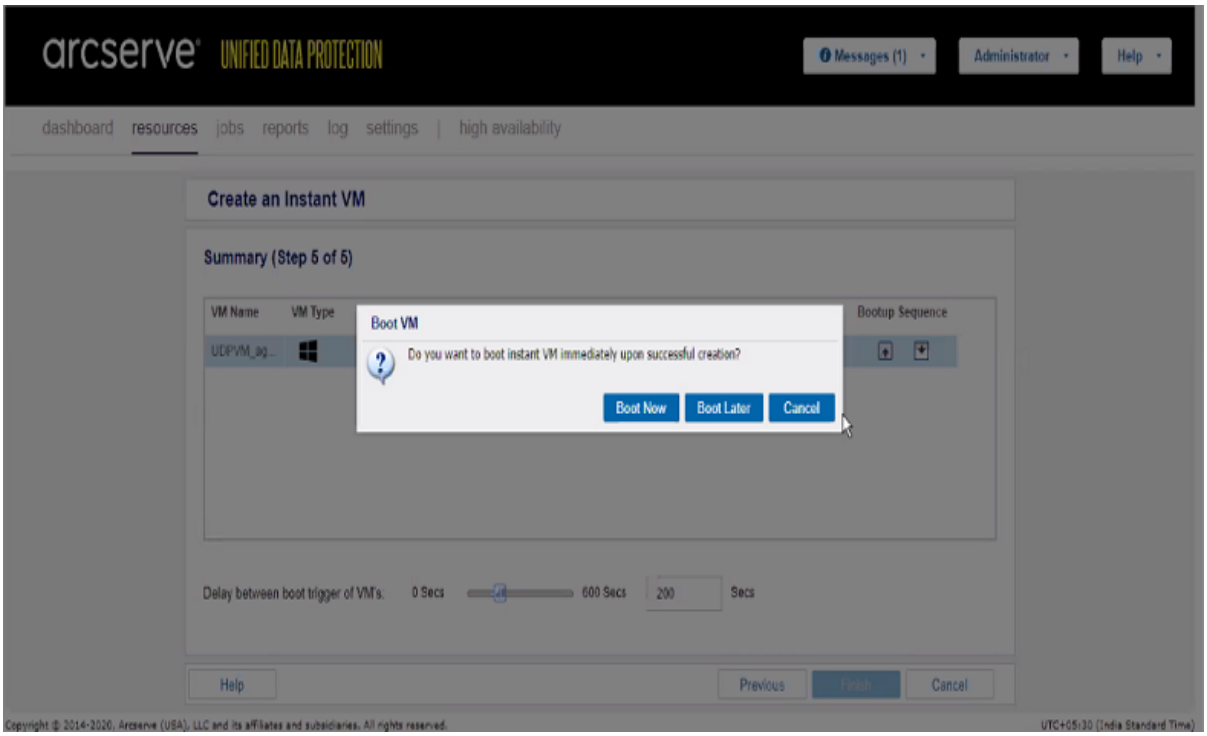
   - En la lista de nodos, en la opción Secuencia de arranque de cada nodo, haga clic en el botón arriba o abajo para priorizar la secuencia de arranque de la máquina virtual.
   - Para Retraso entre el desencadenador de arranque de las máquinas virtuales, escriba el tiempo de retraso en el intervalo de 0 a 600 segundos.

     Nota: También puede utilizar el control deslizante para establecer el tiempo de retraso.

2. Haga clic en **Finalizar**.

   Aparecerá el cuadro de diálogo Arrancar máquina virtual.

3. En el cuadro de diálogo Arrancar máquina virtual, seleccione una de las siguientes opciones:



- **Arrancar ahora:** Crea máquinas virtuales instantáneas simultáneas. Después de crear las máquinas virtuales instantáneas simultáneas, la consola inicia automáticamente las máquinas virtuales.
- **Arrancar más tarde:** Crea máquinas virtuales instantáneas simultáneas. Después de crear las máquinas virtuales instantáneas simultáneas, se pueden iniciar manualmente.
- **Cancelar:** Volverá a la página Crear nuevas máquinas virtuales instantáneas sin crear ninguna máquina virtual instantánea simultánea.

Se crean máquinas virtuales instantáneas simultáneas.

Cómo configurar máquinas de Virtual Standby simultáneas

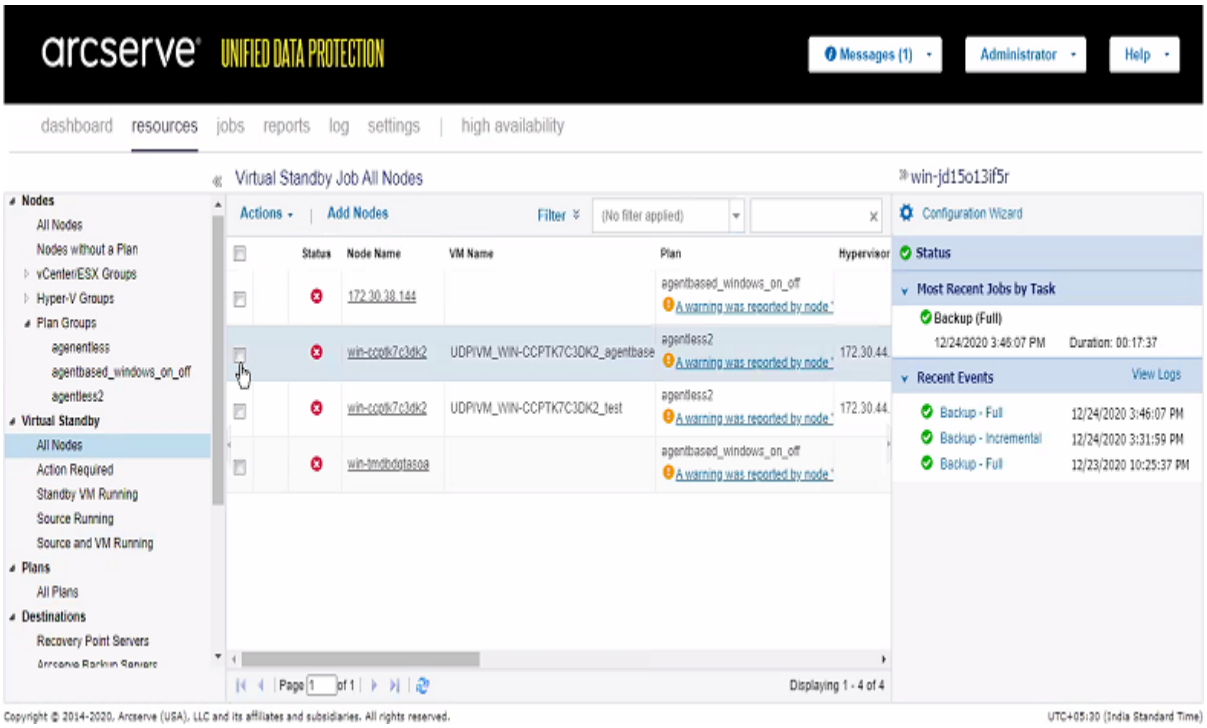
Esta sección proporciona información sobre cómo configurar máquinas de Virtual Standby simultáneas.

Se pueden configurar máquinas de Virtual Standby simultáneas desde la Consola de Arcserve UDP mediante el cuadro de diálogo Máquina de Virtual Standby.

Siga estos pasos:

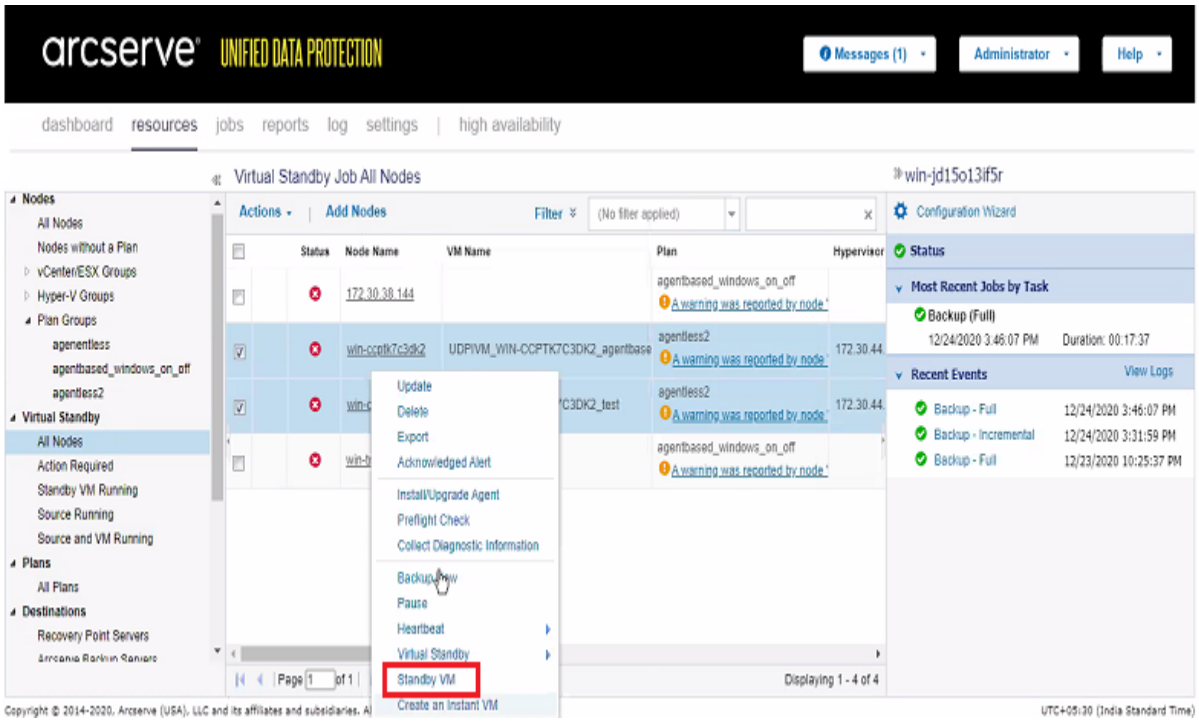
1. Inicie sesión en la Consola de Arcserve UDP.
2. En la página de la Consola de UDP, haga clic en la ficha **recursos**.
3. En el panel izquierdo, vaya a **Nodos** > **Todos los nodos**.

   La lista de nodos existentes aparece en el panel central.



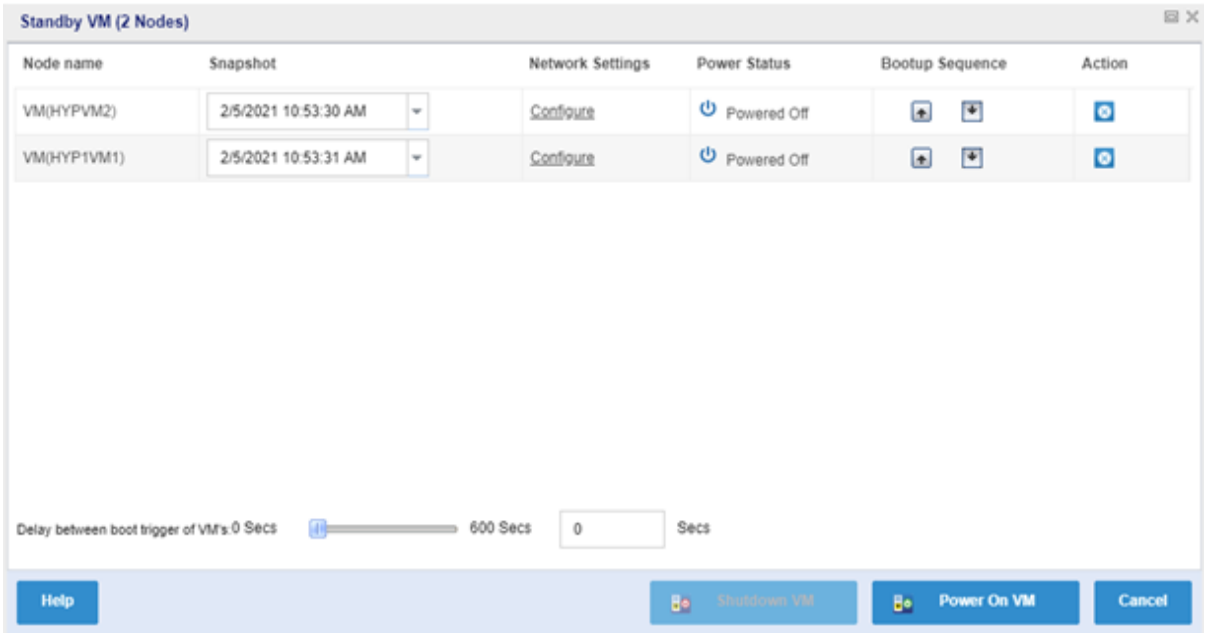
4. Seleccione uno o más nodos que ya estén asociados a un plan.

   Nota: Si un nodo no está asociado con ningún plan, la opción Máquina de Virtual Standby no aparece.



5. Haga clic con el botón secundario del ratón en los nodos seleccionados y, a continuación, seleccione la opción **Máquina de Virtual Standby**.

   Aparece el cuadro de diálogo Máquina de Virtual Standby con la lista de nodos seleccionados.



6. En el cuadro de diálogo Máquina de Virtual Standby, realice las tareas siguientes:

- **Encender la máquina virtual**

  Nota: Esta opción está activada solamente para las máquinas de Virtual Standby apagadas.

  Para encender máquinas virtuales simultáneamente, siga estos pasos:

  a. En la lista de nodos seleccionados, para cada nodo, realice lo siguiente:

     - Para la instantánea, seleccione la fecha y la hora de la instantánea del punto de recuperación en la lista desplegable.

       Nota: Los detalles de la instantánea solo aparecen cuando la tarea de Virtual Standby se completa correctamente.

     - Para Configuración de la red, seleccione el vínculo Configurar. Para obtener más información, consulte Configuración de la red de la máquina de Virtual Standby.

     - Para la secuencia de arranque, haga clic en el botón arriba o abajo para dar prioridad a la secuencia de arranque de la máquina de Virtual Standby.

     - En Acción, haga clic en el icono de la cruz de color azul para eliminar el nodo.

  b. (Opcional) Para Retraso entre el desencadenador de arranque de las máquinas virtuales, escriba el tiempo de retraso en el intervalo de 0 a 600 segundos.

     Nota: También puede utilizar el control deslizante para establecer el tiempo de retraso.

  c. Haga clic en **Encender la máquina virtual**.

     Se encenderán las máquinas de Virtual Standby, utilizando a tal efecto los datos de la instantánea del punto de recuperación.

- **Apagar la máquina virtual**

  Para apagar las máquinas de Virtual Standby simultáneamente, haga clic en **Apagar máquina virtual**.

  Nota: Esta opción está activada solamente para las máquinas de Virtual Standby encendidas.

Capítulo 12: Uso de la instantánea de hardware para la copia de seguridad

Esta sección incluye los siguientes temas:

Cómo utilizar la instantánea de hardware para copias de seguridad

Arcserve UDP puede utilizar las instantáneas de almacenamiento de hardware para realizar copias de seguridad. Se puede especificar si se desea usar una instantánea de hardware durante la creación de una tarea de copia de seguridad. Si se selecciona la instantánea de hardware, Arcserve UDP intenta crear una instantánea de hardware en primer lugar. Si se produce un error en la instantánea de hardware, Arcserve UDP volverá automáticamente a la instantánea de software sin que se produzca un error en la tarea de copia de seguridad.

Se puede utilizar la instantánea de hardware para copias de seguridad basadas en el agente (equipos físicos de Windows) y copias de seguridad sin agente basadas en el host (VMware y Hyper-V).

Matrices de almacenamiento compatibles:

- **Matriz de almacenamiento de NetApp:** Arcserve UDP es compatible con la instantánea de hardware para copias de seguridad basadas en el agente (equipos físicos de Windows) y copias de seguridad sin agente basadas en el host (VMware y Hyper-V).
- **Matriz de almacenamiento de Nimble:** Arcserve UDP es compatible con la instantánea de hardware para copias de seguridad basadas en el agente (equipos físicos de Windows) y copias de seguridad sin agente basadas en el host (VMware y Hyper-V).
- **Matriz de almacenamiento de HPE 3PAR:** Arcserve UDP es compatible con la instantánea de hardware para copias de seguridad basadas en el agente (equipos físicos de Windows) y copias de seguridad sin agente basadas en el host (VMware y Hyper-V).
- **Matriz de almacenamiento de Dell EMC Unity VSA:** Arcserve UDP es compatible con la instantánea de hardware para copias de seguridad basadas en el agente (equipos físicos de Windows) y copias de seguridad sin agente basadas en el host (Hyper-V).

Qué hacer a continuación

- Utilización de la instantánea de hardware para la copia de seguridad sin agente de VMware
- Utilización de la instantánea de hardware para la copia de seguridad sin agente de Hyper-V
- Utilización de la instantánea de hardware para la copia de seguridad basada en el agente

- Verificación del uso de la instantánea de hardware por parte de la copia de seguridad

Utilización de la instantánea de hardware para la copia de seguridad sin agente de VMware

Siga estos pasos:

1. Compruebe si se cumplen los siguientes requisitos previos:

   Para la instantánea de NetApp

   - ARCserve UDP es compatible con los LUN de NetApp iSCSI//FC y con las exportaciones de volúmenes de NetApp NFS que están configurados como almacenes de datos. iSCSI, FC y NFS deben cumplir ciertas condiciones para utilizar la instantánea de hardware.

     Consideraciones para la compatibilidad de NetApp iSCSI/FC con VMware

     Consideraciones para la compatibilidad de NFS con VMware

   - Para crear una instantánea de hardware para VMware, agregue la matriz de almacenamiento a la Consola. Para obtener más información sobre cómo agregar una matriz de almacenamiento, consulte Agregar una matriz de almacenamiento.
   - Para utilizar la instantánea de hardware, se recomienda una licencia de FlexClone para las matrices de almacenamiento de NetApp que se ejecutan con Data ONTAP en 7-Mode y modo de clúster.

   Nota: Para obtener más información sobre la configuración de NetApp, consulte la documentación de NetApp o póngase en contacto con el equipo de soporte de NetApp.

   Instantánea de hardware de HPE 3PAR:

   - Para admitir la instantánea de hardware de la máquina virtual de VMware, HP RMC debe gestionar la matriz de almacenamiento de HPE 3PAR.
   - La matriz de almacenamiento debe tener la licencia de copia virtual.

     Protocolos compatibles para la instantánea de hardware de VMware: FC e iSCSI
   - Para crear una instantánea de hardware para VMware, agregue la matriz de almacenamiento a la Consola. Para obtener más información sobre cómo agregar una matriz de almacenamiento, consulte Agregar una matriz de almacenamiento.

   Instantánea de hardware de Nimble:

- Protocolos compatibles para la instantánea de hardware de VMware: FC e iSCSI
- Para crear una instantánea de hardware para VMware, agregue la matriz de almacenamiento a la Consola. Para obtener más información sobre cómo agregar una matriz de almacenamiento, consulte Agregar una matriz de almacenamiento

  Consideraciones sobre el almacenamiento de Nimble cuando la autenticación CHAP está activada

2. Inicie sesión en la Consola y cree un plan para la copia de seguridad.

   Nota: Para obtener más información sobre cómo crear un plan de copia de seguridad sin agente, consulte Cómo crear un plan de copia de seguridad sin agente basado en el host.

3. Compruebe que se ha seleccionado la opción **Utilizar instantánea de hardware siempre que sea posible** en la ficha **Opciones avanzadas**.

   Nota: Para ejecutar la copia de seguridad solo desde la instantánea de hardware (y no desde la instantánea de software), Arcserve UDP proporciona la siguiente clave de registro: *FallbackToSWSnapshot =0(dword)*

   Se puede aplicar esta clave de registro a un nodo específico, así como a todos los nodos.

   - Para aplicarla a un nodo específico, cree el registro en HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\(Nodeid)

     Nota: (Nodeid) solo se crea después de una copia de seguridad.

   - Para aplicarla a todos los nodos, cree el registro en HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Importante: Si la subclave AFBackupDll no está disponible, se deberá agregar manualmente la subclave *AFBackupDll* en carpeta Engine como Engine\AFBackupDll\ y, a continuación, se deberá agregar *DWORD FallbackToSWSnapshot* en *AFBackupDll*.

4. **Guarde** el plan y **envíe** la tarea de copia de seguridad.

   La tarea de copia de seguridad se ejecuta utilizando la instantánea de hardware.

Consideraciones para la compatibilidad de NetApp iSCSI/FC con VMware

Arcserve UDP proporciona compatibilidad con las instantáneas de hardware para la máquina virtual de VMware solo cuando la matriz de almacenamiento subyacente es una matriz de almacenamiento de NetApp.

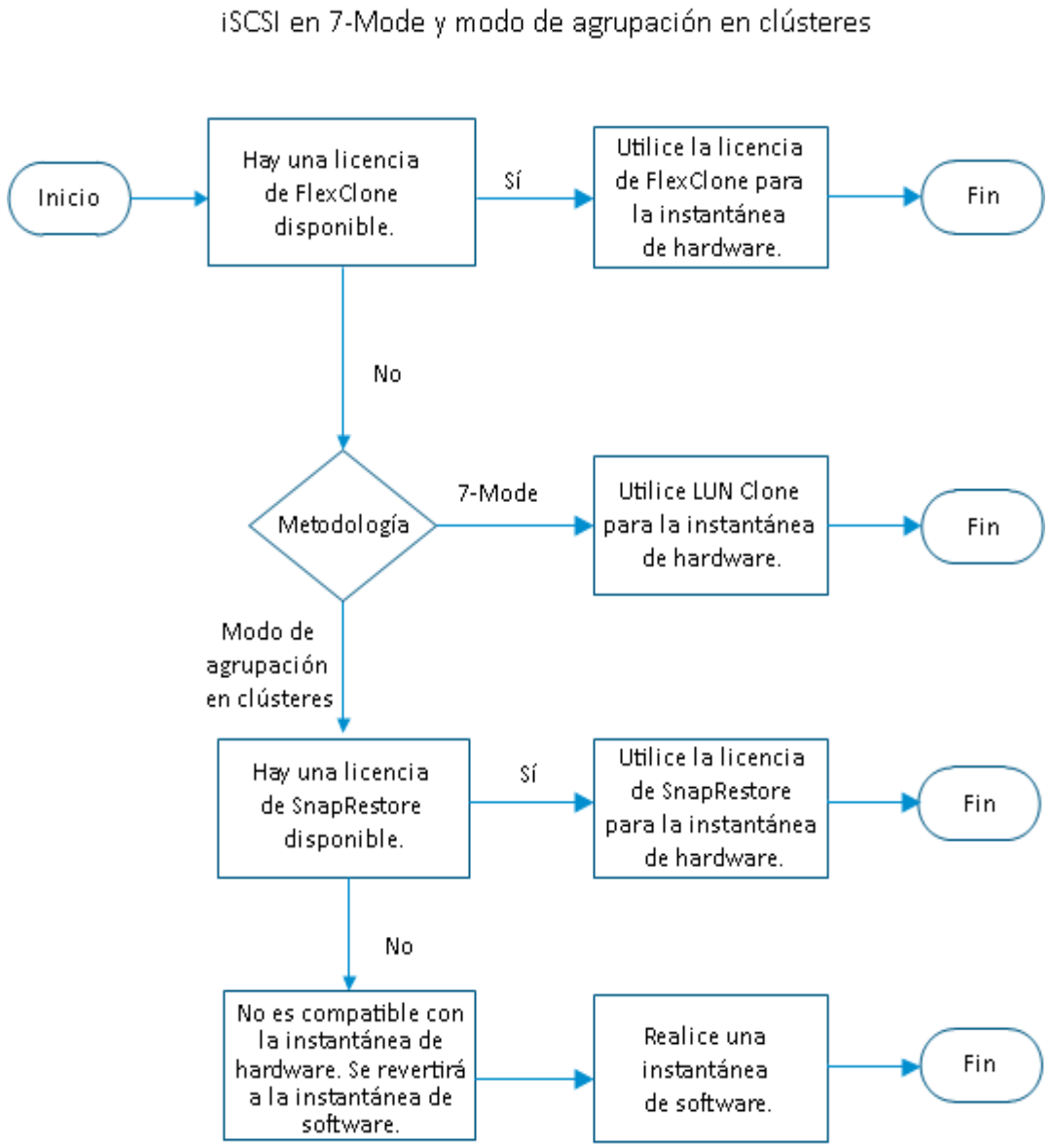
NetApp en 7-mode

Si el sistema de almacenamiento de NetApp se ejecuta en 7-mode, no es obligatorio instalar licencias adicionales para utilizar las instantáneas de hardware. Sin embargo, se recomienda disponer de la licencia de FlexClone instalada.

NetApp en modo de clúster

Si el sistema de almacenamiento de NetApp se ejecuta en el modo de clúster (C-mode), se debe tener la licencia de FlexClone o de SnapRestore instalada para utilizar las instantáneas de hardware.

En el siguiente diagrama de flujo se explican las condiciones que se aplican a la instantánea de hardware para NetApp iSCSI/FC VMware:



Limitación de un clon de LUN

En un clon de LUN tradicional, a veces no se puede suprimir la instantánea de la copia de seguridad durante las operaciones de limpieza. Por lo general, existe una LUN como un archivo en el sistema de archivos. De este modo, una instantánea captura el archivo. Cuando se crea un clon de LUN, se crea otro archivo en el sistema de archivos. De este modo, la siguiente instantánea captura el archivo original y el archivo duplicado. Cuando se capturan varias instantáneas, el clon de LUN se convierte en una parte de la cadena de instantáneas. Ahora, si se suprime una instantánea, la instantánea no se suprimirá debido a que se refiere a un clon de LUN del que, a su vez, otra instantánea ha realizado la copia de seguridad. En tales casos, no se puede suprimir un instantánea hasta que se suprime el clon de LUN y todas las instantáneas que hacen referencia a ese clon de LUN. Como resultado, la política de retención para las instantáneas programadas puede interrumpirse.

Para evitar esta situación, instale la licencia de FlexClone en el sistema de almacenamiento de NetApp y Arcserve UDP utilizará la tecnología de FlexClone para la clonación de LUN.

Claves de registro para SnapRestore

Cuando se utiliza la licencia de SnapRestore, la restauración de los LUN tarda más tiempo dependiendo del tamaño del LUN y del entorno. Esto se debe a que la supresión de una instantánea tarda más tiempo ya que la instantánea está ocupada restaurando el LUN, con lo que se tardará más tiempo. Arcserve UDP no dispone de un mecanismo para controlar el progreso de la restauración de los LUN. Por lo tanto, Arcserve UDP utiliza el mecanismo de reintentos para suprimir la instantánea.

Arcserve UDP proporciona dos claves de registro (**DeleteRetryTimeoutInMins** y **DeleteRetryCount**) que se pueden utilizar para mejorar el rendimiento de la supresión de instantáneas en función del tamaño del LUN y del entorno. Las claves de registro se encuentran en la ubicación siguiente:

SOFTWARE\Arcserve\Unified Data Protection\Engine

DeleteRetryTimeoutInMins

Especifica la duración del tiempo de espera (en minutos) para suprimir una instantánea. Si solo se dispone de SnapRestore y no se dispone de la licencia de FlexClone, es probable que la supresión de instantáneas lleve tiempo. Se puede utilizar la clave de registro para especificar los valores personalizados. Sin embargo, se recomienda utilizar la licencia de FlexClone.

Por ejemplo, si la duración del tiempo de espera es de dos minutos, el agente de UDP esperará dos minutos a que NetApp suprima la instantánea antes de enviar el comando de supresión a la matriz de almacenamiento de NetApp en su próximo reintento. Esta clave de registro se utiliza en combinación con la clave **DeleteRetryCount**.

Valor predeterminado: 1 (en minutos)

Tipo: REG_SZ

DeleteRetryCount

Especifica el número de reintentos necesarios para suprimir una instantánea.

Por ejemplo, si el número de reintentos es de cinco, el agente de UDP intentará cinco veces enviar el comando de supresión de instantáneas a la matriz de almacenamiento de NetApp. Después de intentar cinco veces enviar el comando de supresión de instantáneas, si la instantánea todavía existe se deberá suprimir manualmente la instantánea y, además, se deberá aumentar el número de reintentos en el valor adecuado para que la siguiente copia de

seguridad no tenga este problema. Esta clave de registro se utiliza en combinación con la clave **DeleteRetryTimeoutInMins**.

Valor predeterminado: 30

Tipo: REG_SZ

Claves de registro para desactivar la reserva de espacio de LUN

Cuando se realiza el clon de LUN durante la copia de seguridad utilizando la instantánea de hardware, la reserva de espacio de forma predeterminada se hereda desde el LUN de origen. Arcserve UDP proporciona una clave de registro que puede utilizar para desactivar la reserva de espacio. La clave de registro se encuentra en la ubicación siguiente:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

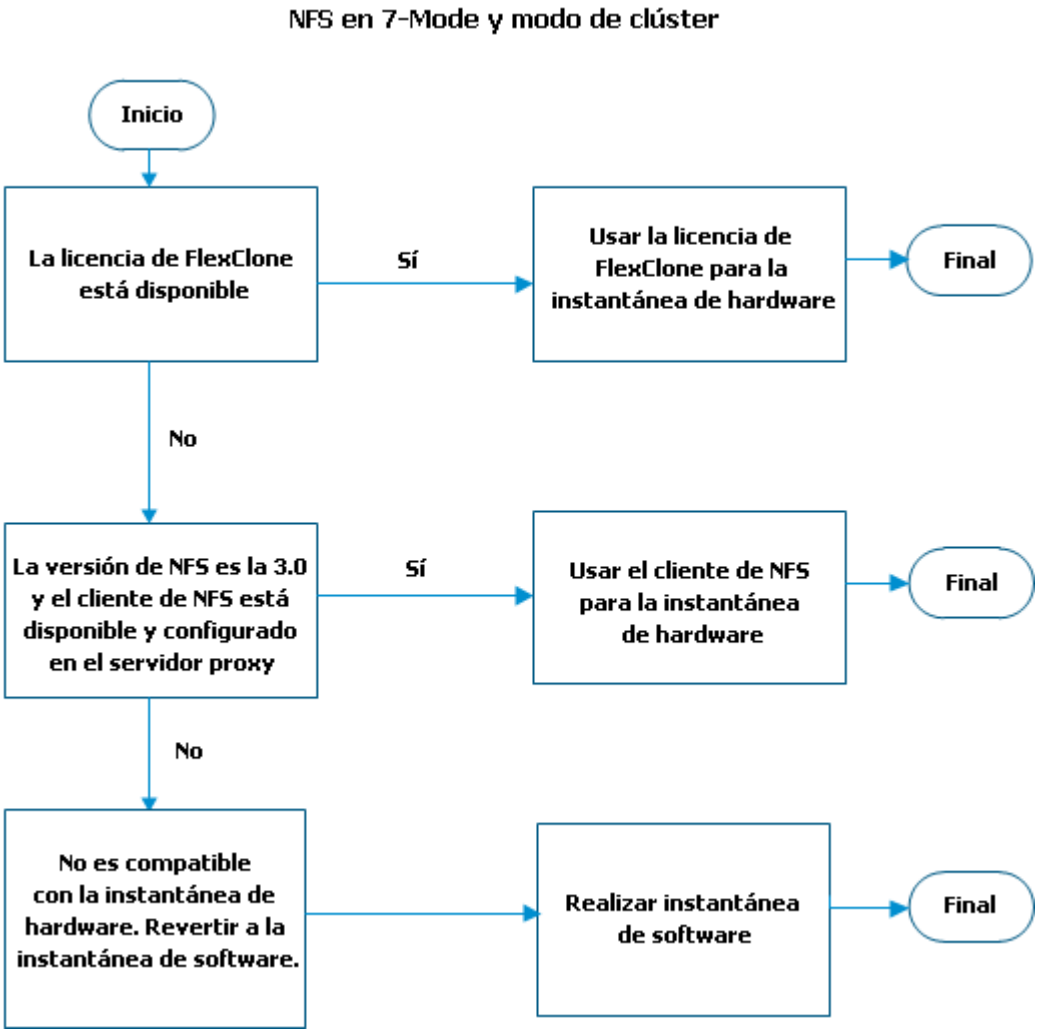
DisableLunSpaceReservation =1

Especifica que se han desactivado las reservas de espacio de LUN.

Nota: Esto solo es aplicable cuando se aplica la licencia de FlexClone.

Consideraciones para la compatibilidad de NFS con VMware

En el siguiente diagrama de flujo se explican las condiciones que se aplican a la instantánea de hardware para NetApp NFS en máquinas virtuales de VMware:



Arcserve UDP es compatible con la instantánea de hardware para los almacenes de datos de NFS versión 3.0. Para utilizar la instantánea de hardware, el proxy de copia de seguridad debe tener el cliente de NFS de Microsoft instalado y configurado.

En la siguiente tabla se muestran las versiones NFS que admiten la máquina virtual de VMware y Arcserve UDP. Asegúrese de que dispone de la versión correcta de NFS con la versión de VMware correspondiente.

Versiones de VMware	Versiones de NFS que admite VMware	Versiones de NFS que admite Arcserve UDP para la instantánea de hardware para FlexC-	Versiones de NFS que admite Arcserve UDP para la instantánea de hardware para el cliente de NFS de

		lone	Windows
VMware 6.0 y posteriores	Compatible con NFS 3.0 y 4.1	Compatible con NFS 3.0 y 4.1	Compatible solo con NFS 3.0 y debe cumplir los requisitos previos
Versiones de VMware posteriores a la 6.0	Compatible solo con NFS 3.0	Compatible con NFS 3.0	Compatible solo con NFS 3.0 y debe cumplir los requisitos previos

Requisito previo para NFS 3.0

- Si la licencia de FlexClone no está presente, para admitir la instantánea de hardware de archivos VMDK hospedados en un almacén de datos de NFS 3.0, el dispositivo de NetApp debe tener las siguientes versiones de ONTAP instaladas:
  - Se admiten todos los sistemas Data ONTAP 7-Mode.
  - Se admiten las versiones de Data ONTAP 8.2 en clúster, a partir de la 8.2.3. También se admiten las versiones de Data ONTAP 8.3 en clúster, a partir de la 8.3.1.
  - De forma predeterminada, la compatibilidad con el cliente de NFS versión 3 de Windows está desactivada. Para activarla en máquinas virtuales de almacenamiento (SVM), utilice el siguiente comando:

  vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled

- El proxy de copia de seguridad, que realiza copias de seguridad de la máquina virtual de VMware, debe tener el cliente de NFS de Microsoft instalado y configurado. El proxy de copia de seguridad debe tener acceso al recurso compartido de NFS. Para instalar manualmente el cliente de NFS en el servidor, consulte Cómo instalar manualmente el cliente de NFS de Microsoft en un servidor Windows.
- Deberá reiniciar el servicio de cliente de NFS de Microsoft en el servidor proxy después de implementar el plan de copia de seguridad sin agente. Se debe reiniciar el servicio solo la primera vez, ya que la implementación del plan activa algunos cambios con respecto al cliente de NFS en el servidor proxy.

Cómo instalar manualmente el cliente de NFS de Microsoft en un servidor Windows

Siga estos pasos para instalar manualmente el cliente de NFS de Microsoft en un servidor Windows.

1. Inicie sesión en el servidor Windows.
2. Abra el Administrador de servidores y haga clic en Administrar.
3. Haga clic en Agregar roles y funciones.
4. En el cuadro de diálogo Antes de empezar, haga clic en Siguiente.
5. En el cuadro de diálogo Seleccionar tipo de instalación, seleccione Instalación basada en características o en roles y, a continuación, haga clic en Siguiente.
6. En el cuadro de diálogo Seleccionar servidor de destino, si está realizando la instalación en el servidor local, haga clic en Siguiente. En caso contrario, seleccione un servidor de la lista Grupo de servidores.
7. En el cuadro de diálogo Seleccionar roles de servidor,haga clic en Siguiente.
8. En el cuadro de diálogo Seleccionar características, desplácese por la lista de características disponibles y seleccione la casilla de verificación Cliente para NFS.
9. Haga clic en Siguiente.
10. En el cuadro de diálogo Confirmar selecciones de instalación, revise las selecciones y haga clic en Instalar.
11. Una vez finalizada la instalación, consulte los resultados y haga clic en Cerrar.

Consideraciones sobre el almacenamiento de Nimble cuando la autenticación CHAP está activada

Se pueden realizar copias de seguridad de la instantánea de hardware cuando el almacenamiento de Nimble tenga activada la autenticación CHAP.

Nota: La autenticación CHAP no es compatible con ESXi 5.0 debido a que la versión de ESXi no tiene SQLite.

Se deberán completar los siguientes requisitos previos:

Requisitos previos

Importante: Solo se aplican los requisitos previos si se desea que la tarea de copia de seguridad sin agente basada en el host utilice SAN como el modo de transporte.

- Active SSH en ESXi donde esté configurado el almacenamiento de Nimble con la autenticación CHAP.
- Compruebe si el equipo proxy dispone de la interfaz de línea de comandos iscsicli necesaria para configurar los dispositivos de destino iSCSI.
- Establezca la política de ejecución en RemoteSigned en el equipo proxy para ejecutar los scripts de PowerShell. Utilice el siguiente comando:

  Set-ExecutionPolicy RemoteSigned
- Guarde las credenciales de ESXi mediante un script de PowerShell para el que se ha configurado el almacenamiento de Nimble con la autenticación CHAP.

  Siga estos pasos para guardar las credenciales de ESXi:

  - Ejecute el script de PowerShell "StoreESXCredentials.ps1" en el servidor proxy.

    Se le pedirá introducir detalles sobre la dirección IP, el nombre de usuario y la contraseña.
  - Introduzca los tres parámetros.

    Las credenciales se almacenan en un archivo CSV llamado ESXCredentials.csv y la contraseña está cifrada.

  Para buscar el script de PowerShell, realice los siguientes pasos:

  - Inicie sesión en el equipo proxy y abra PowerShell.
  - Vaya al siguiente directorio:

    Nota: La ruta cambia en función del directorio de instalación.

    C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN

- Ejecute el script de PowerShell tal y como se indica a continuación:

  PS C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN> .\StoreESXCredentials.ps1

Utilización de la instantánea de hardware para la copia de seguridad sin agente de Hyper-V

Importante: La copia de seguridad sin agente de Hyper-V utiliza la instantánea de hardware solo cuando todos los discos de la máquina virtual se encuentran en volúmenes compatibles con la instantánea de hardware. De lo contrario, la copia de seguridad utiliza la instantánea de software.

Siga estos pasos:

1. Compruebe si se cumplen los siguientes requisitos previos.
   - Instale un proveedor de hardware VSS (por ejemplo, NetApp) en los servidores de Hyper-V. Para admitir la instantánea transportable, instale el proveedor de hardware de VSS en el servidor proxy de la copia de seguridad. Una configuración habitual de un proveedor de hardware VSS incluye:
     - Especificación de un servidor que controle el LUN
     - Especificación de las credenciales de la matriz de discos para acceder a la matriz de discos

     Nota: Para obtener más información sobre cómo configurar el proveedor de hardware VSS, póngase en contacto con el distribuidor del hardware.
   - El servidor Hyper-V y el servidor proxy deben tener una versión del sistema operativo similar.
   - Si el servidor Hyper-V pertenece a un clúster, el servidor proxy no debe formar parte del clúster de Hyper-V.
2. Inicie sesión en la Consola y cree un plan para la copia de seguridad.

   Nota: Para obtener más información sobre cómo crear un plan de copia de seguridad sin agente, consulte Cómo crear un plan de copia de seguridad sin agente basado en el host.
3. Compruebe que se ha seleccionado la opción **Utilizar instantánea de hardware siempre que sea posible** en la ficha **Opciones avanzadas**.

   Nota: Para ejecutar la copia de seguridad solo desde la instantánea de hardware (y no desde la instantánea de software), Arcserve UDP proporciona la siguiente clave de registro: *FallbackToSWSnapshot =0(dword)*

   Se puede aplicar esta clave de registro a un nodo específico, así como a todos los nodos.
   - Para aplicarla a un nodo específico, cree el registro en HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data

Protection\Engine\AFBackupDll\(Nodeid)

Nota: (Nodeid) solo se crea después de una copia de seguridad.

- Para aplicarla a todos los nodos, cree el registro en HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

Importante: Si la subclave AFBackupDll no está disponible, se deberá agregar manualmente la subclave *AFBackupDll* en carpeta Engine como Engine\AFBackupDll\ y, a continuación, se deberá agregar *DWORD FallbackToSWSnapshot* en *AFBackupDll*.

4. **Guarde** el plan y **envíe** la tarea de copia de seguridad.

   La tarea de copia de seguridad se ejecuta utilizando la instantánea de almacenamiento.

Utilización de la instantánea de hardware para la copia de seguridad basada en el agente

Siga estos pasos:

1. Compruebe si se cumplen los siguientes requisitos previos:

   - Instale a un proveedor de hardware VSS compatible con la instantánea de hardware en los Agentes de Arcserve UDP. Una configuración habitual de un proveedor de hardware VSS incluye:

     - Especificación de un servidor que controle el LUN.
     - Especificación de las credenciales de la matriz de discos para acceder a la matriz de discos.

     Nota: Para obtener más información sobre cómo configurar el proveedor de hardware VSS, póngase en contacto con el distribuidor del hardware.

2. Inicie sesión en la Consola y cree un plan para la copia de seguridad.

   Nota: Para obtener más información sobre cómo crear un plan basado en agente para Windows, consulte Cómo crear un plan de copia de seguridad en Windows.

3. Compruebe que se ha seleccionado la opción **Utilizar instantánea de hardware siempre que sea posible** en la ficha **Opciones avanzadas**.

4. Guarde el plan y envíe la tarea de copia de seguridad.

   La tarea de copia de seguridad se ejecuta utilizando la instantánea de alma-cenamiento.

Verificación del uso de la instantánea de hardware por parte de la copia de seguridad

Si no se cumplen los requisitos previos para una instantánea de hardware, Arcserve UDP cambiará automáticamente a una instantánea de software sin producir un error en la tarea de copia de seguridad. Si se produce un error en la instantánea de hardware, el evento se registra en los registros de actividad.

Revise los mensajes de registro para asegurarse de que la copia de seguridad ha utilizado la instantánea de hardware.

Siga estos pasos:

1. Vaya a la ruta siguiente:

   <Carpeta de instalación>\Arcserve\Unified Data Protection\Engine\Logs

2. Abra el archivo correspondiente al ID de tarea respectivo.

   Por ejemplo, si el ID de tarea es JW002, vaya a la carpeta **Logs** y abra el archivo JW002.

3. Revise los mensajes en el archivo para confirmar si la copia de seguridad ha utilizado la instantánea de almacenamiento.

   La instantánea de almacenamiento para una copia de seguridad se ha utilizado correctamente.

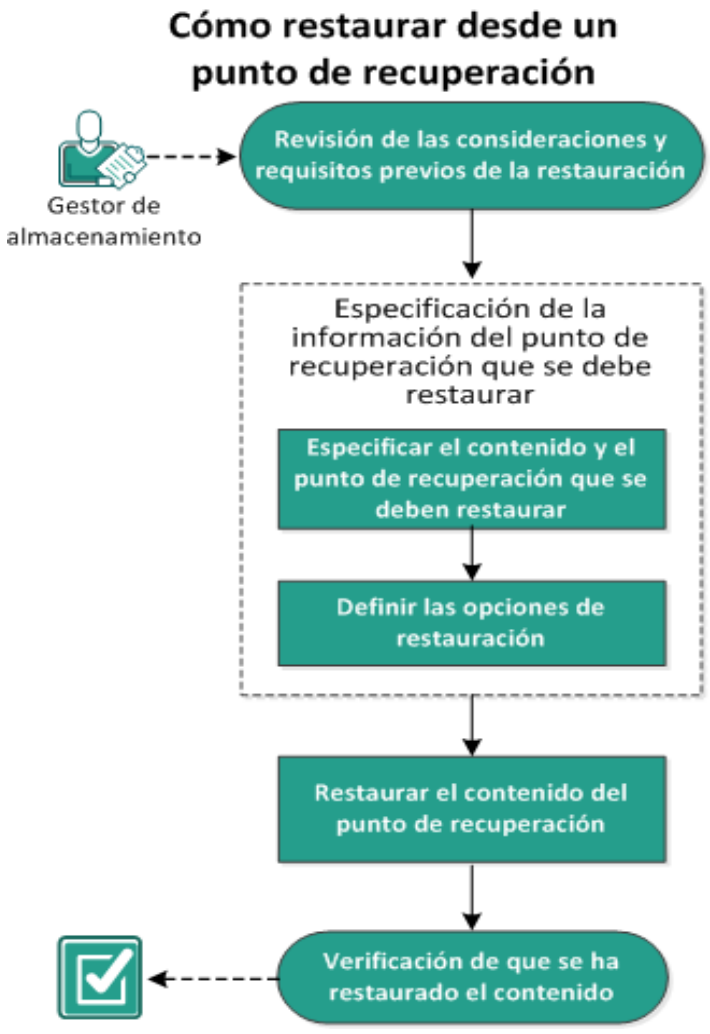
Capítulo 13: Restauración de datos protegidos

Esta sección incluye los siguientes temas:

Cómo restaurar desde un punto de recuperación

Cada vez que Arcserve UDP realiza una copia de seguridad correcta, se crea una imagen de instantánea en un momento dado de la copia de seguridad (punto de recuperación). La recopilación de puntos de recuperación permite ubicar y especificar exactamente la imagen de copia de seguridad que desea restaurar. Si más tarde sospecha que falta información sobre la copia de seguridad realizada, bien que se ha corrompido o que no es fiable, se podrá buscar y restaurar desde una versión correcta anterior ya conocida.

El diagrama siguiente muestra el proceso para restaurar desde un punto de recuperación:



Realice las tareas siguientes para restaurar desde un punto de recuperación:

1. Revisión de las consideraciones y requisitos previos de la restauración
2. Especificación de la información del punto de recuperación que se debe restaurar

   a. Especificación del contenido y del punto de recuperación que se debe restaurar
   b. Definición de las opciones de restauración
3. Restauración del contenido del punto de recuperación
4. Verificación de que se ha restaurado el contenido

Revisión de las consideraciones y requisitos previos de la restauración

Verifique que los requisitos previos siguientes existen antes de realizar una restauración:

- Como mínimo, existe un punto de recuperación disponible para restaurar.
- Tiene un destino del punto de recuperación válido y accesible desde el que poder restaurar el contenido del punto de recuperación.
- Tiene una ubicación de destino válida y accesible a la que poder restaurar el contenido del punto de recuperación.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones sobre la restauración:

- Si la restauración se debe realizar en un destino remoto y si todas las letras de unidad de disco (de la A a la Z) están ocupadas, la restauración a una ruta remota no se realizará correctamente. El Agente de Arcserve UDP (Windows) debe utilizar una letra de unidad de disco para montar la ruta de destino remota.
- (Opcional) Debe entender cómo funciona el proceso de restauración. Para obtener más información, consulte Cómo funciona la restauración de nivel de archivo.
- (Opcional) Revise los archivos que se han omitido durante la restauración. Para obtener más información, consulte Archivos omitidos durante la restauración.
- Cuando se intenta restaurar una sesión de copia de seguridad optimizada en un volumen no vacío (restauración no optimizada), la tarea de restauración puede tardar más tiempo que la hora estimada que aparece en el controlador de tareas. La cantidad de datos que se procesa y el tiempo transcurrido puede aumentar en función de los datos que se optimizan en el volumen.

Ejemplo:

El tamaño del volumen de la copia de seguridad es de 100 GB y después de la optimización el tamaño del volumen se reduce a 50 GB.

Cuando se realiza una restauración no optimizada de este volumen, el controlador de tareas de restauración muestra 100% después de haber restaurado 50 GB, pero llevará más tiempo restaurar los 100 GB.

- El mensaje de registro de actividades siguiente se mostrará al restaurar los archivos del sistema:

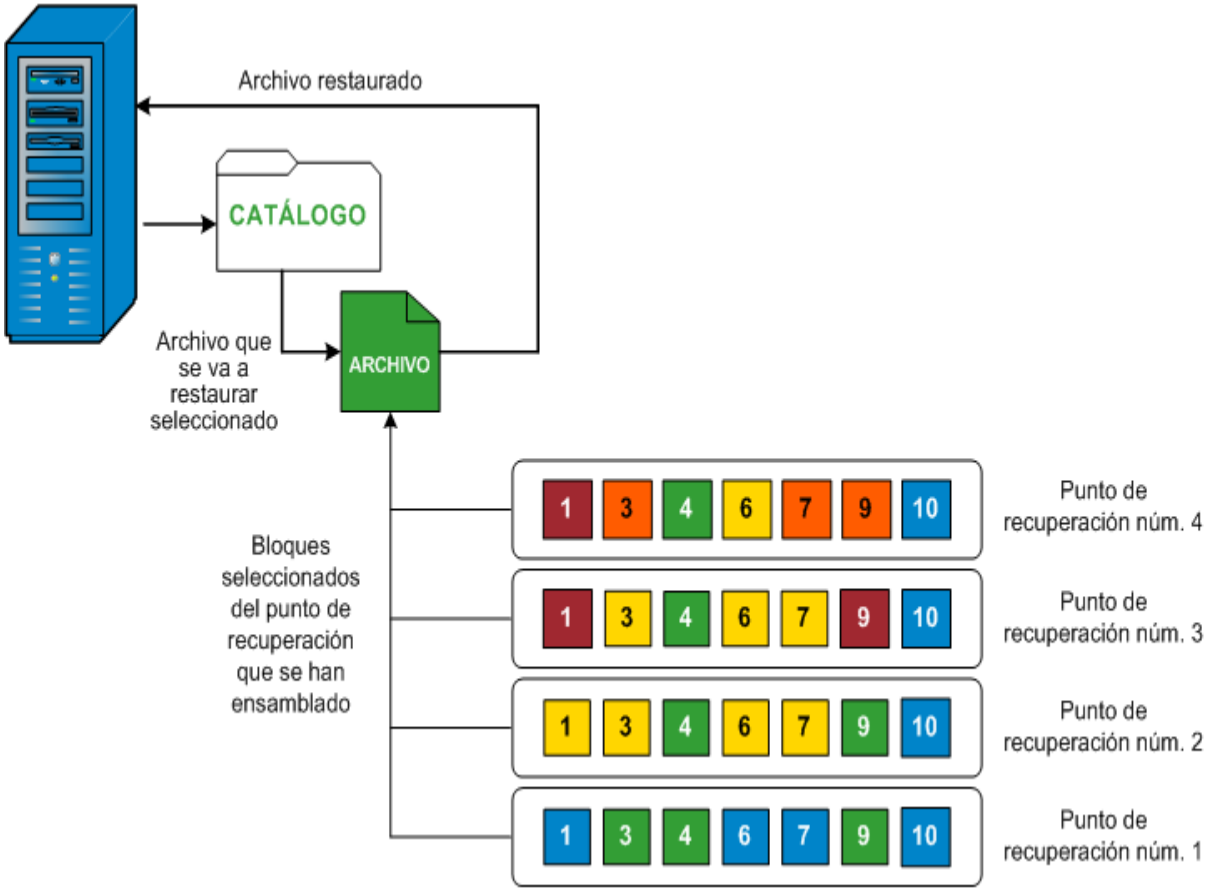
  Se han omitido los archivos del sistema. En caso necesario, se puede utilizar la opción Reconstrucción completa (BMR) para restaurarlos.

Cómo funciona la restauración de nivel de archivo

Durante una copia de seguridad de nivel de bloque, cada archivo con copia de seguridad está compuesto por una recopilación de bloques que definen el archivo en particular. Además, un archivo de catálogo también se crea de forma que contiene una lista de los archivos con copia de seguridad, junto con los bloques individuales que se han utilizado para cada archivo y los puntos de recuperación disponibles para los archivos. Si necesita restaurar un archivo en particular, puede buscar la copia de seguridad y seleccionar el archivo que desea restaurar y el punto de recuperación desde el cual desea empezar a restaurar. A continuación, Arcserve UDP recopilará la versión de los bloques que se han utilizado para el punto de recuperación del archivo especificado, volverá a unir el archivo y lo restaurará.

Nota: Se puede realizar también una restauración sin un archivo de catálogo desde un punto de recuperación de copia de seguridad sin catálogo.

El diagrama de flujo siguiente muestra el proceso de cómo Arcserve UDP restaura un archivo específico:



Archivos omitidos durante la restauración

Mientras el Agente de Arcserve UDP (Windows) realiza una restauración, algunos archivos se pueden omitir intencionadamente.

Se omiten los archivos y las carpetas en la tabla siguiente durante una restauración si se dan las dos condiciones siguientes:

- Se omiten archivos cuando existen tales archivos antes de la restauración y la opción de conflicto es Omitir archivos existentes.
- Se omiten archivos y carpetas que aparecen en la tabla siguiente porque no son un componente importante para Windows o para el Agente de Arcserve UDP (Windows).

SO	Carpeta o ubicación	Nombre del archivo o de la carpeta	Observaciones
Todo	Carpeta Root de cada volumen	CAVolTrc.dat	Utilizado por el controlador de seguimiento de Arcserve UDP.
		cavoltrcsnapshot.dat	
		Información acerca del volumen del sistema*	Utilizado para guardar archivos/carpetas por un sistema Windows, por ejemplo, archivos de instantánea de volumen.
		RECYCLER*	Utilizado solamente en particiones de NTFS. Contiene una papelera de reciclaje para todos los usuarios que se conecten al equipo, que se ordenarán en función del identificador de seguridad (SID).
		$Recycle.Bin*	Cuando se suprime un archivo en el explorador de Windows NT o Mi PC, el archivo se almacena en la Papelera de reciclaje hasta que se vacíe la Papelera de reciclaje o se restaure el archivo.
	Cualquier carpeta puede contener archivos de imagen	Thumbs.db	Almacena pequeñas imágenes para la vista en miniatura del Explorador de Windows.
	Carpeta Root del volumen	PageFile.sys	El archivo de intercambio de memoria virtual de Windows.
		Hiberfil.sys	Se trata del archivo de hibernación, que se utiliza para guardar los datos del sistema cuando un equipo se establece en el modo de hibernación.

Se omiten los archivos y las carpetas siguientes solamente cuando se restaura en la ubicación original o en otra ubicación:

SO	Carpeta o ubicación	Nombre del	Observaciones

		archivo o de la carpeta	
Todo	Carpeta especificada en el registro de valor que se encuentra en: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Todos los archivos/carpetas (recursivamente)	La carpeta contiene un archivo dll en memoria caché que se utiliza para el Comprobador de archivos de sistema (SFC) y el contenido del directorio dll en memoria caché del sistema se reconstruye mediante SFC.
	%SystemRoot%\SYSTEM32\dllCache		
	Carpeta Root de quorum_device	MSCS*	Utilizado para Microsoft Cluster Server.
	%SystemRoot%\SYSTEM32\	perf?00?.dat	Los datos de rendimiento utilizados por el contador de rendimiento de Windows.
		perf?00?.bak	
		CATROOT*	Utilizado para las firmas digitales de registros de la protección de archivos de Windows (WFP) del sistema operativo instala archivos como DLL, EXE, SYS, OCX, etc. para evitar y proteger su supresión o sustitución por versiones anteriores.
	%SystemRoot%\inetsrv\	metabase.bin	El archivo binario metabase de las versiones de IIS anteriores a 6.0.
	Archivo o carpeta especificados en el valor excepto almacenamiento común de SIS en	Todos los archivos/carpetas	No se debe realizar copia de

	HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup	(recursivamente)	seguridad ni acciones de restauración para archivos y/o carpetas. Para obtener más información, consulte este vínculo.
XP W2003	Volumen del sistema	NTLDR	El cargador de arranque principal.
		BOOT.INI	Contiene la configuración de arranque (si esta falta, NTLDR establecerá \Windows como predeterminado en la primera partición de la primera unidad de disco duro).
		NTDETECT.COM	Necesario para iniciar un sistema operativo de NT. Detecta información de hardware básica que es necesaria para un arranque correcto.
Vista y posteriores	Carpeta Root del volumen del sistema	boot*	Carpeta Boot para Windows.
		bootmgr	Archivo del gestor de arranque de Windows.
		EFI\Microsoft\Boot*	Utilizado para el arranque de EFI.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Almacena los archivos de seguimiento de ETW (extensión .etl) para las sesiones de seguimiento

			de eventos en tiempo real.
		config\RegBack*	Copia de seguridad de la tabla de registro actual.
Win8 y posteriores	Volumen del sistema	swapfile.sys	El archivo de controlador del sistema, normalmente alrededor de 256 MB. Utilizado por las aplicaciones de estilo Metro que no se ajustan a las características de paginación tradicionales (como patrón de uso, crecimiento, reserva de espacio) de pagefile.sys.
		BOOTNXT	Utilizado para iniciar el sistema operativo, distinto de Windows 8. Creado para activar las opciones de inicio y actualizado por Windows.

El registro de actividad proporciona la siguiente información:

- Información sobre la hora y la fecha: se omiten los archivos del sistema jobxxxx. Se puede utilizar la opción de recuperación completa (BMR) para restaurarlos.
- Información sobre la hora y la fecha: se omiten los archivos o directorios jobxxxx. Los archivos y directorios omitidos están disponibles en C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\Logs\Restore-<AAAAMMDD>-<hhmmss>-<ID del proceso>-<ID de la tarea>.log.

Especificación de la información del punto de recuperación que se debe restaurar

Arcserve UDP proporciona una opción para restaurar datos desde un punto de recuperación. El objetivo de ejecutar una tarea de restauración correcta es de identificar los datos necesarios de forma rápida y de recuperarlos desde la ubicación de copia de seguridad correspondiente. Cada tarea de restauración necesita un origen y un destino.

El proceso de restauración desde un punto de recuperación se muestra a continuación:

1. Especificación del contenido y del punto de recuperación que se debe restaurar
2. Definición de las opciones de restauración

Especificación del contenido y del punto de recuperación que se debe restaurar

Esta sección proporciona información sobre cómo especificar el punto de recuperación y el contenido para restaurar.

Siga estos pasos:

1. Acceda al cuadro de diálogo Selección del método de recuperación de una de las formas siguientes:

   En la Consola de Arcserve UDP:

   a. Inicie sesión en la Consola de Arcserve UDP.

   b. Vaya a **recursos** > **Nodo** > **Todos los nodos**.

      Se muestran todos los nodos de agregados en el panel central.

   c. Haga clic con el botón secundario del ratón en el nodo y, a continuación, haga clic en **Restaurar**.

      Se inicia sesión automáticamente en la consola del nodo del agente y se abre el cuadro de diálogo Restaurar.

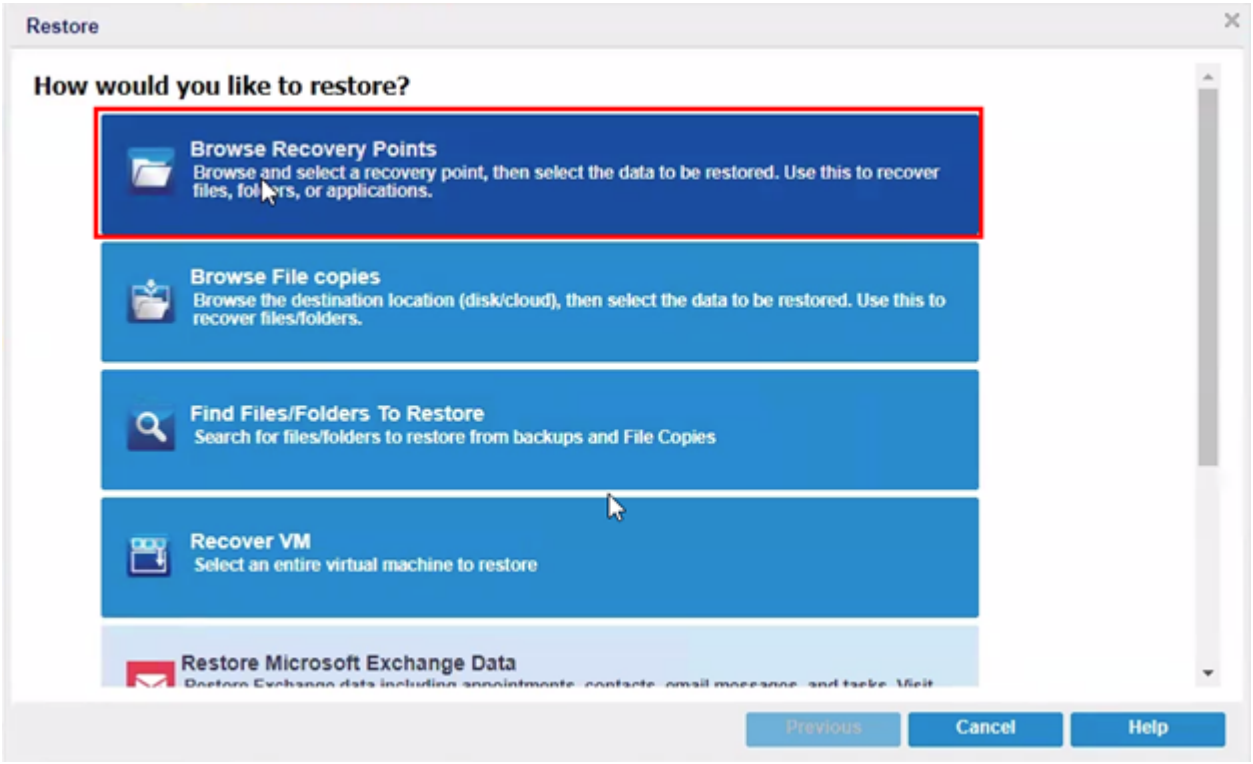
   Desde el Agente de Arcserve UDP (Windows):

   a. Inicie sesión en el Agente de Arcserve UDP (Windows).

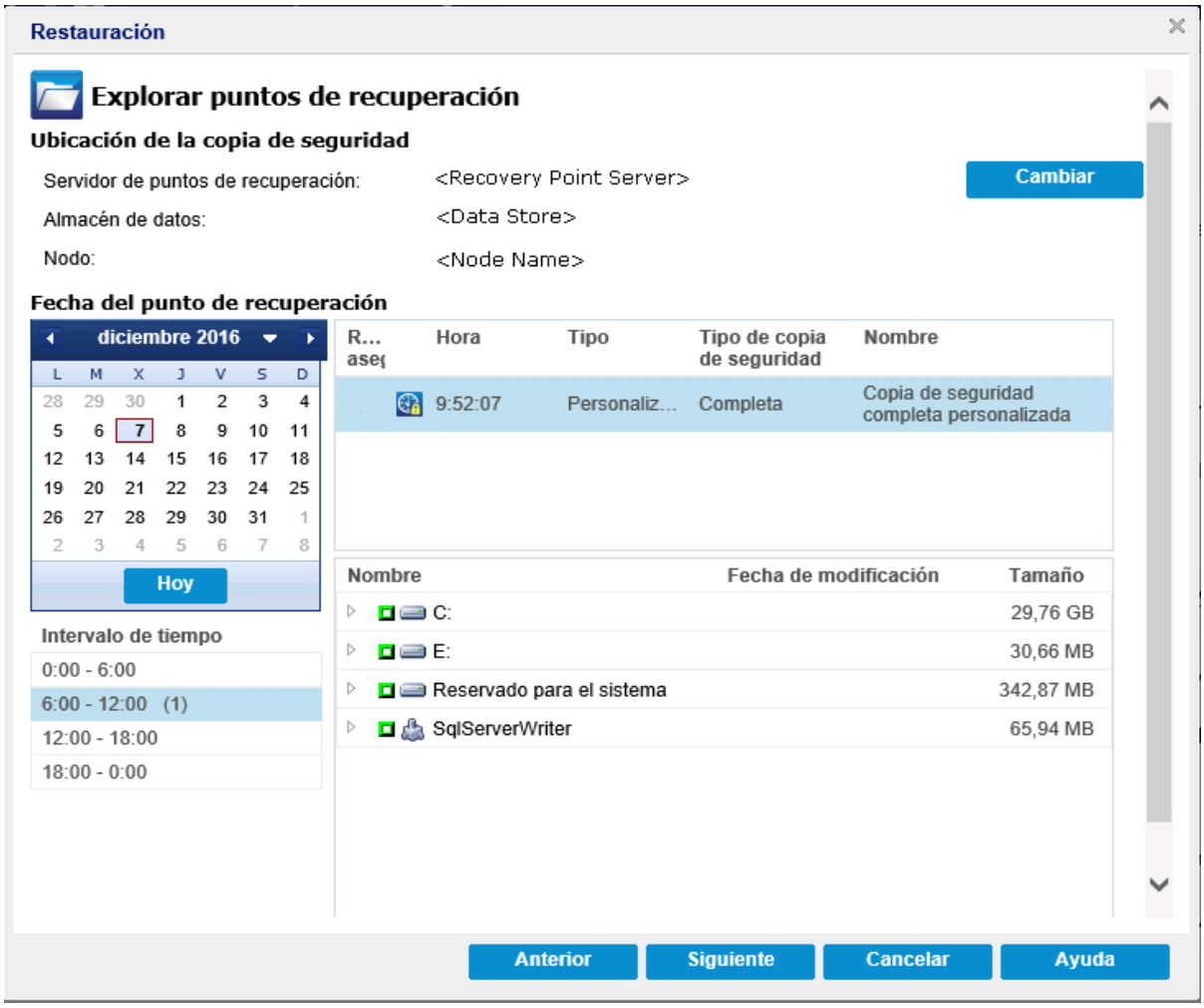
   b. En la página principal, seleccione **Restaurar**.

      Se abrirá el cuadro de diálogo Restauración.

2. En el cuadro de diálogo Restaurar haga clic en la opción **Explorar puntos de recuperación**.



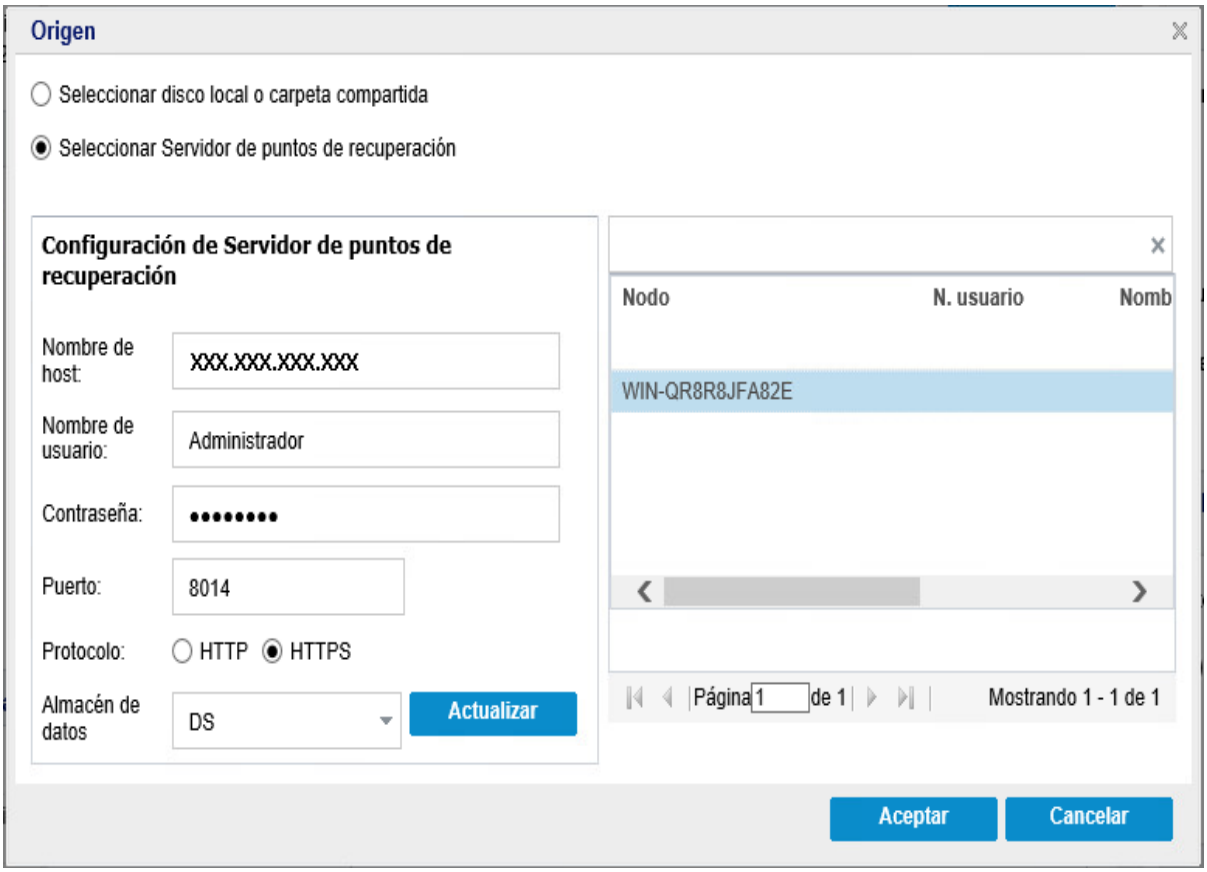
3. En la página Explorar puntos de recuperación, haga lo siguiente:



a. Para actualizar la ubicación de la copia de seguridad, haga clic en **Cambiar**.

   Se abrirá el cuadro de diálogo Origen.

b. En el cuadro de diálogo Origen, seleccione una de las siguientes ubicaciones de copia de seguridad y, a continuación, haga clic en **Aceptar**:



Seleccionar disco local o carpeta compartida

1. Especifique o vaya a la ubicación donde se almacenan las imágenes de copia de seguridad y seleccione el origen de la copia de seguridad adecuado.
2. Para verificar la conexión a la ubicación especificada, haga clic en el botón de flecha verde. Si es necesario, especifique el Nombre de usuario y la Contraseña para acceder a dicha ubicación de origen.

   El cuadro de diálogo Selección de la ubicación de la copia de seguridad se abre.
3. Seleccione la carpeta en la cual se almacenan los puntos de recuperación y, a continuación, haga clic en **Aceptar**.

   El cuadro de diálogo Selección de la ubicación de la copia de seguridad se cierra y se muestra la ubicación de la copia de seguridad en el cuadro de diálogo Origen.

   Los puntos de recuperación se clasifican en el cuadro de diálogo Examinar puntos de recuperación.

Seleccionar servidor de puntos de recuperación

1. Especifique los detalles del valor de configuración del servidor de puntos de recuperación y, a continuación, haga clic en **Actualizar**.

   Todos los agentes se muestran en la columna Agente de protección de datos en el cuadro de diálogo Origen.

2. Seleccione el agente de la lista que se muestra.

   Los puntos de recuperación se clasifican en el cuadro de diálogo Examinar puntos de recuperación.

c. Seleccione la fecha de calendario para la imagen de copia de seguridad que se desea restaurar.

   Todas las fechas que contienen puntos de recuperación para el origen de la copia de seguridad especificado se resaltan en verde.

   Aparecerán los puntos de recuperación correspondientes para la fecha, junto con la hora de la copia de seguridad, el tipo de copia de seguridad que se realiza (completa, incremental o de verificación) y el nombre de la copia de seguridad.

d. Seleccione un punto de recuperación para restaurar.

   Se muestra el contenido de la copia de seguridad (incluyendo cualquier aplicación) del punto de recuperación seleccionado.

   Nota: Si un icono de reloj aparece con el símbolo de candado, significa que el punto de recuperación contiene información cifrada y que puede requerir una contraseña para realizar la restauración.

e. Seleccione el contenido que desee restaurar.

   - Para la restauración de nivel de volumen, es posible especificar la restauración del volumen entero o de los archivos o carpetas seleccionados integrados en el volumen.
   - Para la restauración de nivel de aplicaciones, tiene la opción de especificar la restauración de la aplicación entera o de los componentes seleccionados, las bases de datos, las instancias, etcétera, integrados en la aplicación.

4. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo Opciones de restauración.

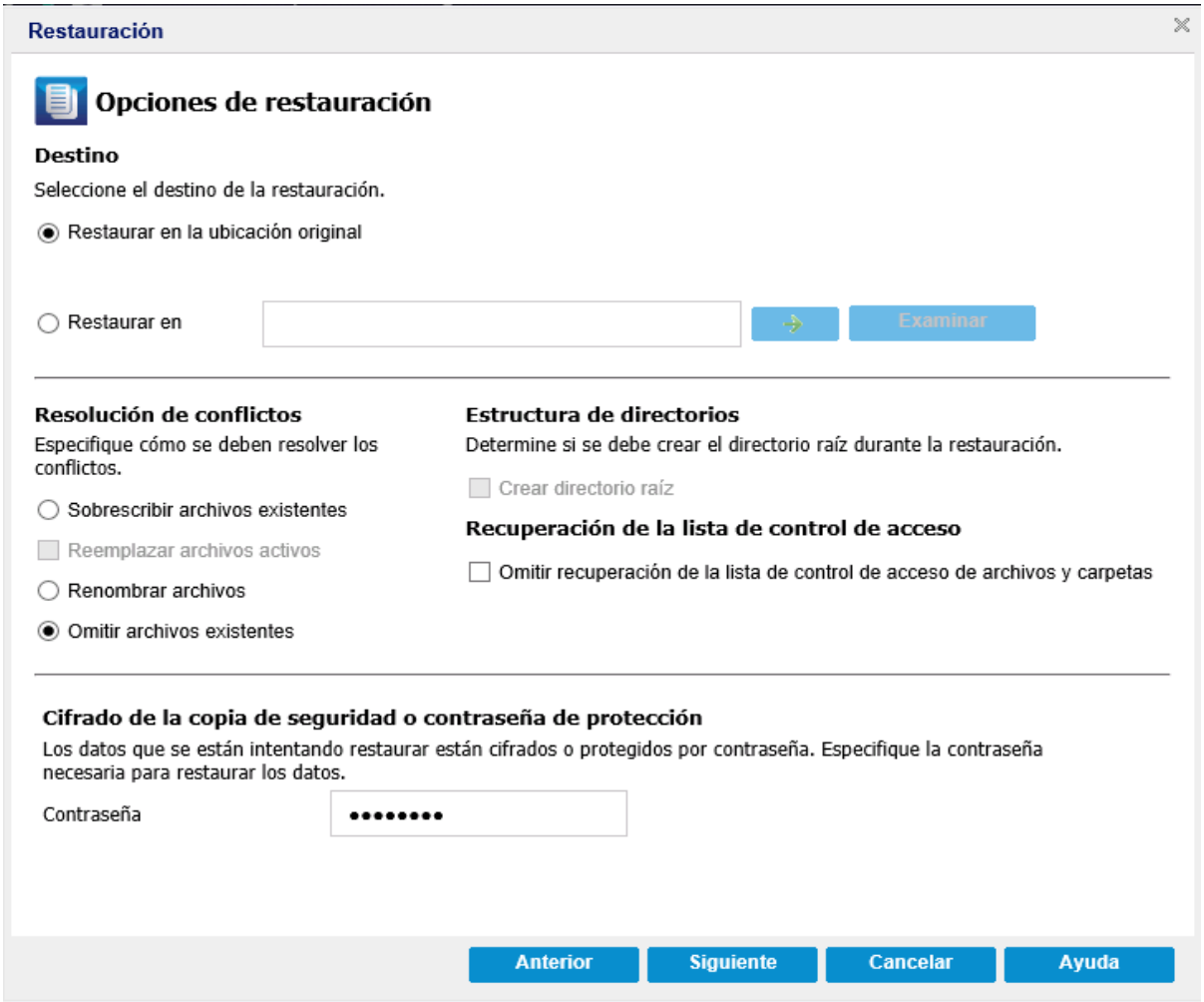
   Se especifica el punto de recuperación y el contenido que se debe restaurar.

Definición de las opciones de restauración

Después de especificar un punto de recuperación y el contenido que se deben restaurar, defina las opciones de copia para el punto de recuperación seleccionado. Esta sección explica cómo definir las opciones de restauración para el punto de recuperación seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo Opciones de restauración, seleccione el destino para la restauración.



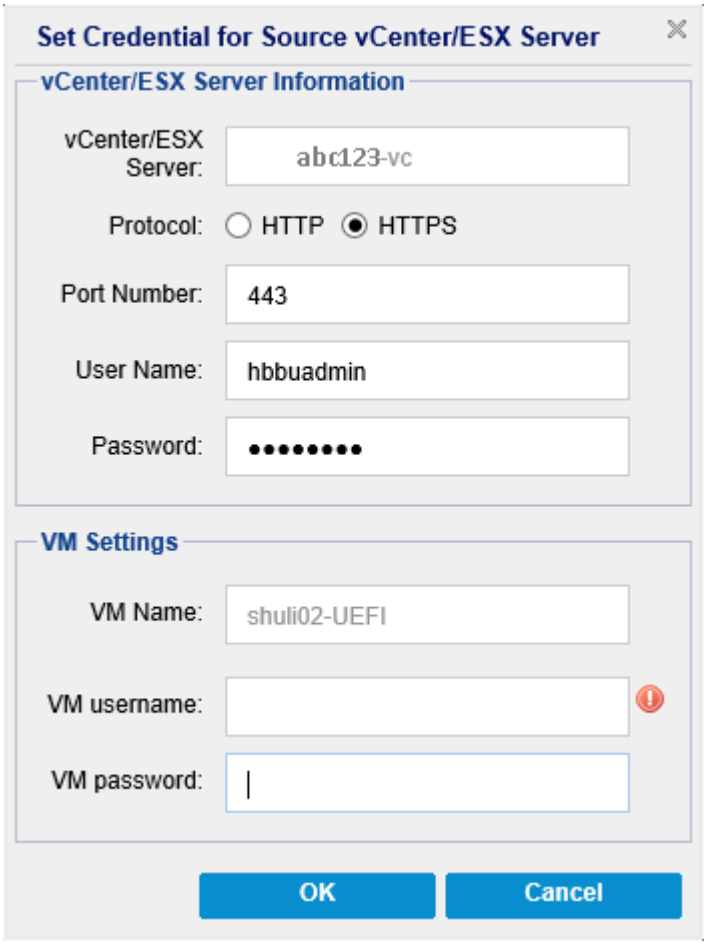
A continuación se especifican las opciones de destino disponibles:

Restauración en la ubicación original

Restaura en la ubicación original desde la que se ha capturado la imagen de copia de seguridad.

Nota: Si se ha realizado la copia de seguridad del punto de recuperación utilizando la copia de seguridad sin agente basada en el host, la restauración en la ubicación original es volver a llevar a cabo la restauración del archivo en la máquina virtual. En este caso, se abre un cuadro de diálogo. Se pueden introducir las credenciales del hipervisor y el sistema operativo de la máquina virtual.

Para la máquina virtual de VMware:



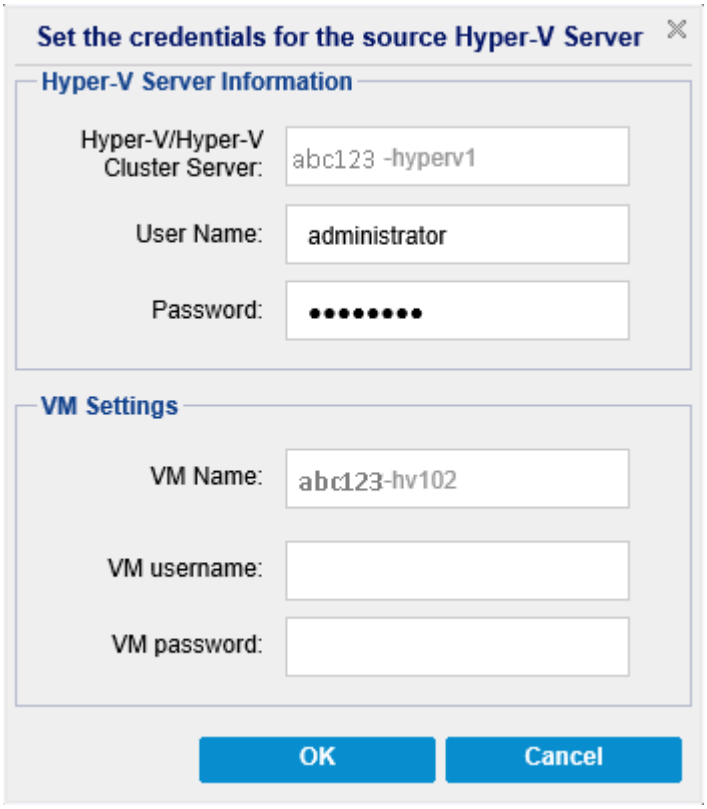
Nota: Para crear o escribir archivos en la máquina virtual, tenga en cuenta los siguientes requisitos para la configuración y los permisos de la cuenta de la máquina virtual:

- VMware Tools está instalado y en ejecución.
- Firewall debe permitir compartir archivos e impresoras.
- La cuenta es el administrador local integrado, el administrador del dominio integrado o la cuenta del dominio que es miembro del grupo de administradores locales. Si se utilizan otras cuentas, haga lo siguiente:

- Desactive el acceso remoto del Control de cuentas de usuario. Para desactivar el acceso remoto del UAC, consulte Importación de la máquina virtual utilizando una cuenta administrativa adicional.
- Desactive el Control de cuentas de usuario en la Política de seguridad local desactivando el valor de configuración Ejecutar todos los administradores en Modo de aprobación de administrador en secpol.msc-> Políticas locales-> Opciones de seguridad. (Secpol.msc es el editor de políticas de seguridad de Microsoft).

  Importante: No intente desactivar el UAC en el cuadro de diálogo Valores de configuración del control de la cuenta de usuario que se abre desde el panel de control.

Para la máquina virtual de Hyper-V:



Nota: Para crear o escribir archivos en la máquina virtual, tenga en cuenta los siguientes requisitos para la configuración y los permisos de la cuenta de la máquina virtual:

- Los servicios de integración de Hyper-V están instalados y en ejecución.

- Firewall debe permitir compartir archivos e impresoras.
- La cuenta es el administrador local integrado, el administrador del dominio integrado o la cuenta del dominio que es miembro del grupo de administradores locales. Si se utilizan otras cuentas, desactive el acceso remoto del Control de cuentas de usuario (UAC). Para desactivar el acceso remoto del UAC, consulte Importación de la máquina virtual utilizando una cuenta administrativa adicional.
- Si el sistema operativo invitado de la máquina virtual es la versión de cliente de Windows (por ejemplo, Windows 10), se deberá configurar manualmente el cortafuegos para permitir el servicio Windows Management Instrumentation (WMI).

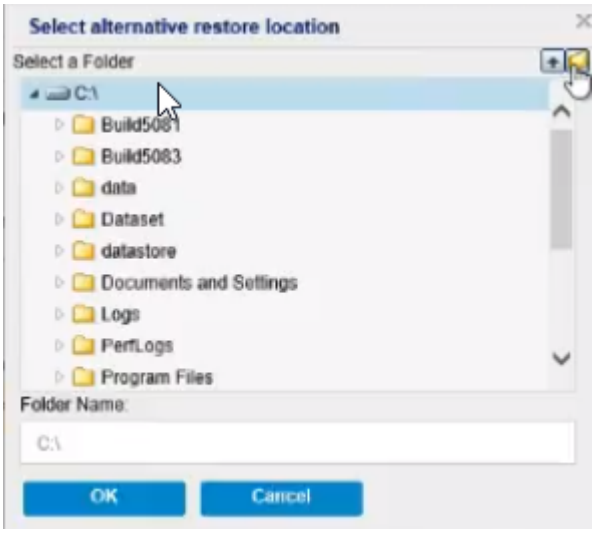
Restaurar en

Restaura en la ubicación especificada. Para restaurar datos en la ubicación especificada, realice lo siguiente:

- Para proporcionar el destino, haga clic en **Examinar**.

  Aparecerá el cuadro de diálogo Seleccionar ubicación de restauración alternativa.

- Seleccione la carpeta existente o cree una nueva según sea necesario y, a continuación, haga clic en **Aceptar**.



- Para verificar la conexión a la ubicación especificada, haga clic en el botón de flecha verde. Si es necesario, especifique el Nombre de usuario y la Contraseña para obtener acceso a dicha ubicación.

2. (Opcional) Para activar la comunicación entre el Agente de Windows y el servidor de puntos de recuperación, seleccione la casilla de verificación **Usar red selec-**

cionada para el tráfico de restauración y, a continuación, seleccione la red en la lista desplegable.

Notas:

- Si no se puede acceder a la red de copia de seguridad seleccionada y para continuar la tarea de copia de seguridad con la red disponible o con la red predeterminada, haga clic en la casilla de verificación **Continuar ejecutando la tarea incluso cuando no se puede conectar con la red de copia de seguridad seleccionada**.
- Para definir la restricción en la función SMB multicanal para que los datos se transfieran solo a través de la red seleccionada, seleccione la casilla de verificación **Utilizar una red Ethernet dedicada si el equipo actual permite SMB multicanal**.

  Esta opción no se encuentra disponible de forma determinada. Para activar esta opción, cree el registro de la cadena *UseDedicatedEthernet* en la ruta siguiente y, a continuación, establezca el valor del registro en 1:

  SOFTWARE\Arcserve\Unified Data Protection\Engine

  - Cuando realice una tarea de restauración desde la página Nodos, cree una clave de registro en el proxy de la copia de seguridad.
  - Cuando se realiza una tarea de restauración desde el agente normal mediante la sesión de la copia de seguridad del servidor de puntos de recuperación, cree una clave de registro en el agente normal.

3. Para mejorar el rendimiento al restaurar un volumen grande con muchos archivos pequeños, seleccione un volumen y, a continuación, en Restauración a nivel de bloque, haga clic en la casilla de verificación **Realizar restauración a nivel de bloque**. Otras opciones se desactivan y aparece una notificación. Para continuar con la restauración a nivel de bloque, haga clic en **Aceptar**.



Nota: Los datos se restauran en la máquina actual del Agente de UDP y se sobrescribe el volumen de destino. No se puede acceder al volumen de destino durante la tarea de restauración.

4. En Resolución de conflictos, especifique la opción correspondiente a la acción que deberá realizar Arcserve UDP si se encuentran conflictos durante el proceso de restauración.

   A continuación se especifican las opciones disponibles:

   Sobrescribir archivos existentes

   Sobrescribe (reemplaza) todos los archivos existentes que se encuentran en el destino de restauración. Todos los objetos se restaurarán desde los archivos de copia de seguridad, independientemente de si actualmente se encuentran en el equipo.

   Reemplazar los archivos activos

   Reemplaza todos los archivos activos después del reinicio. Si durante el intento de restauración, el Agente de Arcserve UDP para Windows detecta que el archivo existente está actualmente en uso o que algún usuario está accediendo al archivo, no sustituye ese archivo de forma inmediata, sino que retrasa la sustitución de los archivos activos hasta que se reinicie de nuevo el equipo con el fin de evitar problemas. (La restauración ocurrirá de forma inmediata pero los archivos activos se sustituirán a partir del reinicio siguiente).

   Esta opción solamente está disponible si selecciona la opción **Sobrescribir archivos existentes**.

   Nota: Si no se selecciona esta opción, se omite de la restauración cualquier archivo activo.

   Cambiar el nombre de los archivos

   Si el nombre de archivo ya existe, crea un archivo nuevo. Al seleccionar esta opción se copiará el archivo de origen en el destino con el mismo nombre de archivo pero con una extensión diferente. A continuación, los datos se restaurarán en un archivo nuevo.

   Omitir archivos existentes

   Omite y no sobrescribe (reemplaza) ningún archivo existente que se encuentre en el destino de restauración. Solo se restaurarán desde los archivos de copia de seguridad los objetos que no estén en el equipo actualmente.

   Valor por omisión: Omitir archivos existentes

5. En Estructura de directorios, si desea crear un directorio raíz durante la restauración, seleccione la casilla de verificación **Crear directorio raíz**.

   La casilla de verificación **Crear directorio raíz** especifica que si existe una estructura de directorio raíz en la imagen de copia de seguridad capturada, Arcserve

UDP recreará la misma estructura de directorio raíz en la ruta de destino de la restauración.

Si no se selecciona esta opción, el archivo o carpeta se restaurará directamente en la carpeta de destino.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt" y "C:\Folder1\SubFolder2\B.txt" y durante la restauración ha especificado como destino de la restauración "D:\Restore".

- Si ha seleccionado la restauración de los archivos "A.txt" y "B.txt" de manera individual, el destino de los archivos restaurados será "D:\Restore\A.txt" y "D:\Restore\B.txt" (no se recreará el directorio raíz anterior en el nivel de archivo especificado).
- Si se selecciona la restauración desde el nivel "Subcarpeta2", el destino para los archivos restaurados será "D:\Restore\SubFolder2\A.txt" y "D:\Restore\SubFolder2\B.txt" (el directorio raíz superior al nivel de carpeta especificada no se recreará).

Si se selecciona esta opción, la ruta completa del directorio raíz para los archivos/carpetas (incluyendo el nombre de volumen) se recrea en la carpeta de destino. Si los archivos o carpetas que deben restaurarse provienen del mismo nombre de volumen, la ruta del directorio raíz de destino no incluirá el nombre del volumen. Sin embargo, si los archivos o carpetas que deben restaurarse provienen de diferentes nombres de volúmenes, la ruta del directorio raíz de destino incluirá el nombre de volumen.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", y también E:\Folder3\SubFolder4\C.txt", y durante la restauración ha especificado el destino de restauración como "D:\Restore".

- Si ha seleccionado la restauración únicamente del archivo "A.txt", el destino para el archivo restaurado será "D:\Restore\Folder1\SubFolder2\A.txt" (se recreará todo el directorio raíz sin el nombre de volumen).
- Si ha seleccionado la restauración tanto del archivo "A.txt" como del archivo "C.txt", el destino para los archivos restaurados será "D:\Restore\C\ Folder1\SubFolder2\A.txt" y "D:\Restore\ E\Folder3\SubFolder4\C.txt" (se recreará todo el directorio raíz con el nombre de volumen).

6. Para la recuperación de la lista de control de acceso, para omitir el permiso original para los archivos o carpetas restaurados, seleccione la casilla de verificación **Omitir recuperación de la lista de control de acceso de archivos y carpetas**. Al seleccionar esta opción se permite heredar los permisos de la carpeta de destino. Si no se selecciona esta opción, se mantienen los permisos originales.

7. Para el **Cifrado de la copia de seguridad o la Protección por contraseña**, si es necesario, especifique la contraseña de cifrado de la copia de seguridad cuando se cifren los datos que intenta restaurar.

   Si se intenta realizar una restauración desde el mismo equipo del Agente de Arcserve UDP para Windows desde el que se ha realizado la copia de seguridad cifrada, no es necesario proporcionar ninguna contraseña. Sin embargo, sí será necesaria una contraseña si se intenta realizar la restauración desde otro equipo del Agente de Arcserve UDP para Windows.

   Nota: Si un icono de reloj aparece con el símbolo de candado, significa que el punto de recuperación contiene información cifrada y que puede requerir una contraseña para realizar la restauración.

8. Haga clic en **Siguiente**.

   Se abrirá la página Resumen de la restauración.

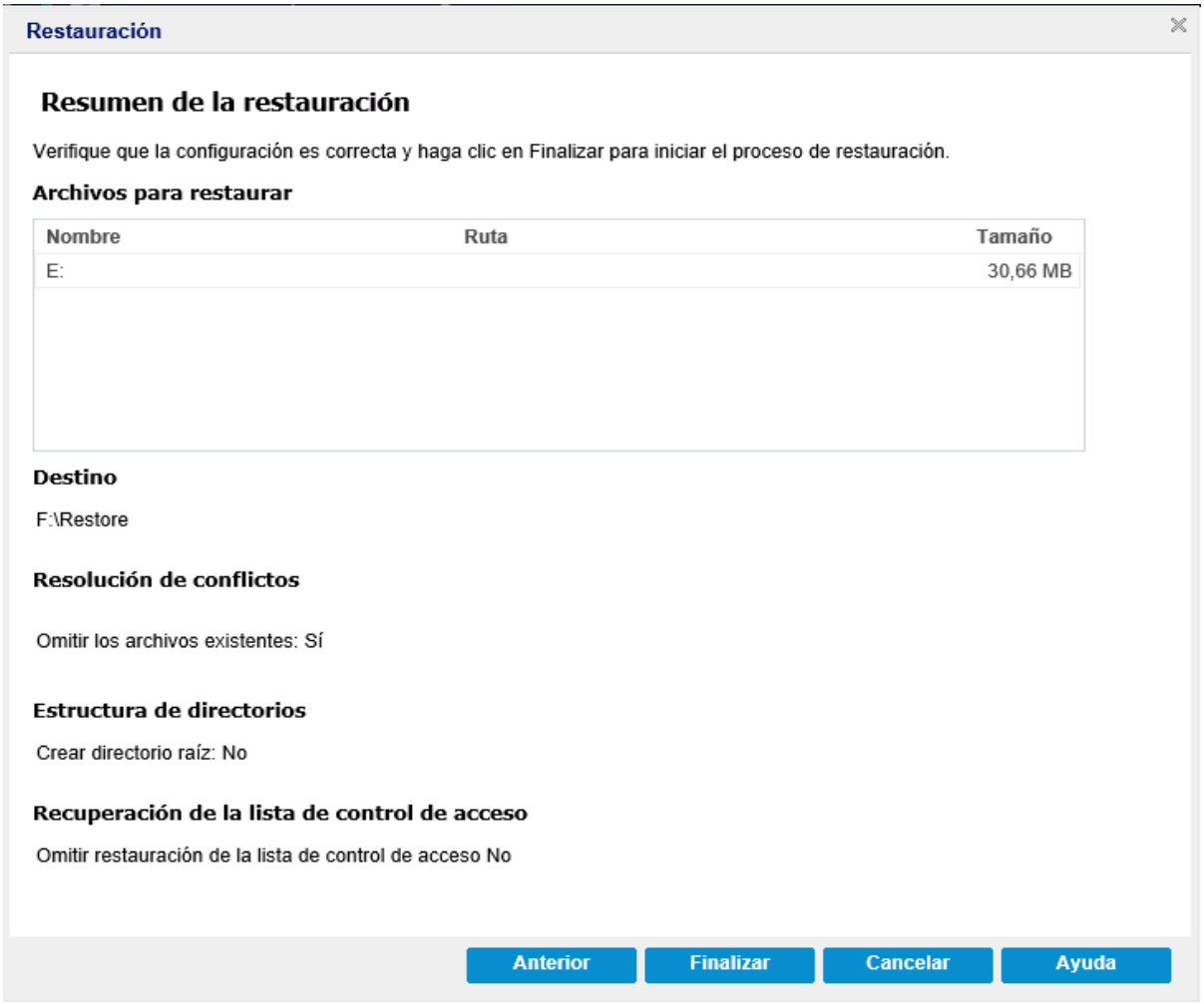
   Las opciones de restauración se han definido para restaurar desde un punto de recuperación.

Restauración del contenido del punto de recuperación

Después de definir las opciones de restauración, verifique que los valores de configuración sean correctos y confirme el proceso de restauración. La página Resumen de la restauración le ayuda a revisar todas las opciones de la restauración definidas y a modificarlas si es necesario.

Siga estos pasos:

1. En el cuadro de diálogo Resumen de la restauración, revise la información que aparece en pantalla para verificar que todas las opciones de restauración y los valores de configuración sean correctos.



2. Realice uno de los procedimientos siguientes:
   - Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para cambiar el valor de configuración incorrecto.

- Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar el proceso de restauración.

El contenido del punto de recuperación se restaura.

Verificación de que se ha restaurado el contenido

Después de la terminación del proceso de restauración, verifique que el contenido se ha restaurado en el destino especificado.

Siga estos pasos:

1. En la Consola de Arcserve UDP, vaya a **tareas** > **Tareas finalizadas correctamente**.

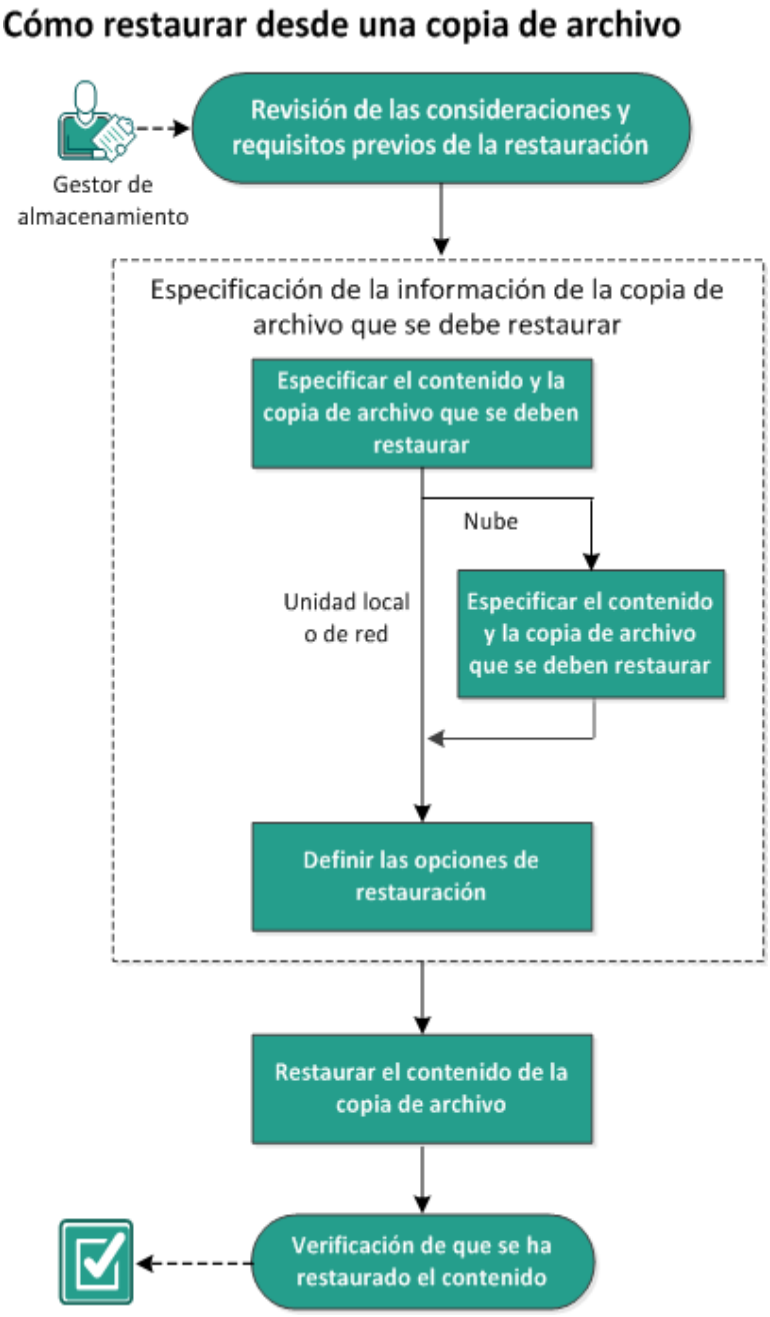
   La lista de tareas de copia de seguridad completadas aparecerá en el panel central.
2. Haga clic en la tarea de replicación inversa finalizada. Se actualiza el panel derecho.
3. En Detalles de la tarea, haga clic en el hipervínculo **Ver registros**.
4. Verifique el contenido para confirmar la tarea de restauración.

   El contenido restaurado se ha verificado correctamente.

Cómo restaurar desde una copia de archivo

Cada vez que Arcserve UDP realiza una tarea de copia de archivo correcta, realiza la copia de seguridad de todos los archivos que han cambiado desde la última tarea de copia de archivo correcta. Este método de restauración permite explorar los datos copiados y especificar exactamente qué archivo se desea restaurar.

El diagrama siguiente muestra el proceso para restaurar desde una copia de archivo:



Realice las tareas siguientes para restaurar desde una copia de archivo:

1. Revisión de las consideraciones y requisitos previos de la restauración
2. Especificación de la información de la copia de archivo que se debe restaurar
    a. Especificación del contenido y de la copia de archivo que se deben restaurar
        - Especificación de la configuración de la nube para la restauración
    b. Definición de las opciones de restauración
3. Restauración del contenido del punto de recuperación
4. Verificación de que se ha restaurado el contenido

Revisión de las consideraciones y requisitos previos de la restauración

Verifique que los requisitos previos siguientes existen antes de realizar una restauración:

- Como mínimo, existe una copia de archivo disponible para restaurar.
- Tiene un destino de copia de archivo válido y accesible desde el que restaurar el contenido de la copia de archivo.
- Tiene una ubicación de destino válida y accesible a la que poder restaurar el contenido de la copia de archivo.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones sobre la restauración:

- Arcserve UDP solamente permite la ejecución de una tarea de restauración cada vez. Si se intenta iniciar una tarea de restauración manualmente mientras otra tarea de restauración está en ejecución, aparecerá un mensaje de alerta informando de que se está ejecutándose otra tarea y solicitará que se vuelva a intentar más tarde.
- Si la restauración se debe realizar en un destino remoto y si todas las letras de unidad de disco (de la A a la Z) están ocupadas, la restauración a una ruta remota no se realizará correctamente. El Agente de Arcserve UDP (Windows) debe utilizar una letra de unidad de disco para montar la ruta de destino remota.
- Mejore la copia de archivo para optimizar el rendimiento:
  - La copia de archivo puede enviar varios fragmentos simultáneamente al destino (ArchMultChunkIO)
  - La copia de archivo puede copiar más de un archivo a la vez desde el destino (ThreadsForArchive).
  - La restauración desde una copia de archivo puede descargar más de un archivo a la vez (ThreadsForRestore).
  - La sincronización de catálogo utiliza varios subprocesos (ThreadForCatalogSync).

  Se pueden cambiar los valores del registro de copia de archivo predeterminados modificando el valor de DWORD adecuado. Para obtener más información, consulte Configuración de los valores de configuración de copia de

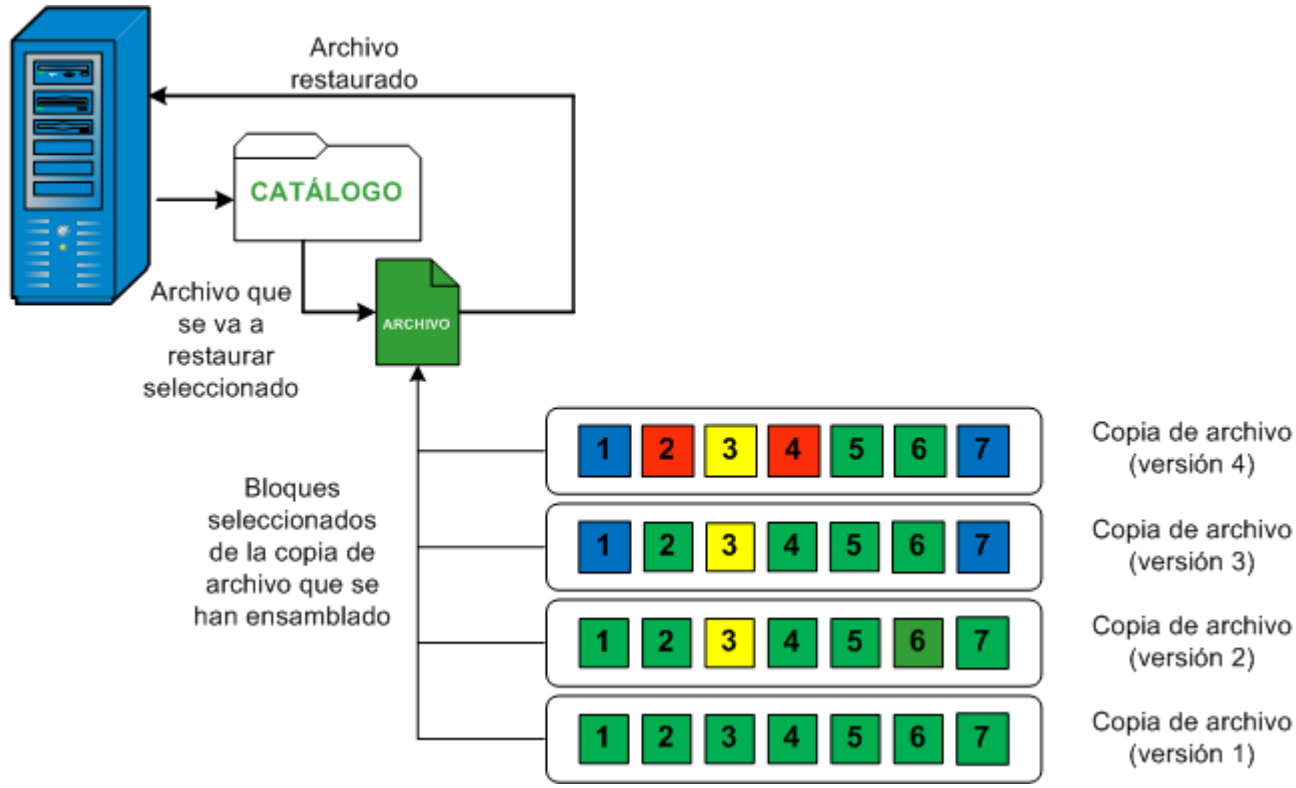
archivo para mejorar el rendimiento en la *Ayuda en línea del Agente para Windows*.

- (Opcional) Debe entender cómo funciona el proceso de restauración. Para obtener más información, consulte Cómo funciona la restauración de nivel de archivo.

Cómo funciona la restauración de nivel de archivo

Durante una copia de archivo, cada archivo de copia de seguridad está formado por una recopilación de bloques que definen a un determinado archivo. Se crea un archivo de catálogo para todas las versiones del archivo de copia de seguridad, junto con los bloques individuales que se utilizaron para estos archivos. Si necesita restaurar un archivo en particular, puede buscar y seleccionar el archivo que desea restaurar y las versiones de la copia de archivo desde las que desea restaurar. A continuación, Arcserve UDP recopila la versión de los bloques que se han utilizado para la copia de archivo del archivo especificado, que reconstruye y restaura el archivo.

El diagrama de flujo siguiente muestra el proceso de cómo Arcserve UDP restaura un archivo específico:



Especificación de la información de la copia de archivo que se debe restaurar

Arcserve UDP proporciona una opción para restaurar datos desde una copia de archivo. El objetivo de ejecutar una tarea de restauración correcta es de identificar los datos necesarios de forma rápida y de recuperarlos desde la ubicación de copia de seguridad correspondiente. Cada tarea de restauración necesita un origen y un destino.

El proceso de restauración desde una copia de archivo se muestra a continuación:

- Especificación del contenido y de la copia de archivo que se deben restaurar
- Definición de las opciones de restauración

Especificación del contenido y de la copia de archivo que se deben restaurar

Utilice la opción **Explorar copias de archivo** para restaurar desde una copia de archivo. Este método de restauración permite explorar los datos copiados y especificar exactamente qué archivo se desea restaurar.

Siga estos pasos:

1. Acceda al cuadro de diálogo Selección del método de recuperación de una de las formas siguientes:

   Desde Arcserve UDP:

   a. Inicie sesión en Arcserve UDP.

   b. Haga clic en la ficha **recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos agregados en el panel central.

   d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   e. Haga clic en **Restaurar** del menú desplegable **Acción**.

      El cuadro de diálogo Selección del método de restauración se abre.

      Nota: Se inicia sesión automáticamente en el nodo del Agente y el cuadro de diálogo Selección del método de restauración se abre desde el nodo del Agente.

   Desde el Agente de Arcserve UDP (Windows):

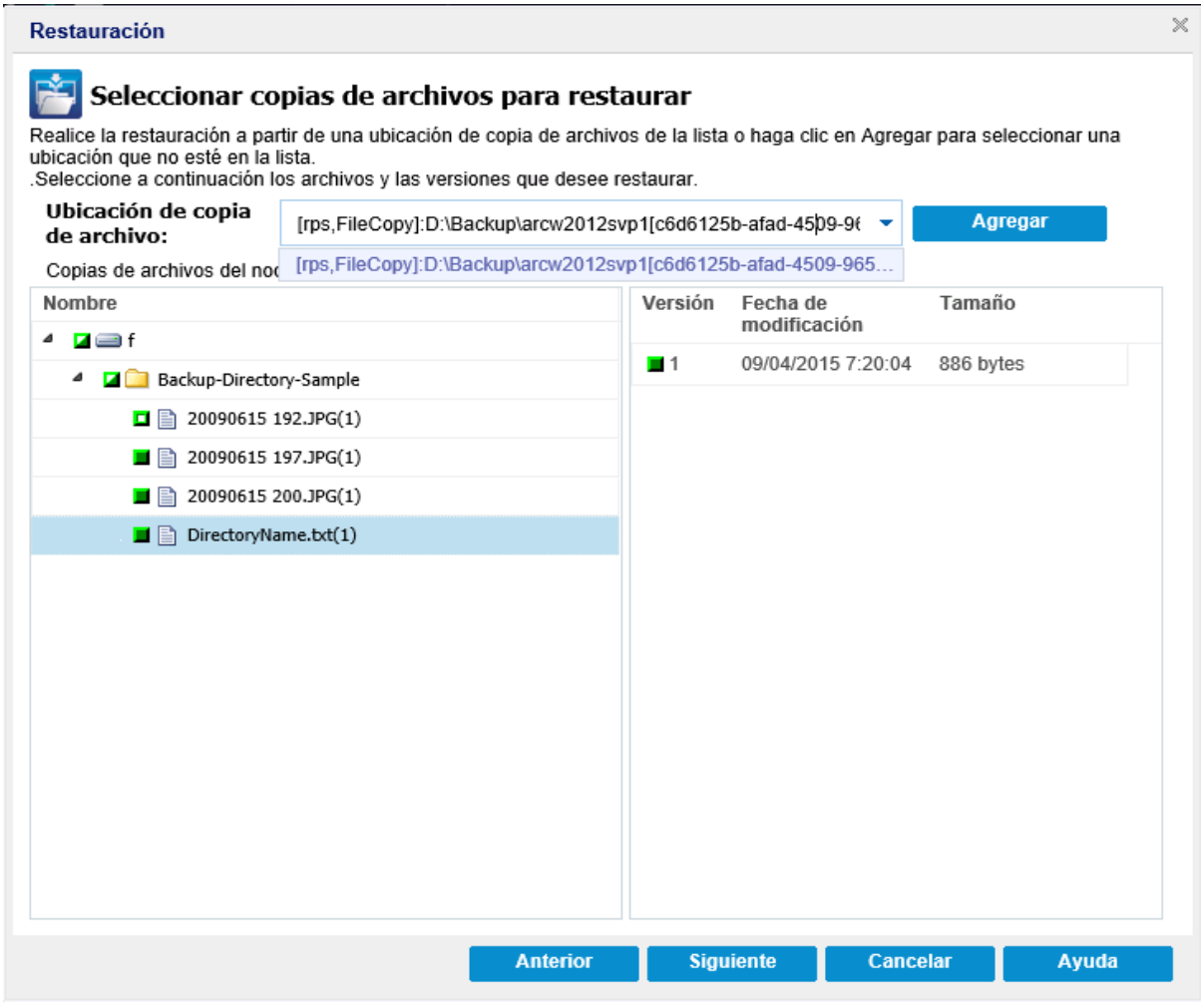
   a. Inicie sesión en el Agente de Arcserve UDP (Windows).

   b. En la página principal, seleccione **Restaurar**.

   El cuadro de diálogo Selección del método de restauración se abre.

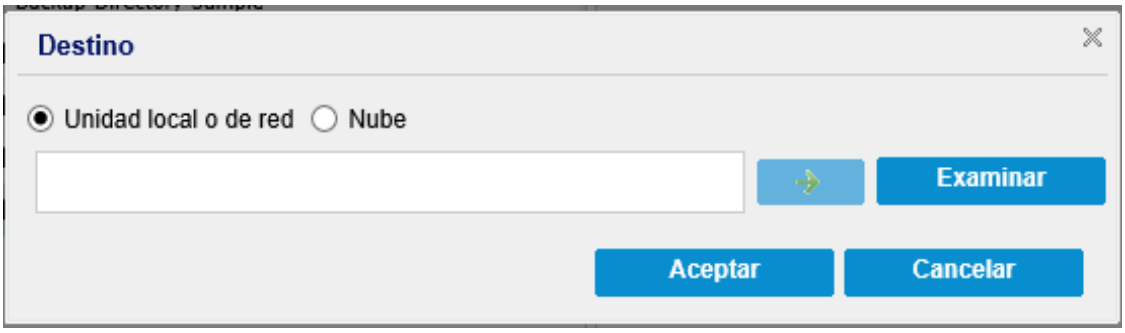
2. Haga clic en la opción **Explorar copias de archivo**.

   Se abrirá el cuadro de diálogo **Restauración.** El destino que se muestra actualmente en el campo **Restaurar desde** es el destino predeterminado de la **copia de archivo**.



3. Si es necesario, se puede hacer clic en **Agregar** para buscar una ubicación alternativa en la cual podrá almacenar las imágenes de la copia de archivo.

   Aparece el cuadro de diálogo **Destino** con las opciones de destino alternativas disponibles.



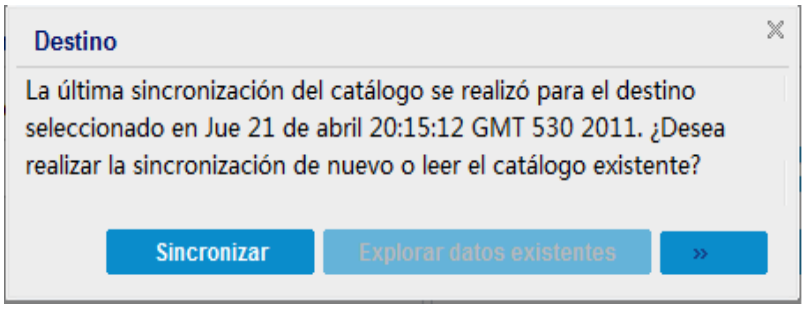
Unidad local o de red

Aparece el cuadro de diálogo **Seleccionar una ubicación de copia de seguridad**, lo que permite buscar y seleccionar una ubicación de unidad local o de red alternativa.

Nube

Se muestra el cuadro de diálogo **Configuración de la nube** que permite el acceso y la selección de una ubicación de la nube alternativa. Para obtener más información sobre este cuadro de diálogo, consulte Especificación de la configuración de la nube para la restauración.

Sin tener en cuenta si se ha seleccionado la restauración desde una **Unidad local o de red** o desde la **Nube**, cuando se cambia el destino a una ubicación alternativa aparece un cuadro emergente que pregunta si desea realizar una nueva sincronización del catálogo o leer desde el catálogo existente.



- Si se está realizando una sincronización del catálogo por primera vez, el botón **Explorar datos existentes** se desactivará porque el catálogo de copia de archivo no existe localmente.
- Si se ha realizado previamente una sincronización de catálogo, este cuadro de diálogo mostrará los detalles de la última vez que se sincronizó el catálogo desde este destino. Si se ejecutan más tareas de copia de archivo después de ese momento, puede que el catálogo no esté sincronizado; para ello se puede seleccionar la opción **Sincronizar** para asegurarse de que el catálogo de copia de archivo está actualizado.

1. Haga clic en **Sincronizar** para descargar el catálogo de copia de archivo del destino de copia de archivo especificado al equipo local para que la exploración sea más rápida.

2. Haga clic en **Explorar datos existentes** para usar el catálogo de copia de archivo que está disponible localmente y no tener que descargarlo/sincronizarlo otra vez.

4. En el panel izquierdo, especifique los datos de copia de archivo que deben restaurarse. Se pueden seleccionar carpetas o archivos copiados para restaurar.

   Cuando se selecciona un archivo individual para restaurar, todas las versiones del archivo copiadas de ese archivo se muestran en el panel derecho. Si hay versiones múltiples disponibles, será necesario seleccionar la versión copiada del archivo que desee restaurar.

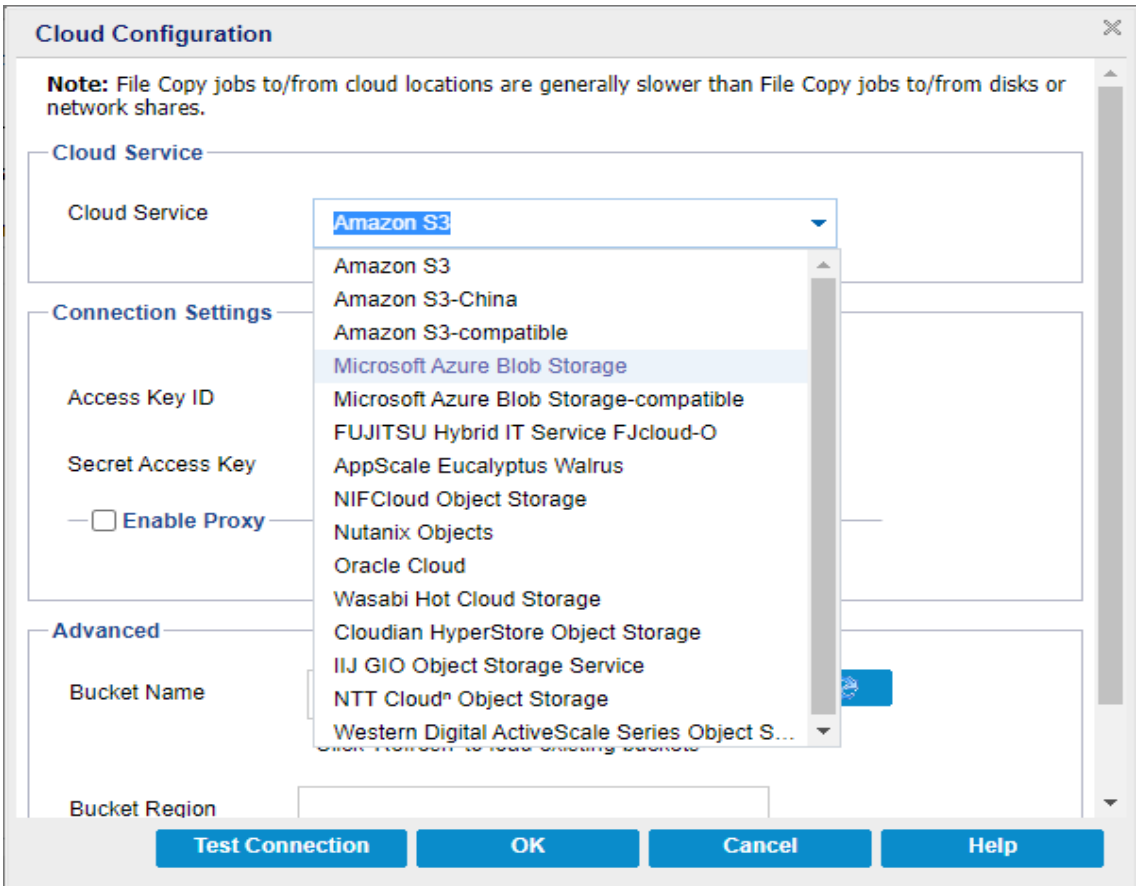
5. Después de seleccionar la carpeta del archivo copiado o la versión del archivo que se debe restaurar, haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Opciones de restauración**.

   Se especifica **la copia de archivo y el contenido que se deben restaurar**.

Especificación de la configuración de la nube para la restauración

Nota: El siguiente procedimiento solamente se aplica si se está restaurando un archivo o carpeta desde una ubicación de la nube de copia o archivado de archivos.



Las opciones disponibles son Amazon S3, Compatible con Amazon S3, Windows Azure, Compatible con Windows Azure, FUJITSU Hybrid IT Service FJcloud-O y Eucalyptus-Walrus. (Amazon S3 es el distribuidor predeterminado).

Nota: Si está utilizando Eucalyptus-Walrus como su distribuidor de la nube de copia de archivos, no podrá copiar archivos cuya longitud de la ruta total sea superior a 170 caracteres.

Las opciones de configuración para cada distribuidor de la nube son similares (con una terminología diferente) y se describe cualquier diferencia patente.

1. Desde la opción **Explorar copias de archivo** o desde la opción **Buscar archivos/carpetas para restaurar, haga clic en Agregar**.

   Se abre el cuadro de diálogo **Destino**.

2. Seleccione **Nube** y haga clic en **Examinar**.

Se abre el cuadro de diálogo **Configuración de la nube**.

3. Introduzca los siguientes detalles:

Nombre de almacenamiento

Especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre de almacenamiento único.

Servicio de almacenamiento

Seleccione el servicio en la lista desplegable. La opción de configuración varía en función del servicio de almacenamiento que se haya seleccionado.

ID de la clave de acceso/Nombre de cuenta/ID de la consulta

Identifica el usuario que solicita acceso esta ubicación.

Para este campo, Amazon S3 utiliza el ID de la clave de acceso, Windows Azure y FUJITSU Hybrid IT Service FJcloud-O utilizan Nombre de cuenta y Eucalyptus-Walrus utiliza ID de la consulta.

Clave de acceso secreta/Clave secreta

Como la clave de acceso no está cifrada, esta clave de acceso secreta es una contraseña que se utiliza para verificar la autenticidad de la solicitud a fin de acceder a esta ubicación.

Importante: Esta clave de acceso secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave de acceso secreta en una página Web ni en otro código de origen accesible públicamente ni la transmita a través de canales no seguros.

Para este campo, Amazon S3 utiliza la Clave de acceso Secreta. Windows Azure, FUJITSU Hybrid IT Service FJcloud-O y Eucalyptus-Walrus utilizan Clave secreta.

Configuración proxy

Especifica la configuración del servidor proxy. Seleccione **Conectar utilizando un servidor proxy**para activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. Se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

Nota: La capacidad de proxy no está disponible para Eucalyptus-Walrus.

Nombre del depósito/contenedor

Todos los archivos y las carpetas movidas o copiadas al distribuidor de la nube se almacenan y se organizan en sus depósitos (o contenedores). Los depósitos son como un contenedor para los archivos y se utilizan para agrupar y organizar objetos conjuntamente. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

Para este campo, Amazon S3 y Eucalyptus-Walrus utilizan Nombre de depósito. Windows Azure y FUJITSU Hybrid IT Service FJcloud-O utilizan Contenedor.

Nota: Para finalizar este paso, todas las referencias a depósitos se pueden aplicar también a los contenedores a menos que se especifique otra cosa.

Zona de depósito

Se refiere a la región del depósito en Amazon y FUJITSU Hybrid IT Service FJcloud-O.

Número de contrato

Hace referencia al número de contrato que proporciona FUJITSU Hybrid IT Service FJcloud-O.

ID del proyecto

Hace referencia al ID del proyecto que genera FUJITSU Hybrid IT Service FJcloud-O.

Activar el almacenamiento de redundancia reducida

Para Amazon S3 solamente, esta opción permite la selección para activar el almacenamiento de redundancia reducida (RRS). RRS es una opción de almacenamiento de Amazon S3 que facilita la reducción de costes a través del almacenamiento de datos no críticos y reproducibles a niveles de redundancia más bajos que el almacenamiento estándar de Amazon S3. Ambas opciones de almacenamiento de redundancia estándares y reducidas almacenan datos en diferentes funcionalidades y dispositivos, pero con RRS los datos se replican menos veces, de modo que el coste es menor. Se debería esperar la misma latencia y rendimiento mediante el almacenamiento estándar de Amazon S3 o RRS. De forma predeterminada, esta opción no está seleccionada (Amazon S3 utiliza la opción de almacenamiento estándar).

4. Haga clic en **Probar conexión** para verificar la conexión a la ubicación de la nube especificada.
5. Haga clic en **Aceptar**.

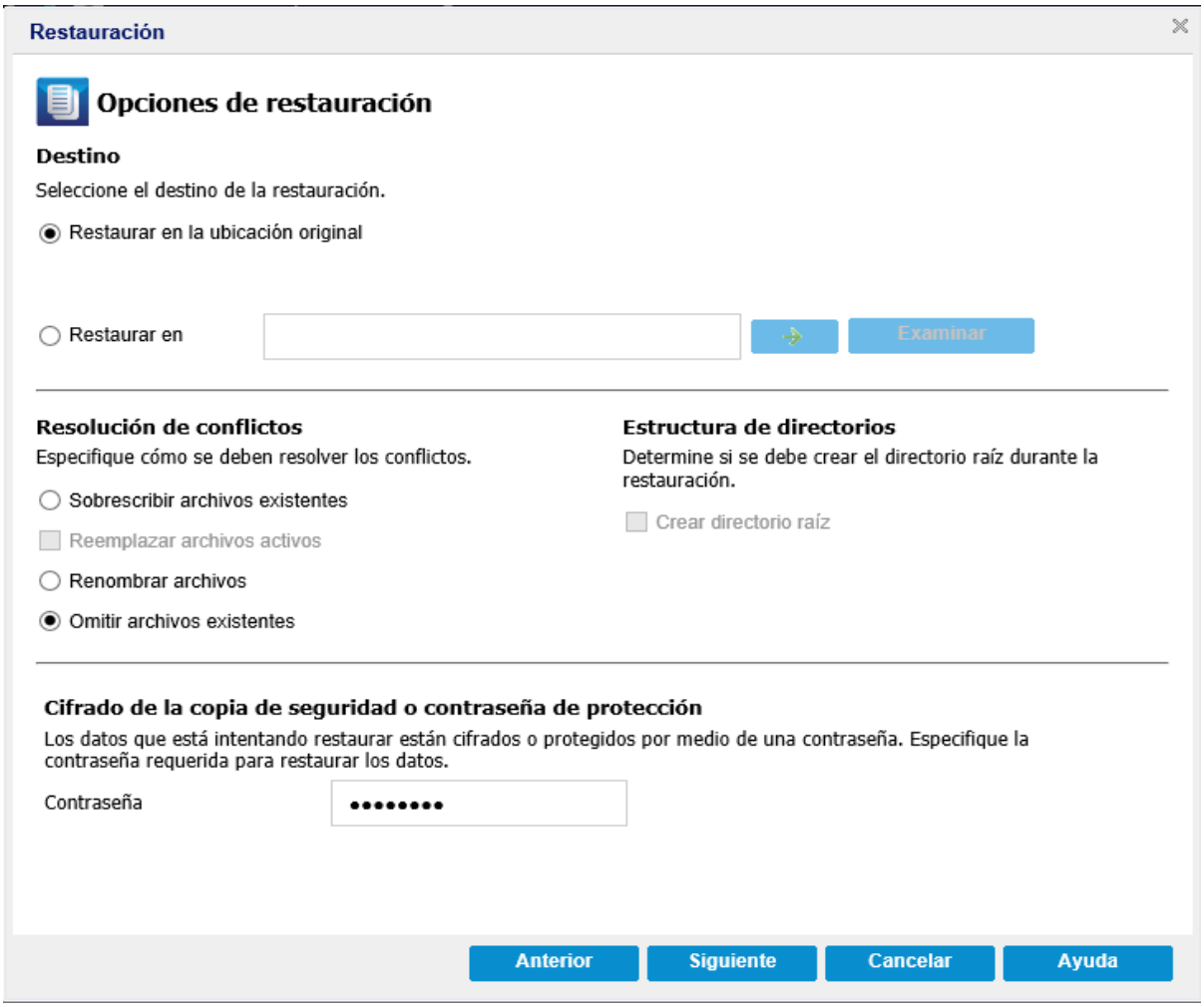
   La cuenta de la nube se agrega a la consola.

Definición de las opciones de restauración

Después de especificar la información de la copia de archivo que se debe restaurar, defina las opciones de copia para la copia de archivo y el contenido seleccionados.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, seleccione el destino para la restauración.



A continuación se especifican las opciones de destino disponibles:

Restaurar en la ubicación original

Restaura en la ubicación original desde la que se ha capturado la imagen de copia de seguridad.

Restaurar en

Restaura en la ubicación especificada. Se puede hacer clic en el botón de la flecha verde para comprobar la conexión con la ubicación especificada. Si es necesario, también puede escribir las credenciales de nombre de usuario y de contraseña para obtener acceso a dicha ubicación.

2. En **Resolución de conflictos**, especifique la opción correspondiente a la acción que deberá realizar Arcserve UDP si se encuentran conflictos durante el proceso de restauración.

   A continuación se especifican las opciones disponibles:

   Sobrescribir archivos existentes

   Sobrescribe (reemplaza) todos los archivos existentes que se encuentran en el destino de restauración. Todos los objetos se restaurarán desde los archivos de copia de seguridad, independientemente de si actualmente se encuentran en el equipo.

   Reemplazar los archivos activos

   Reemplaza todos los archivos activos después del reinicio. Si durante el intento de restauración, el Agente de Arcserve UDP para Windows detecta que el archivo existente está actualmente en uso o que algún usuario está accediendo al archivo, no sustituye ese archivo de forma inmediata, sino que retrasa la sustitución de los archivos activos hasta que se reinicie de nuevo el equipo con el fin de evitar problemas. (La restauración ocurrirá de forma inmediata pero los archivos activos se sustituirán a partir del reinicio siguiente).

   Esta opción solamente está disponible si selecciona la opción **Sobrescribir archivos existentes**.

   Nota: Si no se selecciona esta opción, se omite de la restauración cualquier archivo activo.

   Cambiar el nombre de los archivos

   Si el nombre de archivo ya existe, crea un archivo nuevo. Al seleccionar esta opción se copiará el archivo de origen en el destino con el mismo nombre de archivo pero con una extensión diferente. A continuación, los datos se restaurarán en un archivo nuevo.

   Omitir archivos existentes

Omite y no sobrescribe (reemplaza) ningún archivo existente que se encuentre en el destino de restauración. Solo se restaurarán desde los archivos de copia de seguridad los objetos que no estén en el equipo actualmente.

Valor por omisión: Omitir archivos existentes

3. Especifique la **Estructura de directorios** para crear un directorio raíz durante la restauración.

Crear directorio raíz

Especifica que si existe una estructura de directorio raíz en la imagen de copia de seguridad capturada, Arcserve UDP recreará la misma estructura de directorio raíz en la ruta de destino de la restauración.

Si no se selecciona esta opción, el archivo o carpeta se restaurará directamente en la carpeta de destino.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt" y "C:\Folder1\SubFolder2\B.txt" y durante la restauración ha especificado como destino de la restauración "D:\Restore".

- Si ha seleccionado la restauración de los archivos "A.txt" y "B.txt" de manera individual, el destino de los archivos restaurados será "D:\Restore\A.txt" y "D:\Restore\B.txt" (no se recreará el directorio raíz anterior en el nivel de archivo especificado).
- Si se selecciona la restauración desde el nivel "Subcarpeta2", el destino para los archivos restaurados será "D:\Restore\SubFolder2\A.txt" y "D:\Restore\SubFolder2\B.txt" (el directorio raíz superior al nivel de carpeta especificada no se recreará).

Con esta opción seleccionada, la ruta completa de directorio raíz para los archivos/carpetas (incluyendo el nombre de volumen) se recrea en la carpeta de destino. Si los archivos o carpetas que deben restaurarse provienen del mismo nombre de volumen, la ruta del directorio raíz de destino no incluirá el nombre del volumen. Sin embargo, si los archivos o carpetas que deben restaurarse provienen de diferentes nombres de volúmenes, la ruta del directorio raíz de destino incluirá el nombre de volumen.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", y también E:\Folder3\SubFolder4\C.txt", y durante la restauración ha especificado el destino de restauración como "D:\Restore".

- Si ha seleccionado la restauración únicamente del archivo "A.txt", el destino para el archivo restaurado será "D:\Restore\ Folder1\SubFolder2\A.txt" (se recreará todo el directorio raíz sin el nombre de volumen).

- Si ha seleccionado la restauración tanto del archivo "A.txt" como del archivo "C.txt", el destino para los archivos restaurados será "D:\Restore\C\ Folder1\SubFolder2\A.txt" y "D:\Restore\ E\Folder3\SubFolder4\C.txt" (se recreará todo el directorio raíz con el nombre de volumen).

4. Especifique la contraseña de cifrado en **Contraseña de cifrado de copia de archivo**.
5. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Resumen de la restauración**.

   Las opciones de restauración se han definido para restaurar desde una copia de archivo.

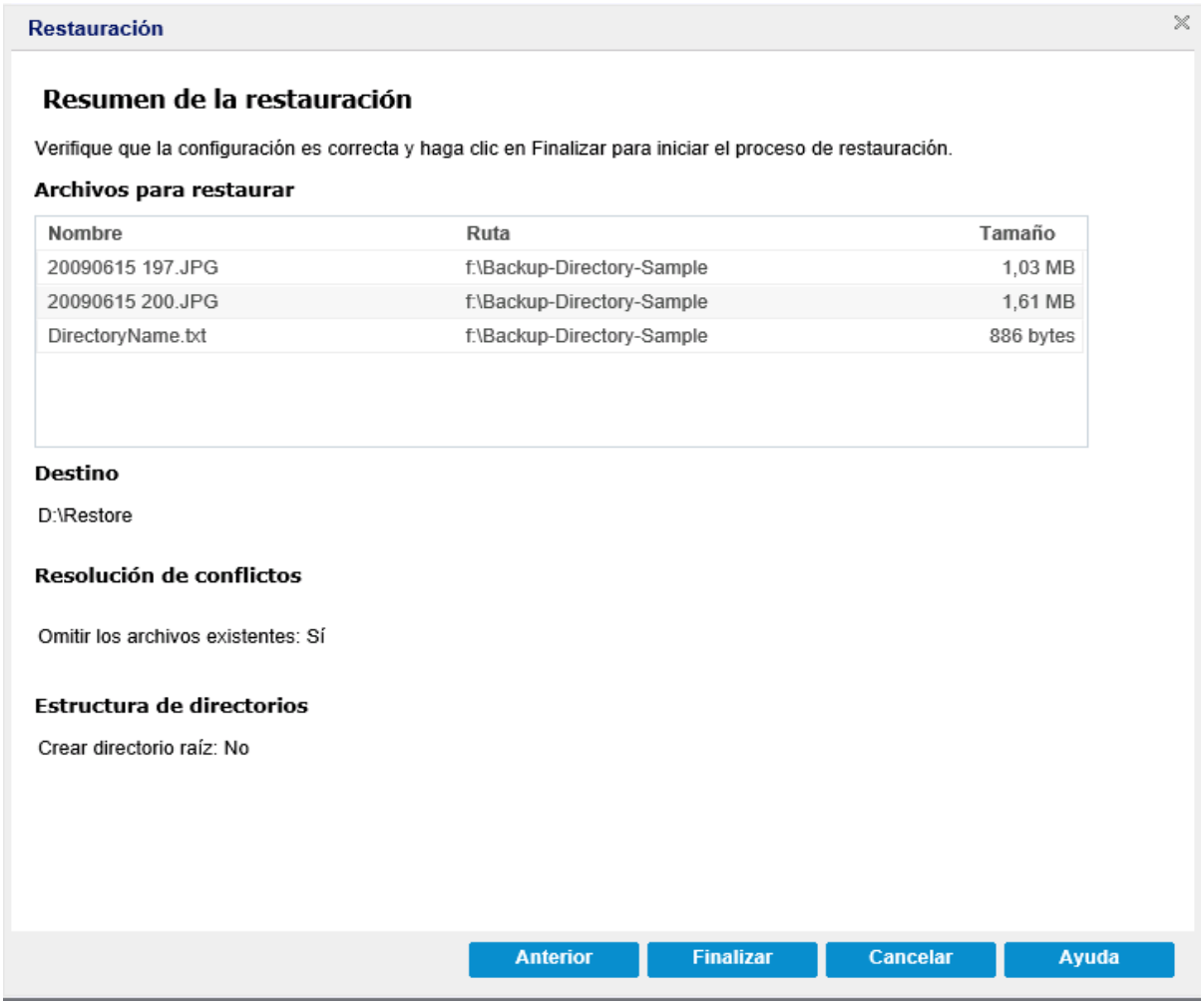
Restauración del contenido de la copia de archivo

Después de definir las opciones de restauración, verifique que los valores de configuración sean correctos y confirme el proceso de restauración. El **Resumen de la restauración** le ayuda a revisar todas las opciones de la restauración definidas y a modificarlas si es necesario.

Siga estos pasos:

1. En el cuadro de diálogo **Resumen de la restauración**, revise la información que aparece en pantalla para verificar que todas las opciones de restauración y los valores

de configuración sean correctos.



- Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para cambiar el valor de configuración incorrecto.
- Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar el proceso de restauración.

El contenido de la copia de archivo se restaura.

Verificación de que se ha restaurado el contenido

Después de la terminación del proceso de restauración, verifique que el contenido se ha restaurado en el destino especificado.

Siga estos pasos:

1. Vaya al destino de la restauración que se ha especificado.

   Aparecerá una lista de carpetas.

2. Encuentre el archivo en el cual ha restaurado el contenido.

   Por ejemplo, si selecciona restaurar el archivo **A.txt** en el destino de la restauración D:\Restore, vaya a la ubicación siguiente:

   D:\Restore\A.txt

3. Verifique el contenido para confirmar la tarea de restauración.

   El contenido restaurado se ha verificado correctamente.

Cómo restaurar desde un archivado de archivos

Cada vez que Arcserve UDP realiza una tarea de copia de archivado de archivos correcta, archiva todos los archivos que han cambiado desde la última tarea de copia de archivado de archivos correcta. Este método de restauración permite explorar los archivos archivados y especificar exactamente qué archivo se desea restaurar.

El proceso de restauración del archivado de archivos es idéntico a la restauración de copia de archivo.

Realice las tareas siguientes para restaurar desde un archivado de archivos:

1. Revisión de las consideraciones y requisitos previos de la restauración
2. Especificación de la información de la copia de archivo que se debe restaurar
    a. Especificación del contenido y de la copia de archivo que se deben restaurar
        - Especificación de la configuración de la nube para la restauración
    b. Definición de las opciones de restauración
3. Restauración del contenido del punto de recuperación
4. Verificación de que se ha restaurado el contenido

Revisión de las consideraciones y requisitos previos de la restauración

Verifique que los requisitos previos siguientes existen antes de realizar una restauración:

- Como mínimo, existe una copia de archivo disponible para restaurar.
- Tiene un destino de copia de archivo válido y accesible desde el que restaurar el contenido de la copia de archivo.
- Tiene una ubicación de destino válida y accesible a la que poder restaurar el contenido de la copia de archivo.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones sobre la restauración:

- Arcserve UDP solamente permite la ejecución de una tarea de restauración cada vez. Si se intenta iniciar una tarea de restauración manualmente mientras otra tarea de restauración está en ejecución, aparecerá un mensaje de alerta informando de que se está ejecutándose otra tarea y solicitará que se vuelva a intentar más tarde.
- Si la restauración se debe realizar en un destino remoto y si todas las letras de unidad de disco (de la A a la Z) están ocupadas, la restauración a una ruta remota no se realizará correctamente. El Agente de Arcserve UDP (Windows) debe utilizar una letra de unidad de disco para montar la ruta de destino remota.
- Mejore la copia de archivo para optimizar el rendimiento:
  - La copia de archivo puede enviar varios fragmentos simultáneamente al destino (ArchMultChunkIO)
  - La copia de archivo puede copiar más de un archivo a la vez desde el destino (ThreadsForArchive).
  - La restauración desde una copia de archivo puede descargar más de un archivo a la vez (ThreadsForRestore).
  - La sincronización de catálogo utiliza varios subprocesos (ThreadForCatalogSync).

  Se pueden cambiar los valores del registro de copia de archivo predeterminados modificando el valor de DWORD adecuado. Para obtener más información, consulte Configuración de los valores de configuración de copia de

archivo para mejorar el rendimiento en la *Ayuda en línea del Agente para Windows*.

- (Opcional) Debe entender cómo funciona el proceso de restauración. Para obtener más información, consulte Cómo funciona la restauración de nivel de archivo.

Especificación de la información de la copia de archivo que se debe restaurar

Arcserve UDP proporciona una opción para restaurar datos desde una copia de archivo. El objetivo de ejecutar una tarea de restauración correcta es de identificar los datos necesarios de forma rápida y de recuperarlos desde la ubicación de copia de seguridad correspondiente. Cada tarea de restauración necesita un origen y un destino.

El proceso de restauración desde una copia de archivo se muestra a continuación:

- Especificación del contenido y de la copia de archivo que se deben restaurar
- Definición de las opciones de restauración

Especificación del contenido y de la copia de archivo que se deben restaurar

Utilice la opción **Explorar copias de archivo** para restaurar desde una copia de archivo. Este método de restauración permite explorar los datos copiados y especificar exactamente qué archivo se desea restaurar.

Siga estos pasos:

1. Acceda al cuadro de diálogo Selección del método de recuperación de una de las formas siguientes:

   Desde Arcserve UDP:

   a. Inicie sesión en Arcserve UDP.

   b. Haga clic en la ficha **recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos agregados en el panel central.

   d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   e. Haga clic en **Restaurar** del menú desplegable **Acción**.

      El cuadro de diálogo Selección del método de restauración se abre.

      Nota: Se inicia sesión automáticamente en el nodo del Agente y el cuadro de diálogo Selección del método de restauración se abre desde el nodo del Agente.

   Desde el Agente de Arcserve UDP (Windows):

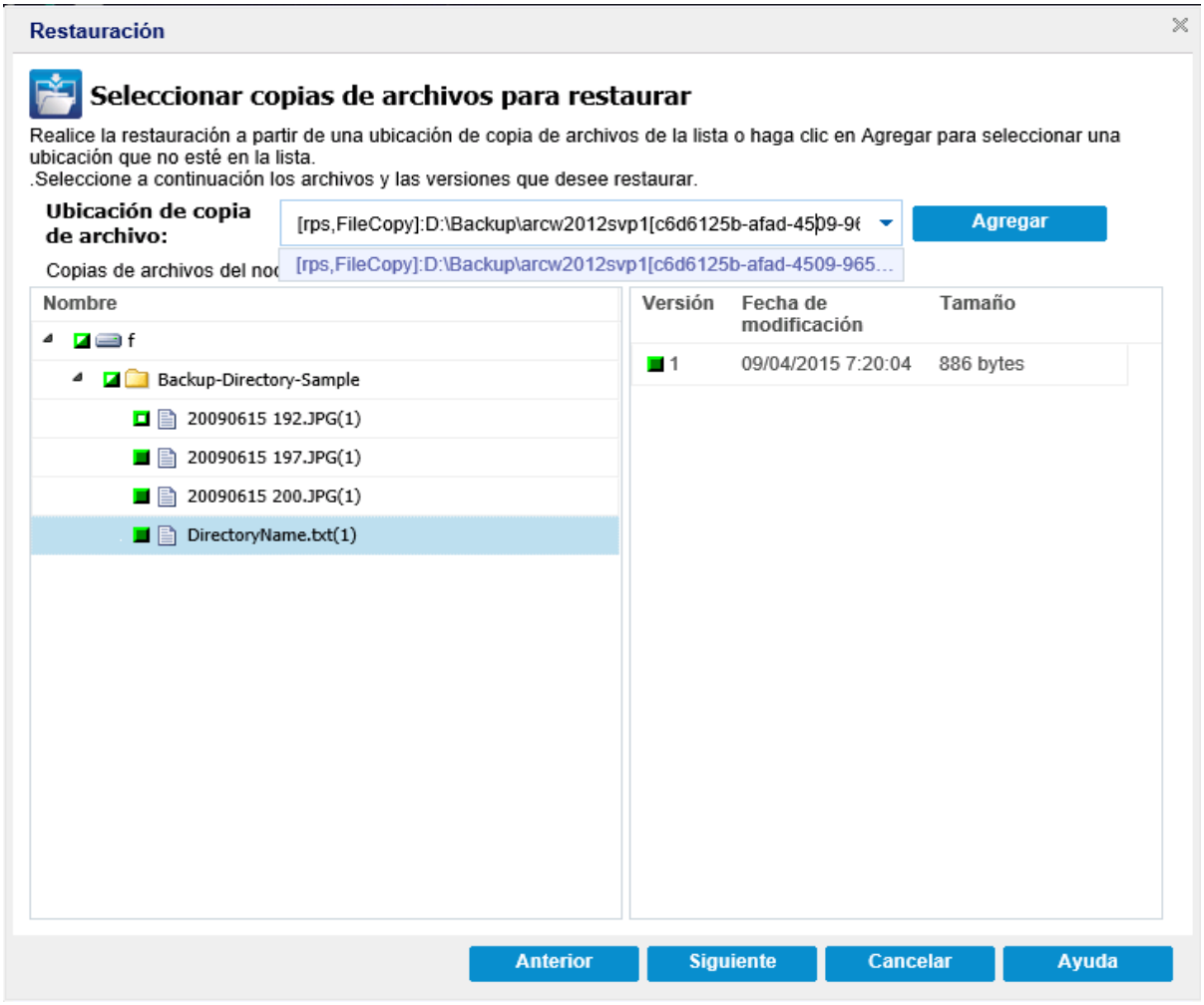
   a. Inicie sesión en el Agente de Arcserve UDP (Windows).

   b. En la página principal, seleccione **Restaurar**.

   El cuadro de diálogo Selección del método de restauración se abre.

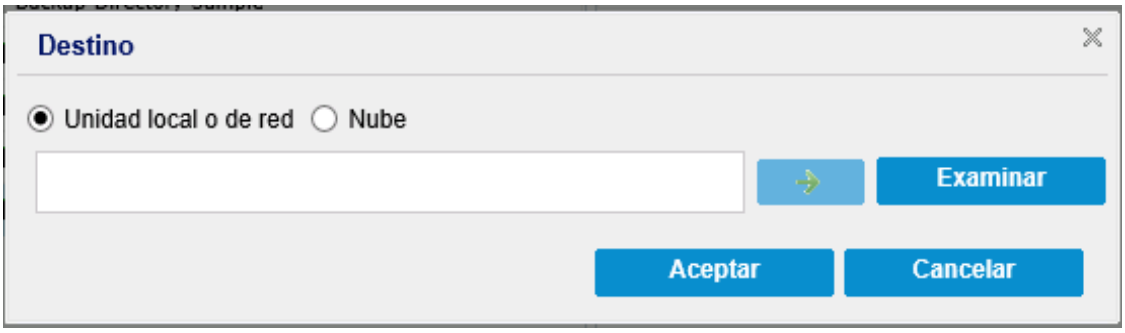
2. Haga clic en la opción **Explorar copias de archivo**.

   Se abrirá el cuadro de diálogo **Restauración.** El destino que se muestra actualmente en el campo **Restaurar desde** es el destino predeterminado de la **copia de archivo**.



3. Si es necesario, se puede hacer clic en **Agregar** para buscar una ubicación alternativa en la cual podrá almacenar las imágenes de la copia de archivo.

   Aparece el cuadro de diálogo **Destino** con las opciones de destino alternativas disponibles.



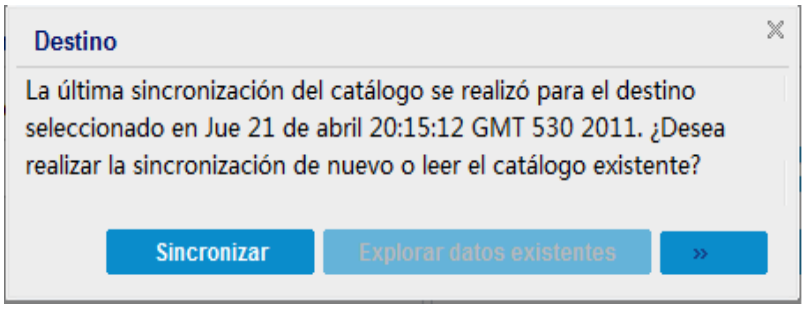
Unidad local o de red

Aparece el cuadro de diálogo **Seleccionar una ubicación de copia de seguridad**, lo que permite buscar y seleccionar una ubicación de unidad local o de red alternativa.

Nube

Se muestra el cuadro de diálogo **Configuración de la nube** que permite el acceso y la selección de una ubicación de la nube alternativa. Para obtener más información sobre este cuadro de diálogo, consulte Especificación de la configuración de la nube para la restauración.

Sin tener en cuenta si se ha seleccionado la restauración desde una **Unidad local o de red** o desde la **Nube**, cuando se cambia el destino a una ubicación alternativa aparece un cuadro emergente que pregunta si desea realizar una nueva sincronización del catálogo o leer desde el catálogo existente.



- Si se está realizando una sincronización del catálogo por primera vez, el botón **Explorar datos existentes** se desactivará porque el catálogo de copia de archivo no existe localmente.
- Si se ha realizado previamente una sincronización de catálogo, este cuadro de diálogo mostrará los detalles de la última vez que se sincronizó el catálogo desde este destino. Si se ejecutan más tareas de copia de archivo después de ese momento, puede que el catálogo no esté sincronizado; para ello se puede seleccionar la opción **Sincronizar** para asegurarse de que el catálogo de copia de archivo está actualizado.

1. Haga clic en **Sincronizar** para descargar el catálogo de copia de archivo del destino de copia de archivo especificado al equipo local para que la exploración sea más rápida.

2. Haga clic en **Explorar datos existentes** para usar el catálogo de copia de archivo que está disponible localmente y no tener que descargarlo/sincronizarlo otra vez.

4. En el panel izquierdo, especifique los datos de copia de archivo que deben restaurarse. Se pueden seleccionar carpetas o archivos copiados para restaurar.

   Cuando se selecciona un archivo individual para restaurar, todas las versiones del archivo copiadas de ese archivo se muestran en el panel derecho. Si hay versiones múltiples disponibles, será necesario seleccionar la versión copiada del archivo que desee restaurar.

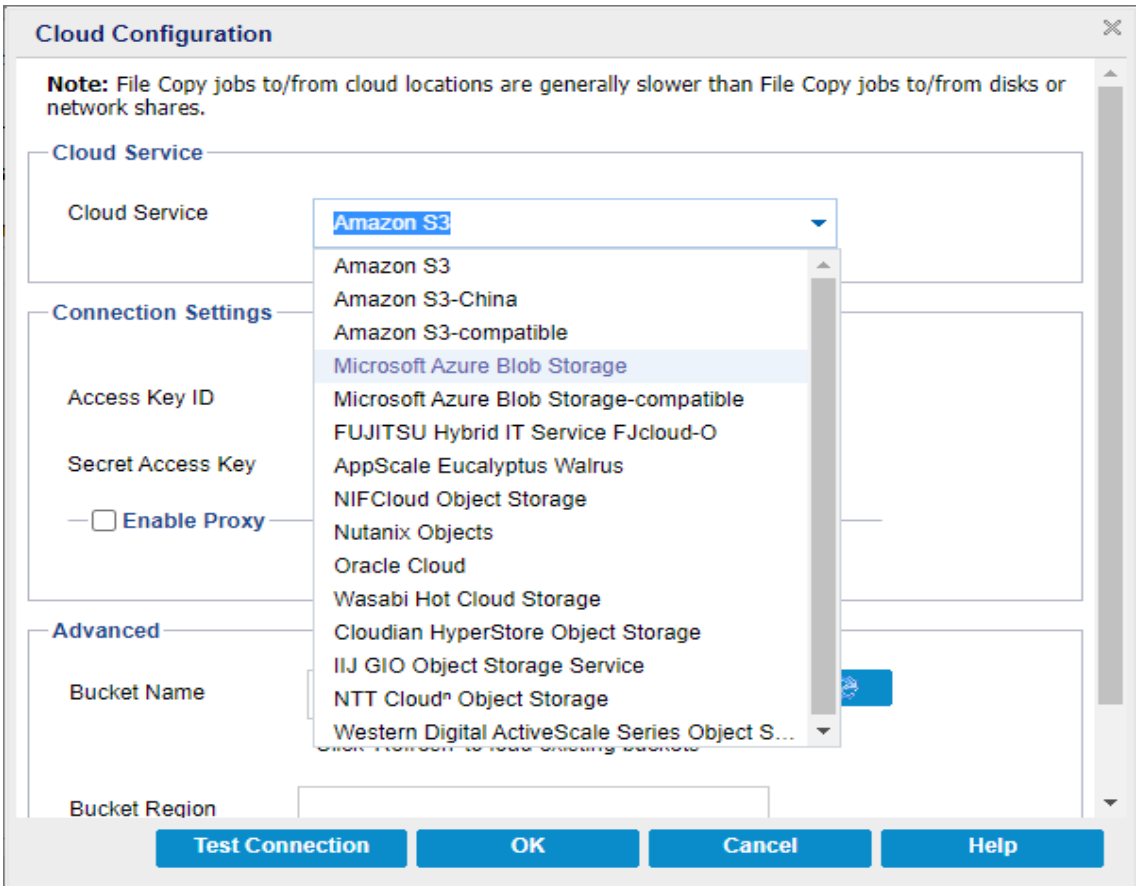
5. Después de seleccionar la carpeta del archivo copiado o la versión del archivo que se debe restaurar, haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Opciones de restauración**.

   Se especifica **la copia de archivo y el contenido que se deben restaurar**.

Especificación de la configuración de la nube para la restauración

Nota: El siguiente procedimiento solamente se aplica si se está restaurando un archivo o carpeta desde una ubicación de la nube de copia o archivado de archivos.



Las opciones disponibles son Amazon S3, Compatible con Amazon S3, Windows Azure, Compatible con Windows Azure, FUJITSU Hybrid IT Service FJcloud-O y Eucalyptus-Walrus. (Amazon S3 es el distribuidor predeterminado).

Nota: Si está utilizando Eucalyptus-Walrus como su distribuidor de la nube de copia de archivos, no podrá copiar archivos cuya longitud de la ruta total sea superior a 170 caracteres.

Las opciones de configuración para cada distribuidor de la nube son similares (con una terminología diferente) y se describe cualquier diferencia patente.

1. Desde la opción **Explorar copias de archivo** o desde la opción **Buscar archivos/carpetas para restaurar, haga clic en Agregar**.

   Se abre el cuadro de diálogo **Destino**.

2. Seleccione **Nube** y haga clic en **Examinar**.

Se abre el cuadro de diálogo **Configuración de la nube**.

3. Introduzca los siguientes detalles:

Nombre de almacenamiento

Especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre de almacenamiento único.

Servicio de almacenamiento

Seleccione el servicio en la lista desplegable. La opción de configuración varía en función del servicio de almacenamiento que se haya seleccionado.

ID de la clave de acceso/Nombre de cuenta/ID de la consulta

Identifica el usuario que solicita acceso esta ubicación.

Para este campo, Amazon S3 utiliza el ID de la clave de acceso, Windows Azure y FUJITSU Hybrid IT Service FJcloud-O utilizan Nombre de cuenta y Eucalyptus-Walrus utiliza ID de la consulta.

Clave de acceso secreta/Clave secreta

Como la clave de acceso no está cifrada, esta clave de acceso secreta es una contraseña que se utiliza para verificar la autenticidad de la solicitud a fin de acceder a esta ubicación.

Importante: Esta clave de acceso secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave de acceso secreta en una página Web ni en otro código de origen accesible públicamente ni la transmita a través de canales no seguros.

Para este campo, Amazon S3 utiliza la Clave de acceso Secreta. Windows Azure, FUJITSU Hybrid IT Service FJcloud-O y Eucalyptus-Walrus utilizan Clave secreta.

Configuración proxy

Especifica la configuración del servidor proxy. Seleccione **Conectar utilizando un servidor proxy**para activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. Se debe proporcionar la información de autenticación correspondiente (Nombre de dominio\nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

Nota: La capacidad de proxy no está disponible para Eucalyptus-Walrus.

Nombre del depósito/contenedor

Todos los archivos y las carpetas movidas o copiadas al distribuidor de la nube se almacenan y se organizan en sus depósitos (o contenedores). Los depósitos son como un contenedor para los archivos y se utilizan para agrupar y organizar objetos conjuntamente. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

Para este campo, Amazon S3 y Eucalyptus-Walrus utilizan Nombre de depósito. Windows Azure y FUJITSU Hybrid IT Service FJcloud-O utilizan Contenedor.

Nota: Para finalizar este paso, todas las referencias a depósitos se pueden aplicar también a los contenedores a menos que se especifique otra cosa.

Zona de depósito

Se refiere a la región del depósito en Amazon y FUJITSU Hybrid IT Service FJcloud-O.

Número de contrato

Hace referencia al número de contrato que proporciona FUJITSU Hybrid IT Service FJcloud-O.

ID del proyecto

Hace referencia al ID del proyecto que genera FUJITSU Hybrid IT Service FJcloud-O.

Activar el almacenamiento de redundancia reducida

Para Amazon S3 solamente, esta opción permite la selección para activar el almacenamiento de redundancia reducida (RRS). RRS es una opción de almacenamiento de Amazon S3 que facilita la reducción de costes a través del almacenamiento de datos no críticos y reproducibles a niveles de redundancia más bajos que el almacenamiento estándar de Amazon S3. Ambas opciones de almacenamiento de redundancia estándares y reducidas almacenan datos en diferentes funcionalidades y dispositivos, pero con RRS los datos se replican menos veces, de modo que el coste es menor. Se debería esperar la misma latencia y rendimiento mediante el almacenamiento estándar de Amazon S3 o RRS. De forma predeterminada, esta opción no está seleccionada (Amazon S3 utiliza la opción de almacenamiento estándar).

4. Haga clic en **Probar conexión** para verificar la conexión a la ubicación de la nube especificada.
5. Haga clic en **Aceptar**.

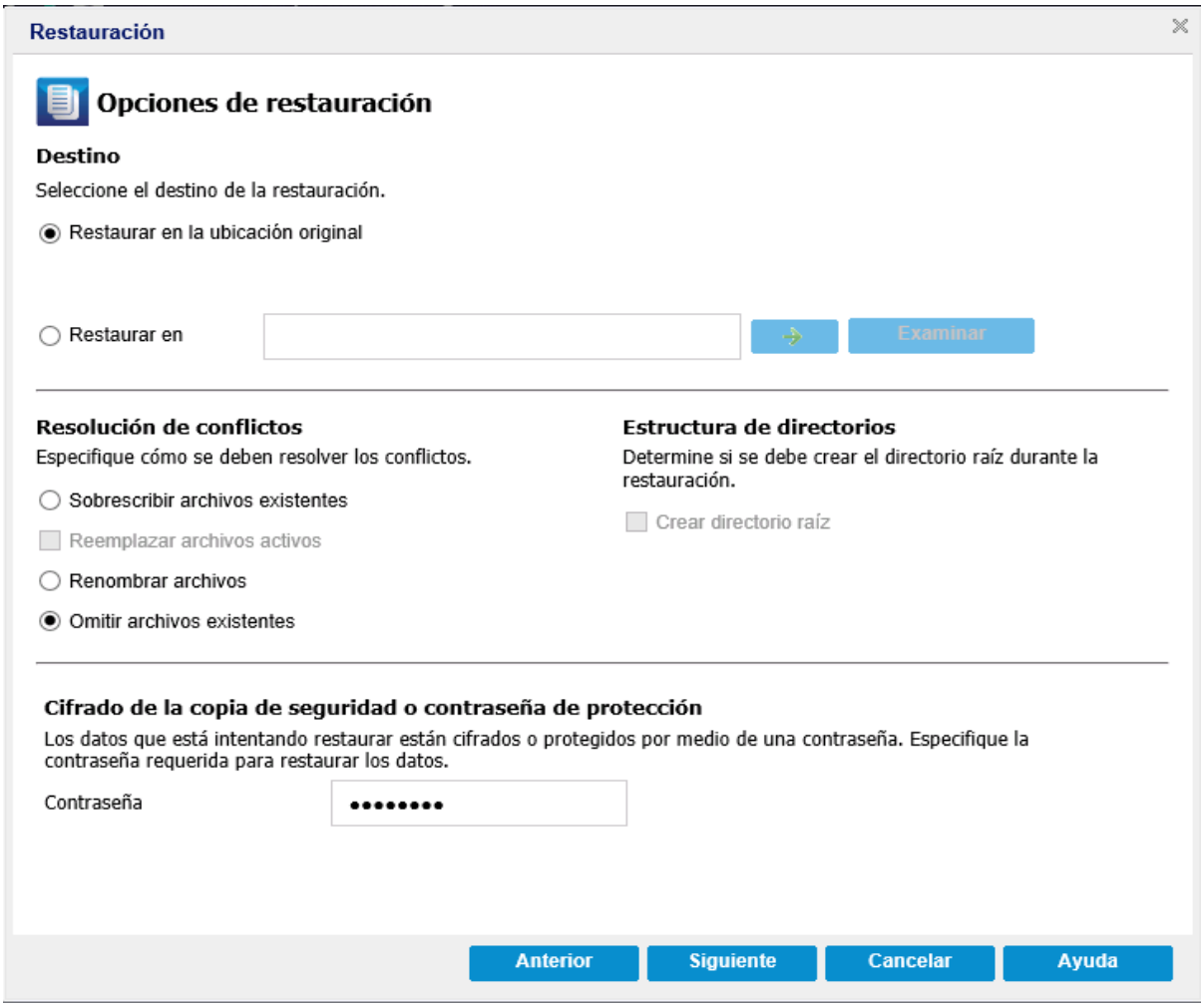
   La cuenta de la nube se agrega a la consola.

Definición de las opciones de restauración

Después de especificar la información de la copia de archivo que se debe restaurar, defina las opciones de copia para la copia de archivo y el contenido seleccionados.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, seleccione el destino para la restauración.



A continuación se especifican las opciones de destino disponibles:

Restaurar en la ubicación original

Restaura en la ubicación original desde la que se ha capturado la imagen de copia de seguridad.

Restaurar en

Restaura en la ubicación especificada. Se puede hacer clic en el botón de la flecha verde para comprobar la conexión con la ubicación especificada. Si es necesario, también puede escribir las credenciales de nombre de usuario y de contraseña para obtener acceso a dicha ubicación.

2. En **Resolución de conflictos**, especifique la opción correspondiente a la acción que deberá realizar Arcserve UDP si se encuentran conflictos durante el proceso de restauración.

   A continuación se especifican las opciones disponibles:

   Sobrescribir archivos existentes

   Sobrescribe (reemplaza) todos los archivos existentes que se encuentran en el destino de restauración. Todos los objetos se restaurarán desde los archivos de copia de seguridad, independientemente de si actualmente se encuentran en el equipo.

   Reemplazar los archivos activos

   Reemplaza todos los archivos activos después del reinicio. Si durante el intento de restauración, el Agente de Arcserve UDP para Windows detecta que el archivo existente está actualmente en uso o que algún usuario está accediendo al archivo, no sustituye ese archivo de forma inmediata, sino que retrasa la sustitución de los archivos activos hasta que se reinicie de nuevo el equipo con el fin de evitar problemas. (La restauración ocurrirá de forma inmediata pero los archivos activos se sustituirán a partir del reinicio siguiente).

   Esta opción solamente está disponible si selecciona la opción **Sobrescribir archivos existentes**.

   Nota: Si no se selecciona esta opción, se omite de la restauración cualquier archivo activo.

   Cambiar el nombre de los archivos

   Si el nombre de archivo ya existe, crea un archivo nuevo. Al seleccionar esta opción se copiará el archivo de origen en el destino con el mismo nombre de archivo pero con una extensión diferente. A continuación, los datos se restaurarán en un archivo nuevo.

   Omitir archivos existentes

Omite y no sobrescribe (reemplaza) ningún archivo existente que se encuentre en el destino de restauración. Solo se restaurarán desde los archivos de copia de seguridad los objetos que no estén en el equipo actualmente.

Valor por omisión: Omitir archivos existentes

3. Especifique la **Estructura de directorios** para crear un directorio raíz durante la restauración.

Crear directorio raíz

Especifica que si existe una estructura de directorio raíz en la imagen de copia de seguridad capturada, Arcserve UDP recreará la misma estructura de directorio raíz en la ruta de destino de la restauración.

Si no se selecciona esta opción, el archivo o carpeta se restaurará directamente en la carpeta de destino.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt" y "C:\Folder1\SubFolder2\B.txt" y durante la restauración ha especificado como destino de la restauración "D:\Restore".

- Si ha seleccionado la restauración de los archivos "A.txt" y "B.txt" de manera individual, el destino de los archivos restaurados será "D:\Restore\A.txt" y "D:\Restore\B.txt" (no se recreará el directorio raíz anterior en el nivel de archivo especificado).
- Si se selecciona la restauración desde el nivel "Subcarpeta2", el destino para los archivos restaurados será "D:\Restore\SubFolder2\A.txt" y "D:\Restore\SubFolder2\B.txt" (el directorio raíz superior al nivel de carpeta especificada no se recreará).

Con esta opción seleccionada, la ruta completa de directorio raíz para los archivos/carpetas (incluyendo el nombre de volumen) se recrea en la carpeta de destino. Si los archivos o carpetas que deben restaurarse provienen del mismo nombre de volumen, la ruta del directorio raíz de destino no incluirá el nombre del volumen. Sin embargo, si los archivos o carpetas que deben restaurarse provienen de diferentes nombres de volúmenes, la ruta del directorio raíz de destino incluirá el nombre de volumen.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", y también E:\Folder3\SubFolder4\C.txt", y durante la restauración ha especificado el destino de restauración como "D:\Restore".

- Si ha seleccionado la restauración únicamente del archivo "A.txt", el destino para el archivo restaurado será "D:\Restore\ Folder1\SubFolder2\A.txt" (se recreará todo el directorio raíz sin el nombre de volumen).

- Si ha seleccionado la restauración tanto del archivo "A.txt" como del archivo "C.txt", el destino para los archivos restaurados será "D:\Restore\C\ Folder1\SubFolder2\A.txt" y "D:\Restore\ E\Folder3\SubFolder4\C.txt" (se recreará todo el directorio raíz con el nombre de volumen).

4. Especifique la contraseña de cifrado en **Contraseña de cifrado de copia de archivo**.
5. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Resumen de la restauración**.

   Las opciones de restauración se han definido para restaurar desde una copia de archivo.

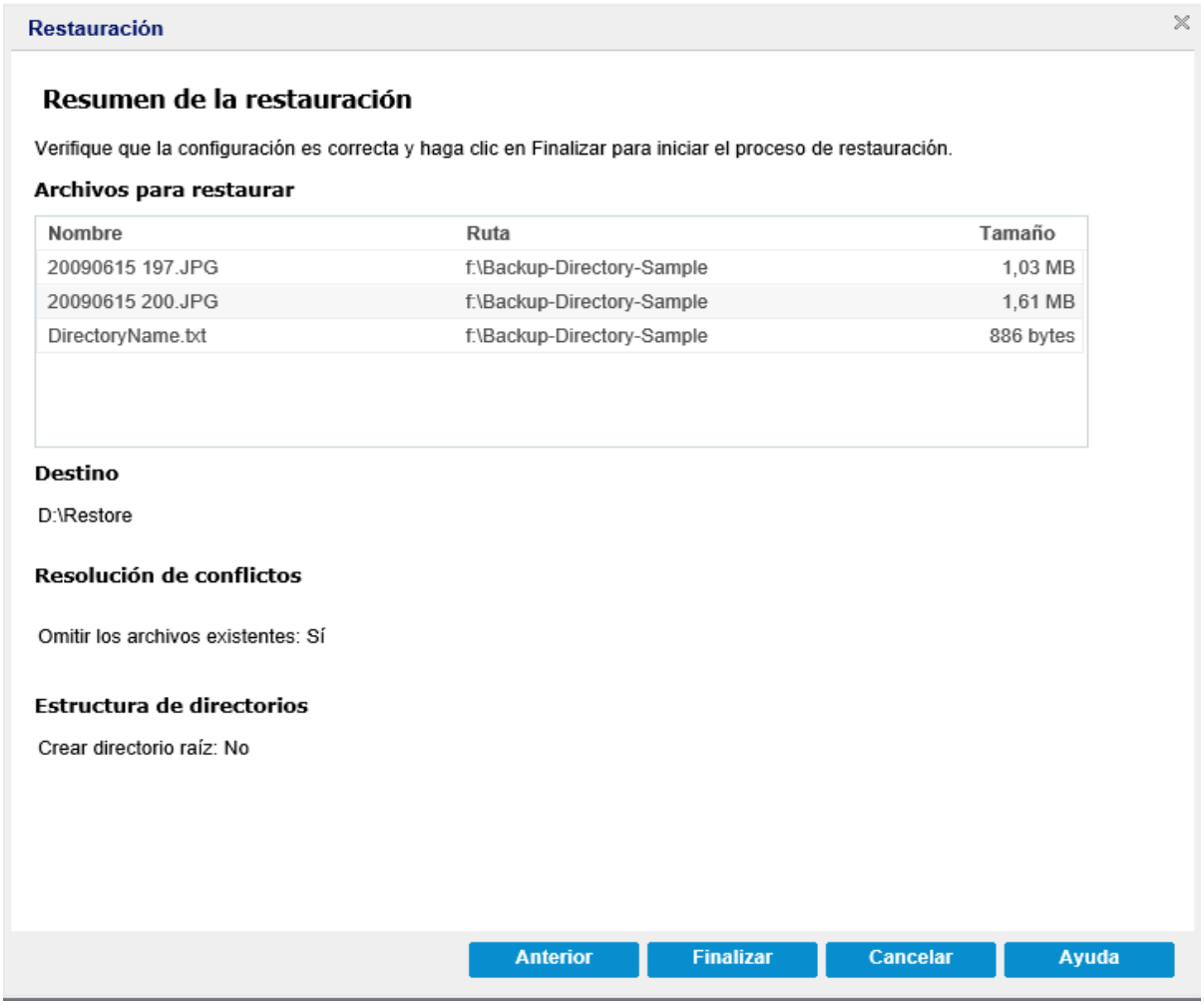
Restauración del contenido del punto de recuperación

Después de definir las opciones de restauración, verifique que los valores de configuración sean correctos y confirme el proceso de restauración. El **Resumen de la restauración** le ayuda a revisar todas las opciones de la restauración definidas y a modificarlas si es necesario.

Siga estos pasos:

1. En el cuadro de diálogo **Resumen de la restauración**, revise la información que aparece en pantalla para verificar que todas las opciones de restauración y los valores

de configuración sean correctos.



- Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para cambiar el valor de configuración incorrecto.
- Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar el proceso de restauración.

El contenido de la copia de archivo se restaura.

Verificación de que se ha restaurado el contenido

Después de la terminación del proceso de restauración, verifique que el contenido se ha restaurado en el destino especificado.

Siga estos pasos:

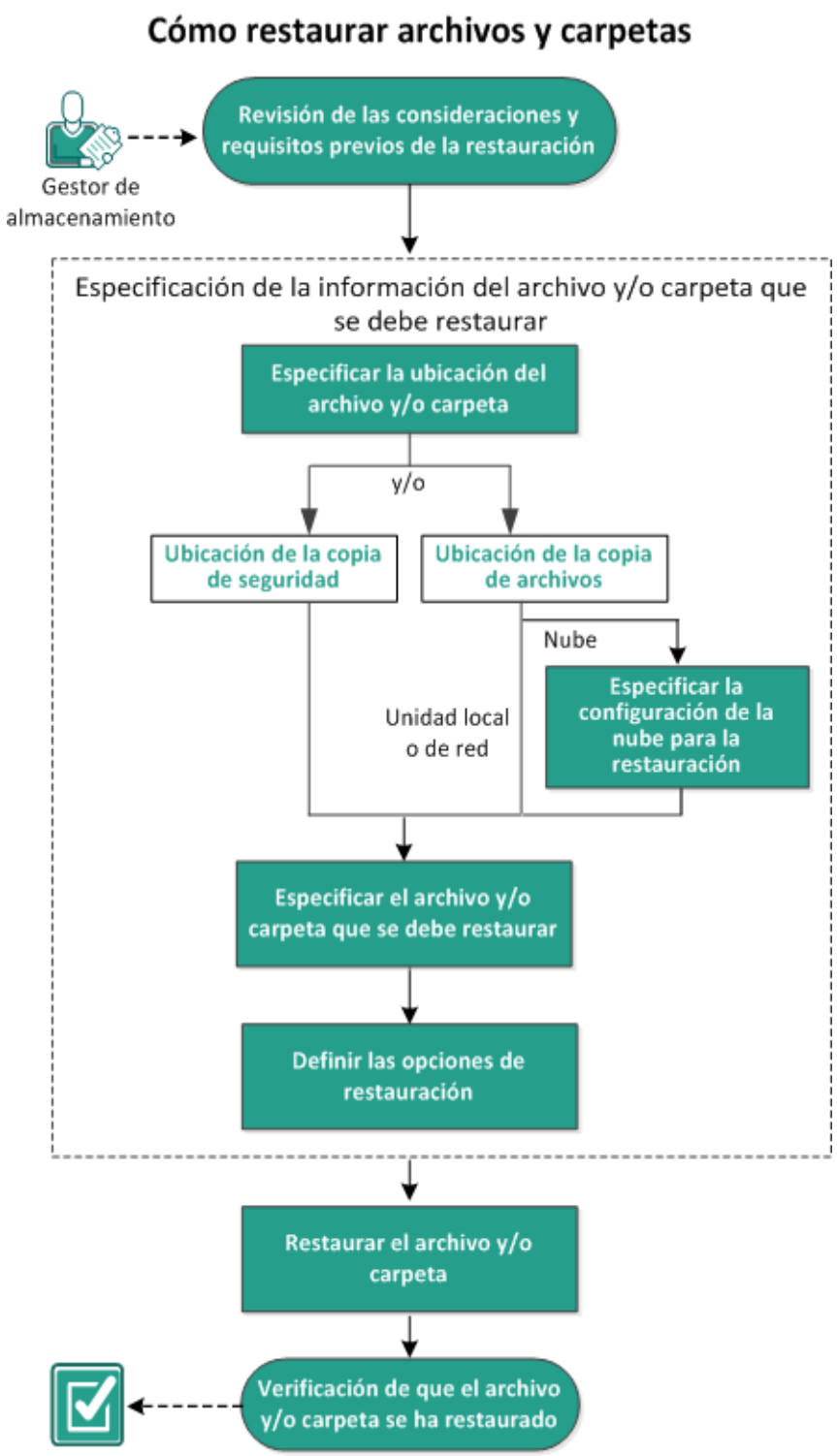
1. Inicie sesión en el buzón de correo de destino.
2. Compruebe que existe el elemento del buzón de correo que se ha restaurado.
3. Verifique el contenido restaurado.

   El contenido restaurado se ha verificado correctamente.

Cómo restaurar archivos y carpetas

Siempre que Arcserve UDP realiza una copia de seguridad correcta, todos los archivos o carpetas de los que se ha hecho una copia de seguridad se incluyen en una imagen de instantánea de la copia de seguridad. Este método de restauración permite especificar exactamente los archivos y carpetas que se desea restaurar.

El diagrama siguiente ilustra el proceso para restaurar archivos y carpetas específicos:



Realice las tareas siguientes para restaurar archivos y carpetas:

1. Revisión de las consideraciones y requisitos previos de la restauración
2. Especificación de la información del archivo y/o carpeta que se debe restaurar

a. Especificación de la ubicación del archivo y/o carpeta
    - Especificación de la configuración de la nube para la restauración
b. Especificación del archivo y/o carpeta que se debe restaurar
c. Definición de las opciones de restauración

3. Restauración del archivo y/o carpeta
4. Verificación de que el archivo y/o carpeta se ha restaurado

Revisión de las consideraciones y requisitos previos de la restauración

Verifique que los requisitos previos siguientes existen antes de realizar una restauración:

- Como mínimo, existe una versión de la copia de archivo o de la copia de seguridad disponible para restaurarla.
- Tiene un destino de la copia de archivo o de la copia de seguridad válido y accesible desde el que restaurar el contenido de la copia de archivo o de la copia de seguridad.
- Tiene una ubicación de destino válida y accesible a la que poder restaurar el contenido de la copia de archivo o de la copia de seguridad.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones sobre la restauración:

- Para un punto de recuperación sin un catálogo del sistema de archivos creado, para garantizar que se puede explorar y seleccionar archivos/carpetas para restaurar desde la interfaz de usuario, se debe conceder acceso a la cuenta/grupo a todas las carpetas y archivos en todos los volúmenes con el acceso de lectura/lista antes de realizar la copia de seguridad.

  El grupo del sistema local (SYSTEM) o el grupo de los administradores integrado (BUILTIN\Administrators) se debe agregar a la lista de control de acceso de las carpetas para que el Agente de Arcserve UDP (Windows) pueda explorar una copia de seguridad que no tenga un catálogo del sistema de archivos creado. De lo contrario, el Agente de Arcserve UDP (Windows) no podrá explorar las carpetas desde la interfaz de usuario de restauración.
- (Opcional) Debe entender cómo funciona el proceso de restauración. Para obtener más información, consulte Cómo funciona la restauración de nivel de archivo.

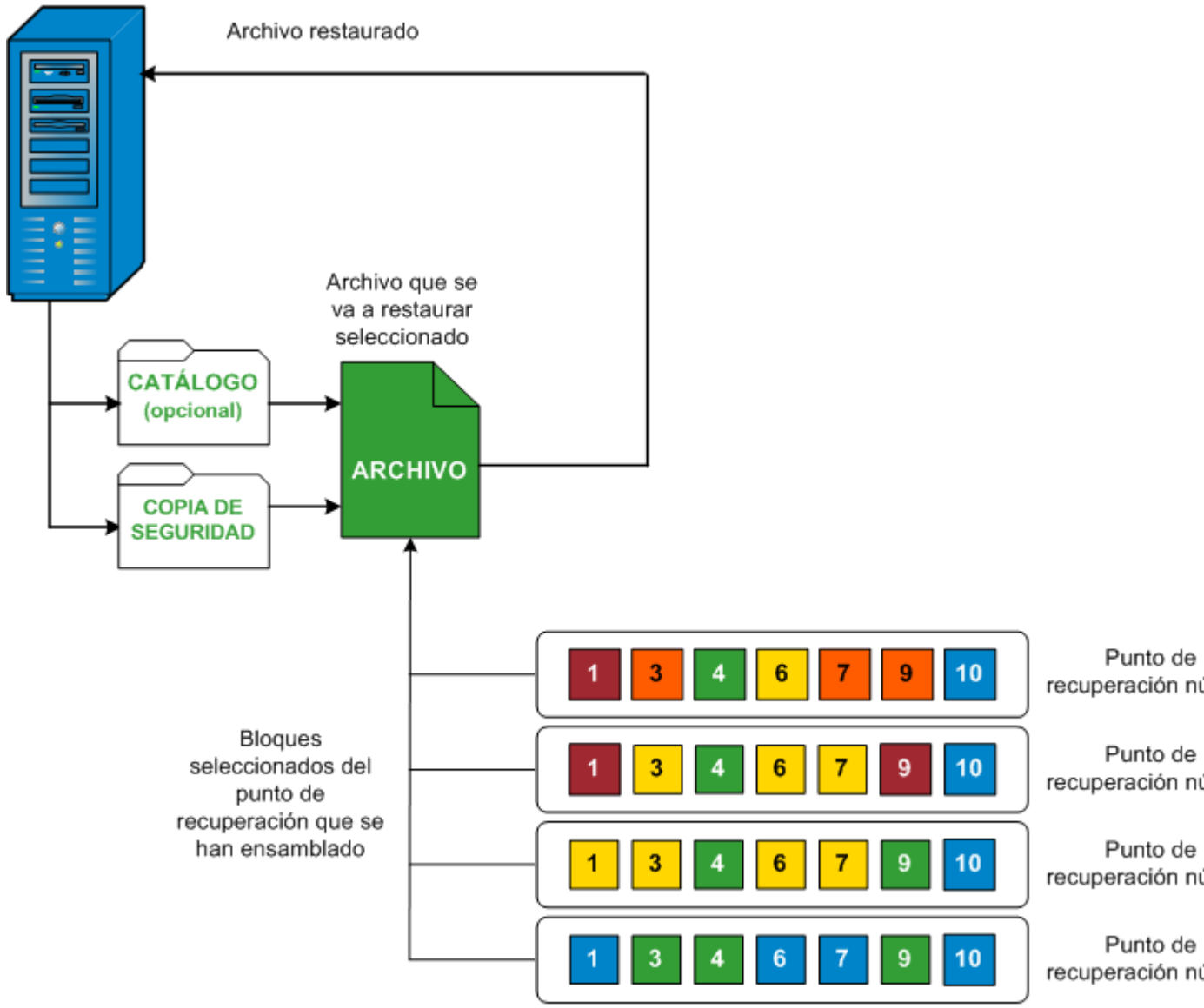
  Nota: El proceso para restaurar desde una ubicación de copia de archivo es similar a restaurar desde una ubicación de copia de seguridad.
- (Opcional) Revise los archivos que se han omitido durante la restauración. Para obtener más información, consulte Archivos omitidos durante la restauración.

Cómo funciona la restauración de nivel de archivo

Durante una copia de seguridad de nivel de bloque, cada archivo con copia de seguridad está compuesto por una recopilación de bloques que definen el archivo en particular. Si necesita restaurar un archivo en particular, puede buscar la copia de seguridad y seleccionar el archivo que desea restaurar y el punto de recuperación desde el cual desea empezar a restaurar. A continuación, el Agente de Arcserve UDP (Windows) recopilará la versión de los bloques que se han utilizado para el punto de recuperación del archivo especificado, volverá a unir el archivo y lo restaurará.

Nota: Cuando se especifican los valores de configuración de la copia de seguridad, tiene una opción para crear un catálogo del archivo durante la copia de seguridad. Este catálogo del archivo permite buscar las sesiones de copia de seguridad de una forma más rápida durante la restauración. Si elige no crear el catálogo durante la copia de seguridad, todavía se puede crear más tarde.

El diagrama de flujo siguiente muestra el proceso de cómo Arcserve UDP restaura un archivo específico.


Archivo restaurado
Archivo que se va a restaurar seleccionado
CATÁLOGO (opcional)
COPIA DE SEGURIDAD
ARCHIVO
Bloques seleccionados del punto de recuperación que se han ensamblado
1 3 4 6 7 9 10
1 3 4 6 7 9 10
1 3 4 6 7 9 10
1 3 4 6 7 9 10
Punto de
Punto de
Punto de
Punto de

Archivos omitidos durante la restauración

Mientras el Agente de Arcserve UDP (Windows) realiza una restauración, algunos archivos se pueden omitir intencionadamente.

Se omiten los archivos y las carpetas en la tabla siguiente durante una restauración si se dan las dos condiciones siguientes:

- Se omiten archivos cuando existen tales archivos antes de la restauración y la opción de conflicto es Omitir archivos existentes.
- Se omiten archivos y carpetas que aparecen en la tabla siguiente porque no son un componente importante para Windows o para el Agente de Arcserve UDP (Windows).

SO	Carpeta o ubicación	Nombre del archivo o de la carpeta	Observaciones
Todo	Carpeta Root de cada volumen	CAVolTrc.dat	Utilizado por el controlador de seguimiento de Arcserve UDP.
		cavoltrcsnapshot.dat	
		Información acerca del volumen del sistema*	Utilizado para guardar archivos/carpetas por un sistema Windows, por ejemplo, archivos de instantánea de volumen.
		RECYCLER*	Utilizado solamente en particiones de NTFS. Contiene una papelera de reciclaje para todos los usuarios que se conecten al equipo, que se ordenarán en función del identificador de seguridad (SID).
		$Recycle.Bin*	Cuando se suprime un archivo en el explorador de Windows NT o Mi PC, el archivo se almacena en la Papelera de reciclaje hasta que se vacíe la Papelera de reciclaje o se restaure el archivo.
	Cualquier carpeta puede contener archivos de imagen	Thumbs.db	Almacena pequeñas imágenes para la vista en miniatura del Explorador de Windows.
	Carpeta Root del volumen	PageFile.sys	El archivo de intercambio de memoria virtual de Windows.
		Hiberfil.sys	Se trata del archivo de hibernación, que se utiliza para guardar los datos del sistema cuando un equipo se establece en el modo de hibernación.

Se omiten los archivos y las carpetas siguientes solamente cuando se restaura en la ubicación original o en otra ubicación:

SO	Carpeta o ubicación	Nombre del	Observaciones

		archivo o de la carpeta	
Todo	Carpeta especificada en el registro de valor que se encuentra en: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Todos los archivos/carpetas (recursivamente)	La carpeta contiene un archivo dll en memoria caché que se utiliza para el Comprobador de archivos de sistema (SFC) y el contenido del directorio dll en memoria caché del sistema se reconstruye mediante SFC.
	%SystemRoot%\SYSTEM32\dllCache		
	Carpeta Root de quorum_device	MSCS*	Utilizado para Microsoft Cluster Server.
	%SystemRoot%\SYSTEM32\	perf?00?.dat	Los datos de rendimiento utilizados por el contador de rendimiento de Windows.
		perf?00?.bak	
		CATROOT*	Utilizado para las firmas digitales de registros de la protección de archivos de Windows (WFP) del sistema operativo instala archivos como DLL, EXE, SYS, OCX, etc. para evitar y proteger su supresión o sustitución por versiones anteriores.
	%SystemRoot%\inetsrv\	metabase.bin	El archivo binario metabase de las versiones de IIS anteriores a 6.0.
	Archivo o carpeta especificados en el valor excepto almacenamiento común de SIS en	Todos los archivos/carpetas	No se debe realizar copia de

	HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup	(recursivamente)	seguridad ni acciones de restauración para archivos y/o carpetas. Para obtener más información, consulte este vínculo.
XP W2003	Volumen del sistema	NTLDR	El cargador de arranque principal.
		BOOT.INI	Contiene la configuración de arranque (si esta falta, NTLDR establecerá \Windows como predeterminado en la primera partición de la primera unidad de disco duro).
		NTDETECT.COM	Necesario para iniciar un sistema operativo de NT. Detecta información de hardware básica que es necesaria para un arranque correcto.
Vista y posteriores	Carpeta Root del volumen del sistema	boot*	Carpeta Boot para Windows.
		bootmgr	Archivo del gestor de arranque de Windows.
		EFI\Microsoft\Boot*	Utilizado para el arranque de EFI.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Almacena los archivos de seguimiento de ETW (extensión .etl) para las sesiones de seguimiento

			de eventos en tiempo real.
		con-fig\RegBack*	Copia de seguridad de la tabla de registro actual.
Win8 y posteriores	Volumen del sistema	swapfile.sys	El archivo de controlador del sistema, normalmente alrededor de 256 MB. Utilizado por las aplicaciones de estilo Metro que no se ajustan a las características de paginación tradicionales (como patrón de uso, crecimiento, reserva de espacio) de pagefile.sys.
		BOOTNXT	Utilizado para iniciar el sistema operativo, distinto de Windows 8. Creado para activar las opciones de inicio y actualizado por Windows.

El registro de actividad proporciona la siguiente información:

- Información sobre la hora y la fecha: se omiten los archivos del sistema jobxxxx. Se puede utilizar la opción de recuperación completa (BMR) para restaurarlos.
- Información sobre la hora y la fecha: se omiten los archivos o directorios jobxxxx. Los archivos y directorios omitidos están disponibles en C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\Logs\Restore-<AAAAMMDD>-<hhmmss>-<ID del proceso>-<ID de la tarea>.log.

Especificación de la información del archivo y/o carpeta que se debe restaurar

Arcserve UDP proporciona una opción para buscar y restaurar un archivo o carpeta específicos. El objetivo de ejecutar una tarea de restauración correcta es de identificar los datos necesarios de forma rápida y de recuperarlos desde la ubicación de copia de seguridad correspondiente. Cada tarea de restauración necesita un origen y un destino.

El proceso implicado en la restauración busca archivos y/o carpetas tal y como se muestra a continuación:

1. Especificación de la ubicación del archivo y/o carpeta
    - Especificación de la configuración de la nube para la restauración
2. Especificación del archivo y/o carpeta que se debe restaurar
3. Definición de las opciones de restauración

Especificación de la ubicación del archivo y/o carpeta

Utilice la opción **Buscar archivos/carpetas** para restaurar archivos y carpetas. Este método de restauración permite especificar exactamente qué archivos y carpetas desean restaurarse.

Siga estos pasos:

1. Acceda al cuadro de diálogo Selección del método de recuperación de una de las formas siguientes:

   Desde Arcserve UDP:

   a. Inicie sesión en Arcserve UDP.

   b. Haga clic en la ficha **recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos agregados en el panel central.

   d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   e. Haga clic en **Restaurar** de la opción desplegable **Acción**.

      El cuadro de diálogo Selección del método de restauración se abre.

      Nota: Se inicia sesión automáticamente en el nodo del Agente y el cuadro de diálogo Selección del método de restauración se abre desde el nodo del Agente.

   Desde el Agente de Arcserve UDP (Windows):

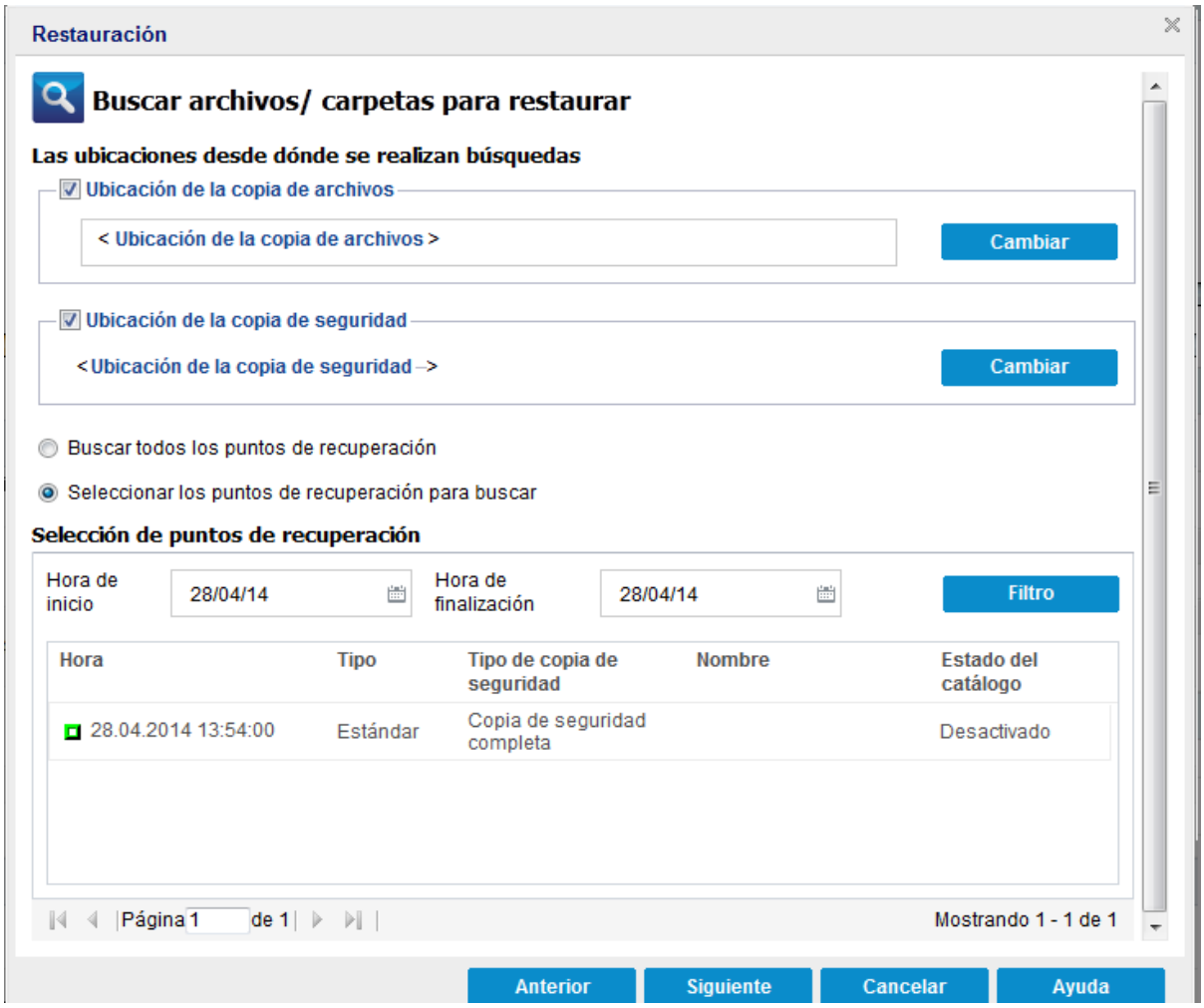
   a. Inicie sesión en el Agente de Arcserve UDP (Windows).

   b. En la página principal, seleccione **Restaurar**.

   El cuadro de diálogo Selección del método de restauración se abre.

2. Haga clic en la opción **Buscar archivos/carpetas para restauración**.

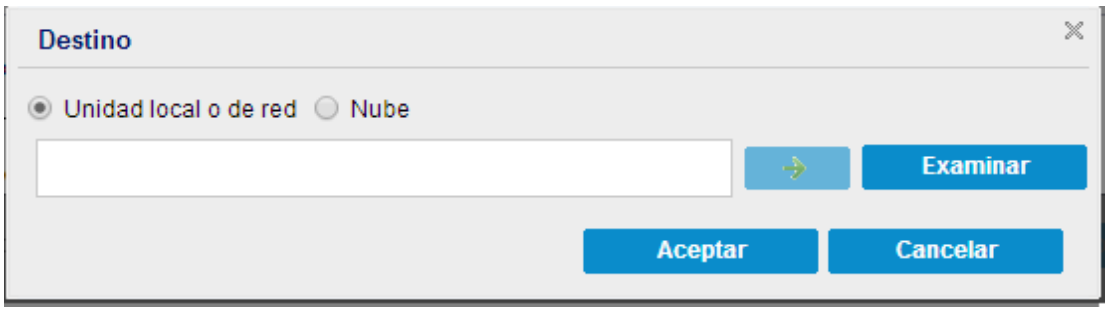
   Aparecerá el cuadro de diálogo **Buscar archivos/carpetas para restauración**.



3. Seleccione la casilla de verificación **Ubicación de la copia de archivo** y haga clic en el botón **Cambiar** para modificar la ubicación de búsqueda al destino donde están almacenadas las imágenes de la copia de archivo.

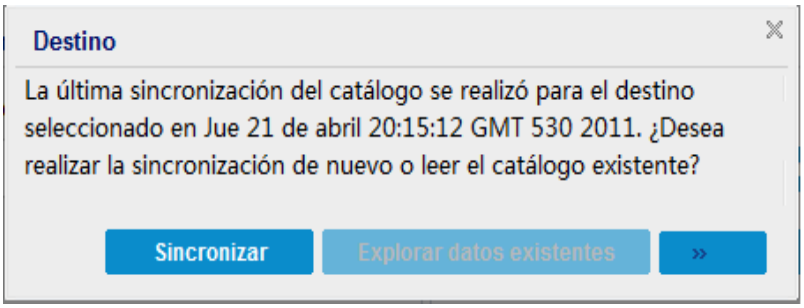
   Se abrirá el cuadro de diálogo **Destino** y se podrá seleccionar **Unidad local o de red** o **Nube**.

   Nota: De forma predeterminada, los campos **Ubicación de la copia de seguridad** y **Ubicación de la copia de archivo** muestran la ruta correspondiente utilizada para los destinos de copia de seguridad y de copia de archivo más recientes.



- Si selecciona **Unidad local o de red**, especifique una ubicación o vaya a la ubicación donde se almacenan las imágenes de copia de archivo.
- Es posible hacer clic en el icono de validación de la flecha verde para garantizar el acceso adecuado a la ubicación de origen.
- Si selecciona **Nube**, especifique una ubicación de la nube o haga clic en el botón **Configurar** para mostrar el cuadro de diálogo **Configuración de la nube**. Para obtener más información, consulte Cómo especificar la configuración de la nube para la restauración.

  Sin tener en cuenta si se ha seleccionado la restauración desde una **Unidad local o de red** o desde la **Nube**, cuando se cambia el destino a una ubicación alternativa aparece un cuadro emergente que pregunta si desea realizar una nueva sincronización del catálogo o leer desde el catálogo existente.



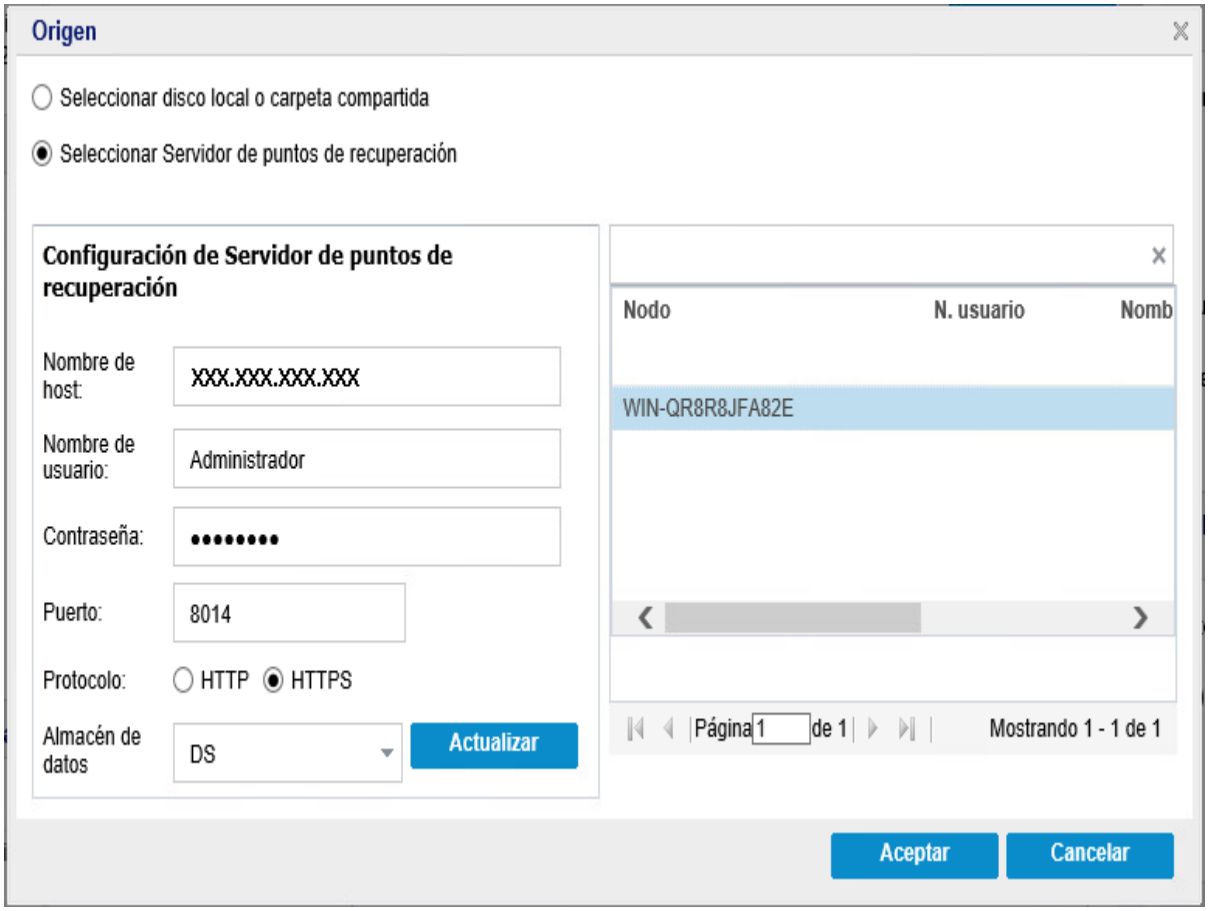
  - Si se está realizando una sincronización del catálogo por primera vez, el botón **Explorar datos existentes** se desactivará porque el catálogo de copia de archivo no existe localmente.
  - Si se ha realizado previamente una sincronización de catálogo, este cuadro de diálogo mostrará los detalles sobre la última vez que se sincronizó el catálogo desde este destino. Si se ejecutan más tareas de copia de archivo después de ese momento, puede que el catálogo no esté sincronizado; para ello se puede seleccionar la opción **Sincronizar** para asegurarse de que el catálogo de copia de archivo está actualizado.

    1. Haga clic en **Sincronizar** para descargar el catálogo de copia de archivo del destino de copia de archivo especificado al equipo local para que la exploración sea más rápida.

    2. Haga clic en **Explorar datos existentes** para usar el catálogo de copia de archivo que está disponible localmente y no tener que descargar o sincronizar otra vez.

4. Seleccione la casilla de verificación **Ubicación de la copia de seguridad** y haga clic en **Cambiar** para modificar la ubicación de la copia de seguridad.

El cuadro de diálogo **Origen** se abre donde se puede seleccionar la ubicación de la copia de seguridad.



5. Seleccione una de las siguientes opciones en el cuadro de diálogo **Origen**:

   Seleccionar disco local o carpeta compartida

   a. Especifique o vaya a la ubicación donde se almacenan las imágenes de copia de seguridad y seleccione el origen de la copia de seguridad adecuado.

      Se puede hacer clic en el botón de la flecha verde para comprobar la conexión con la ubicación especificada. Si es necesario, también puede escribir las credenciales de Nombre de usuario y Contraseña para obtener acceso a dicha ubicación de origen.

      El cuadro de diálogo **Selección de la ubicación de la copia de seguridad** se abre.

   b. Seleccione la carpeta en la cual se almacenan los puntos de recuperación y haga clic en **Aceptar**.

El cuadro de diálogo **Selección de la ubicación de la copia de seguridad** se cierra y se puede ver la ubicación de la copia de seguridad en el cuadro de diálogo **Origen**.

c. Haga clic en **Aceptar**.

Los puntos de recuperación se clasifican en el cuadro de diálogo **Buscar archivos/carpetas para restaurar**.

Seleccionar servidor de puntos de recuperación

a. Especifique los detalles del valor de configuración del servidor de puntos de recuperación y haga clic en **Actualizar**.

Todos los agentes se muestran en la columna **Agente de protección de datos** en el cuadro de diálogo **Origen**.

b. Seleccione el agente de la lista mostrada y haga clic en **Aceptar**.

Los puntos de recuperación se clasifican en el cuadro de diálogo **Buscar archivos/carpetas para restaurar**.

Nota: Si se selecciona un agente diferente y si los puntos de recuperación están cifrados, entonces se tiene que proporcionar la contraseña de cifrado cuando se le solicite.

6. Seleccione una de las opciones siguientes para buscar puntos de recuperación:

Buscar todos los puntos de recuperación

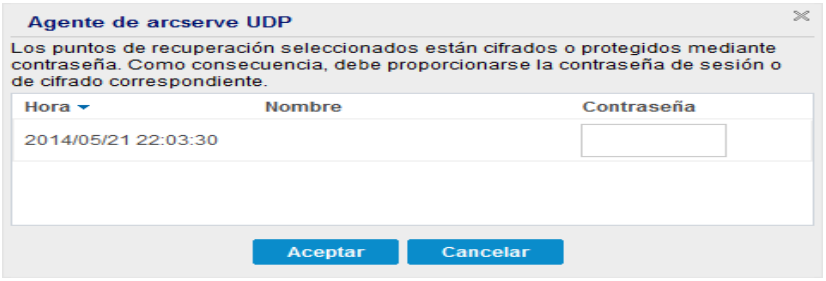
Busca el archivo o carpeta en todos los puntos de recuperación almacenados en la ubicación proporcionada. Se tiene que especificar el archivo o carpeta que se desea buscar en el cuadro de diálogo **Buscar archivos/carpetas para restaurar**.

Seleccionar los puntos de recuperación para buscar

Muestra los puntos de recuperación durante el período de tiempo especificado. Se puede especificar la hora de inicio y la hora de finalización y, a continuación, seleccionar el punto de recuperación en un período de tiempo especificado.

7. Seleccione el punto de recuperación y haga clic en **Siguiente**.

Nota: Si se ha seleccionado un agente diferente en el cuadro de diálogo **Origen** y si los puntos de recuperación están cifrados, entonces se abrirá el cuadro de diálogo de cifrado. Proporcione la contraseña y haga clic en **Aceptar**.



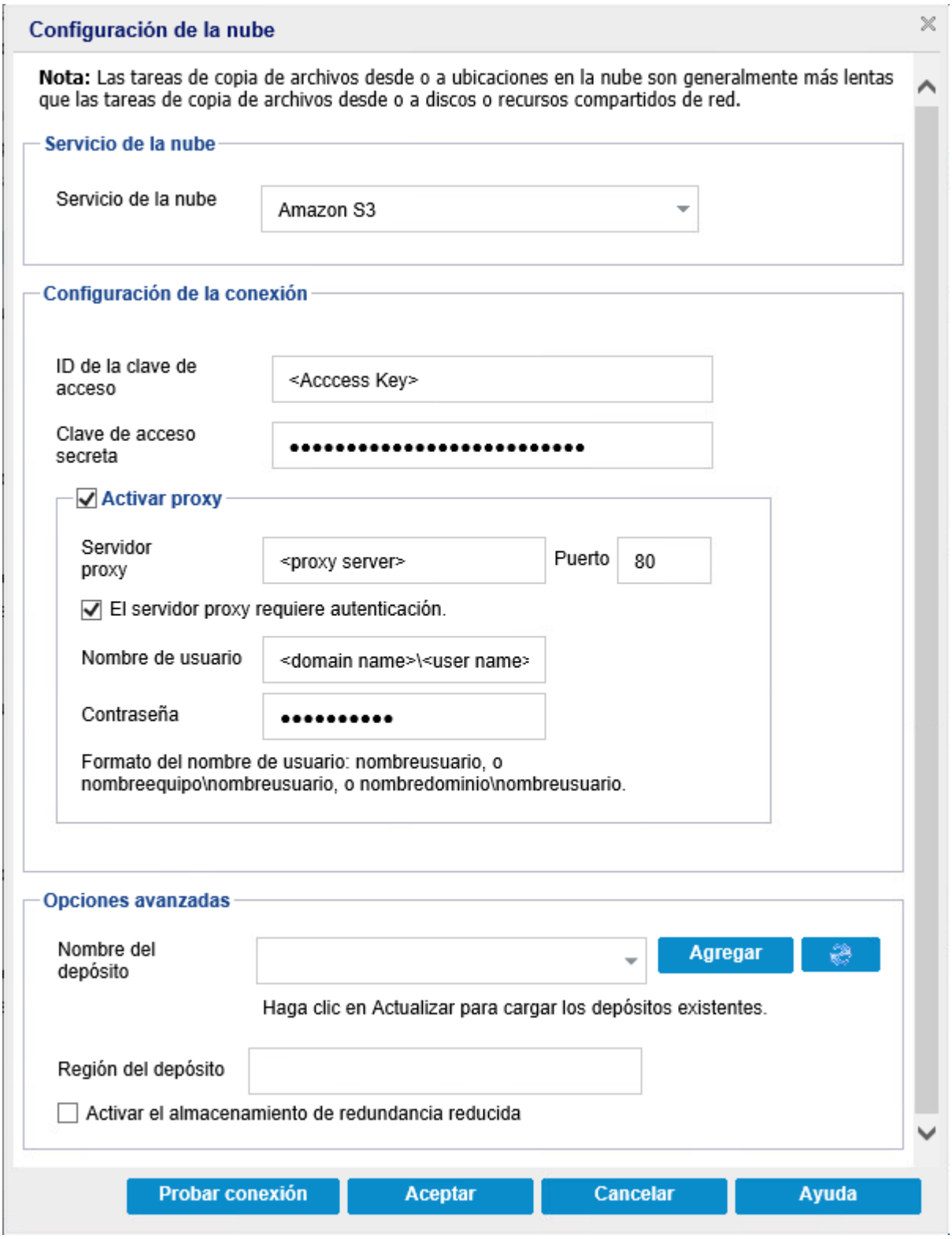
Aparecerá el cuadro de diálogo **Buscar archivos/carpetas para restauración**.

Se especifica la ubicación de la **copia de seguridad o de la copia de archivo**.

Especificación de la configuración de la nube para la restauración

Nota: El procedimiento siguiente solamente se aplica si se está restaurando un archivo o carpeta desde una ubicación de la nube de la copia de archivo.

Desde la opción **Explorar copias de archivo** o **Buscar archivos/carpetas para la restauración**, haga clic en el botón **Configurar** para mostrar el cuadro de diálogo **Configuración de la nube**.



Siga estos pasos:

1. En el cuadro de diálogo **Configuración de la nube**, utilice el menú desplegable para seleccionar desde qué tipo de distribuidor de la nube se desea restaurar. Las opciones disponibles son **Amazon S3**, **Windows Azure**, **FUJITSU Hybrid IT Service**

FJcloud-O y **Eucalyptus-Walrus**. (**Amazon S3** es el distribuidor predeterminado). Para obtener más información sobre Fujitsu Cloud (Windows Azure) y FUJITSU Hybrid IT Service FJcloud-O, consulte las secciones Descripción general y Registro.

Nota: Después de codificar el nombre del depósito, si la longitud de la ruta es superior a 170 caracteres, Eucalyptus-Walrus no podrá copiar archivos.

2. Especifique las **Opciones de configuración**.

   Las opciones de configuración para cada distribuidor de la nube son similares (con una terminología diferente) y se describe cualquier diferencia patente.

   a. Especifique la **Configuración de conexión**:

      URL del distribuidor

      Identifica la dirección URL del proveedor de la nube.

      Para Amazon S3 y Windows Azure, la dirección URL del suministrador se rellena automáticamente de forma previa. Para Eucalyptus-Walrus, las direcciones URL del distribuidor se deberán introducir manualmente mediante el formato especificado.

      ID de la clave de acceso/Nombre de cuenta/ID de la consulta

      Identifica el usuario que solicita acceso esta ubicación.

      Para este campo, Amazon S3 utiliza el ID de la clave de acceso, Windows Azure y FUJITSU Hybrid IT Service FJcloud-O utilizan Nombre de cuenta y Eucalyptus-Walrus utiliza ID de la consulta.

      Clave de acceso secreta/Clave secreta

      Como la clave de acceso no está cifrada, esta clave de acceso secreta es una contraseña que se utiliza para verificar la autenticidad de la solicitud a fin de acceder a esta ubicación.

      Importante: Esta clave de acceso secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave de acceso secreta en una página Web ni en otro código de origen accesible públicamente ni la transmita a través de canales no seguros.

      Para este campo, Amazon S3 utiliza la Clave de acceso Secreta. Windows Azure, FUJITSU Hybrid IT Service FJcloud-O y Eucalyptus-Walrus utilizan Clave secreta.

      Activar proxy

      Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el

servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. Se debe proporcionar la información de autenticación correspondiente (nombre de usuario y contraseña) necesaria para utilizar el servidor proxy.

(La capacidad de proxy no está disponible para Eucalyptus-Walrus).

b. Especifique la **Configuración avanzada**:

Nombre del depósito/contenedor

Todos los archivos y las carpetas movidas o copiadas al distribuidor de la nube se almacenan y se organizan en sus depósitos (o contenedores). Los depósitos son como un contenedor para los archivos y se utilizan para agrupar y organizar objetos conjuntamente. Todos los objetos almacenados en el distribuidor de la nube se colocan en un depósito.

Seleccione un nombre de depósito de la lista desplegable. Si es necesario, se puede hacer clic en el botón **Actualizar** para actualizar la lista de depósitos disponibles.

Para este campo, Amazon S3 y Eucalyptus-Walrus utilizan Nombre de depósito. Windows Azure y FUJITSU Hybrid IT Service FJcloud-O utilizan Contenedor.

Zona de depósito

Se refiere a la región del depósito en Amazon y FUJITSU Hybrid IT Service FJcloud-O.

Número de contrato

Hace referencia al número de contrato que proporciona FUJITSU Hybrid IT Service FJcloud-O.

ID del proyecto

Hace referencia al ID del proyecto que genera FUJITSU Hybrid IT Service FJcloud-O.

Activar el almacenamiento de redundancia reducida

Para Amazon S3 solamente, esta opción permite la selección para activar el almacenamiento de redundancia reducida (RRS). RRS es una opción de almacenamiento de Amazon S3 que facilita la reducción de costes a través del almacenamiento de datos no críticos y reproducibles a niveles de redundancia más bajos que el almacenamiento estándar de Amazon S3. Ambas opciones de almacenamiento de redundancia estándares y reducidas almacenan datos en diferentes funcionalidades y dispositivos, pero con RRS los datos se replican menos veces, de modo que el coste es

menor. Se debería esperar la misma latencia y rendimiento mediante el almacenamiento estándar de Amazon S3 o RRS. De forma pre-determinada, esta opción no está seleccionada (Amazon S3 utiliza la opción de almacenamiento estándar).

3. Haga clic en **Probar conexión** para verificar la conexión a la ubicación de la nube especificada.
4. Haga clic en **Aceptar** para salir del cuadro de diálogo Configuración de la nube.

Especificación del archivo y/o carpeta que se debe restaurar

Después de especificar la ubicación de la copia de seguridad o de la copia de archivo, busque el nombre del archivo o de la carpeta que se debe restaurar. Si un archivo tiene varias versiones de copia de archivo, se enumeran todas las versiones y se clasifican por fecha (con la más reciente enumerada primero).

Siga estos pasos:

1. En el diálogo **Buscar archivos/carpetas para restauración**, especifique qué desea buscar (el nombre del archivo o de la carpeta que se debe restaurar).

   Nota: El campo **Nombre del archivo** también admite búsquedas de nombres completos y búsquedas de comodines. En caso de desconocer el nombre completo del archivo, puede simplificar los resultados de la búsqueda especificando los caracteres comodín "*" y "?" en el campo Nombre del archivo.

   Los caracteres comodín compatibles con el nombre del archivo o carpeta son los siguientes:

   - Utilice el asterisco para sustituir cero o más caracteres en un nombre de archivo o directorio.
   - Utilice el signo de interrogación para sustituir un carácter único en el nombre del archivo o carpeta.

   Por ejemplo, si especifica *.txt, en los resultados de la búsqueda aparecerán todos los archivos con una extensión de archivo .txt.

2. (Opcional)Especifique una ruta para filtrar la búsqueda de forma avanzada y seleccionar si desea incluir o no los subdirectorios.

3. Haga clic en **Buscar** para iniciar los resultados de la búsqueda.

   Los resultados de la búsqueda se muestran. Si el archivo encontrado tiene varias versiones de copia de archivo, se enumerarán todas las versiones clasificadas por la fecha (con la más reciente enumerada primero). También indica si se ha realizado una copia de seguridad o si se ha copiado el archivo encontrado.

4. Seleccione la versión (repetición) del archivo/carpeta que desee restaurar y haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Opciones de restauración**.

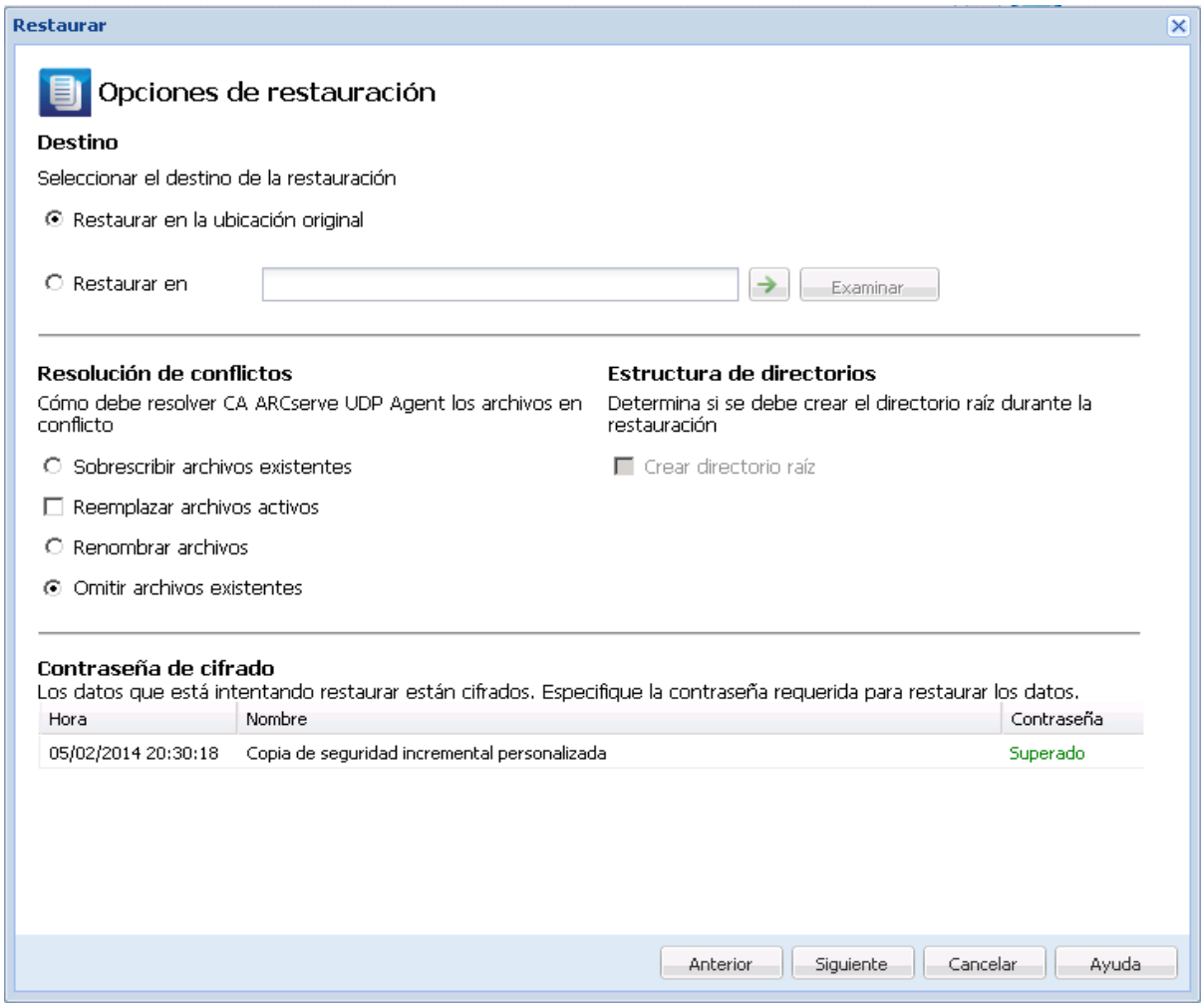
   Se especifica el nombre del archivo o de la carpeta que se tiene que restaurar.

Definición de las opciones de restauración

Después de especificar el archivo o carpeta que se debe restaurar, defina las opciones de restauración para el archivo o carpeta seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, seleccione el destino de la restauración.



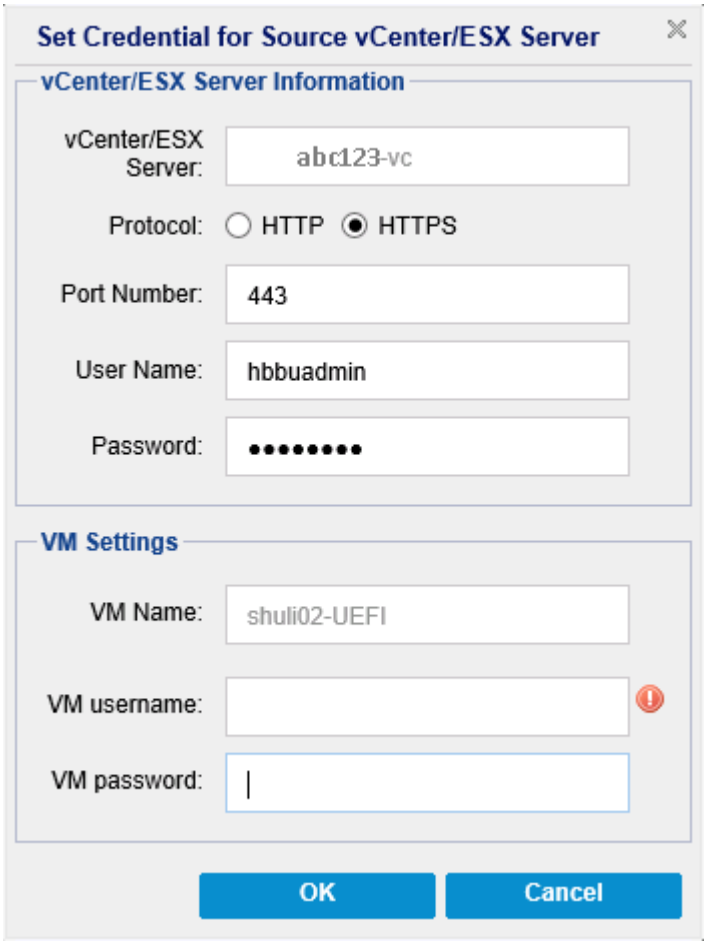
A continuación se especifican las opciones de destino disponibles:

Restaurar en la ubicación original

Restaura en la ubicación original desde la que se ha capturado la imagen de copia de seguridad.

Nota: Si se ha realizado la copia de seguridad del punto de recuperación utilizando la copia de seguridad sin agente basada en el host, la restauración en la ubicación original es volver a llevar a cabo la restauración del archivo en la máquina virtual. En este caso, se abre un cuadro de diálogo. Se pueden introducir las credenciales del hipervisor y el sistema operativo de la máquina virtual.

Para la máquina virtual de VMware:



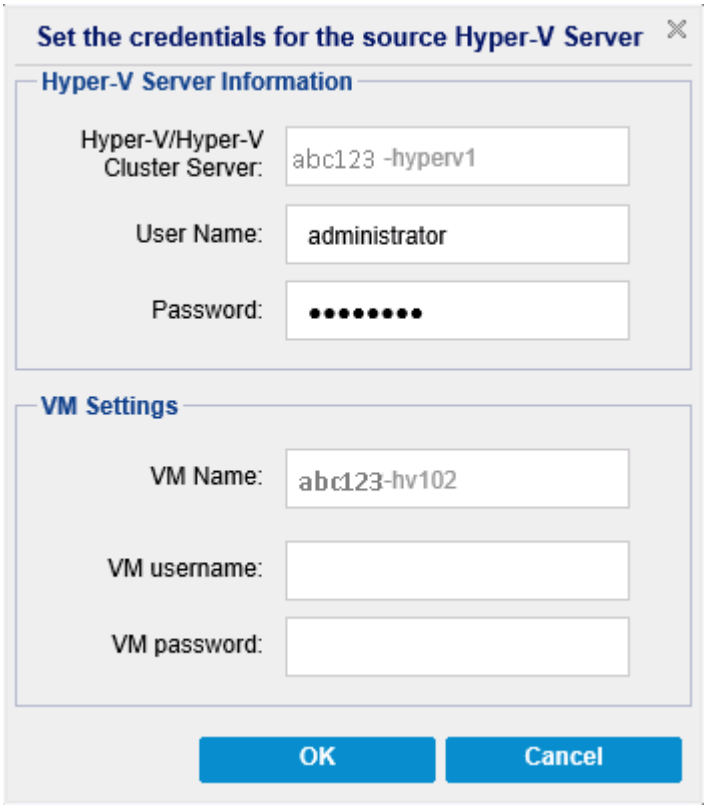
Nota: Para poder crear o escribir archivos en la máquina virtual, tenga en cuenta los siguientes requisitos para la configuración y los permisos de la cuenta de la máquina virtual:

- VMware Tools está instalado y en ejecución.
- Firewall debe permitir compartir archivos e impresoras.

- La cuenta es el administrador local integrado, el administrador del dominio integrado o la cuenta del dominio que es miembro del grupo de administradores locales. Si se utilizan otras cuentas:
  - Desactive el acceso remoto del Control de cuentas de usuario. Para desactivar el acceso remoto del UAC, consulte Importación de la máquina virtual utilizando una cuenta administrativa adicional.
  - Desactive el Control de cuentas de usuario en la Política de seguridad local desactivando el valor de configuración Ejecutar todos los administradores en Modo de aprobación de administrador en secpol.msc-> Políticas locales-> Opciones de seguridad. (Secpol.msc es el editor de políticas de seguridad de Microsoft).

    Importante: No intente desactivar el Control de cuentas de usuario en el cuadro de diálogo Configuración del Control de cuentas de usuario que se abre desde el Panel de control.

Para la máquina virtual de Hyper-V:

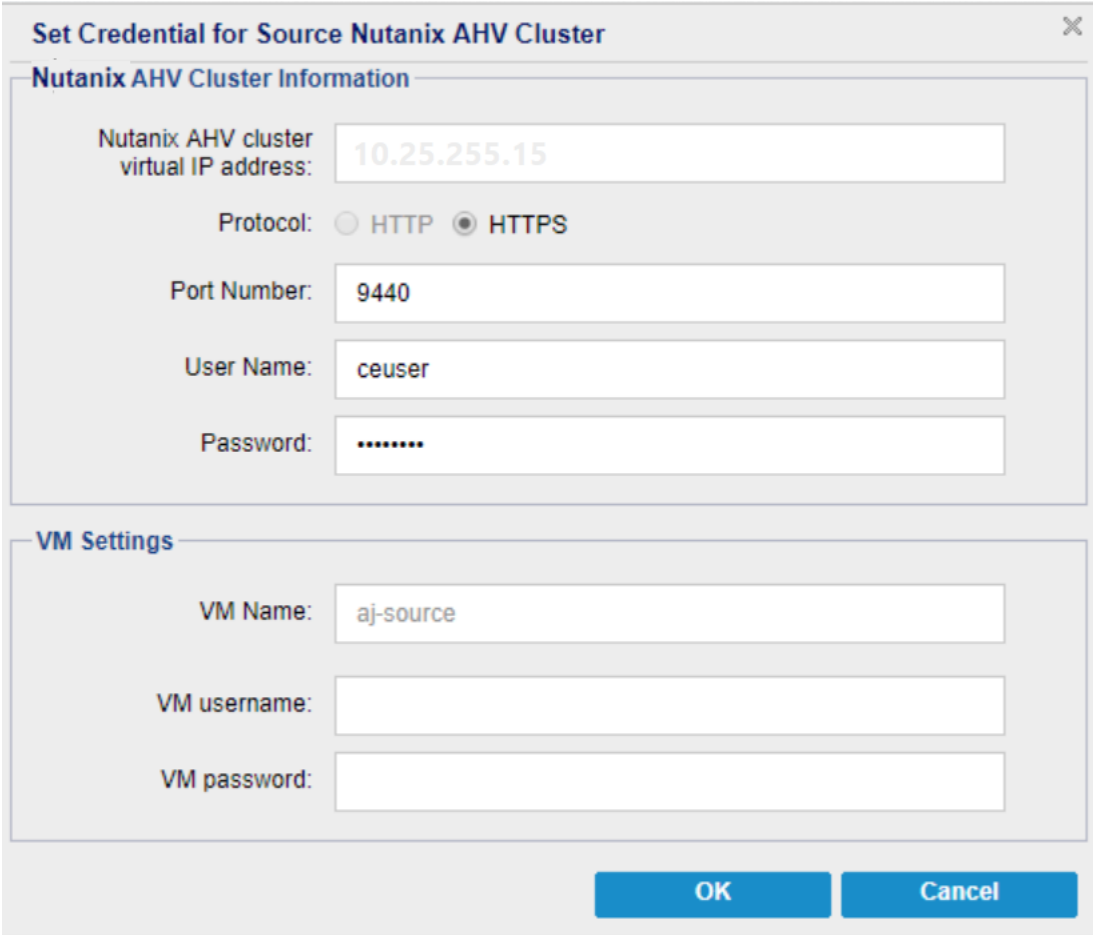


Nota: Para poder crear o escribir archivos en la máquina virtual, tenga en cuenta los siguientes requisitos para la configuración y los permisos de la cuenta de la máquina virtual:

- Los servicios de integración de Hyper-V están instalados y en ejecución.
- Firewall debe permitir compartir archivos e impresoras.
- La cuenta es el administrador local integrado, el administrador del dominio integrado o la cuenta del dominio que es miembro del grupo de administradores locales. Si se utilizan otras cuentas:

  Desactive el acceso remoto del Control de cuentas de usuario. Para desactivar el acceso remoto del UAC, consulte Importación de la máquina virtual utilizando una cuenta administrativa adicional.
- Si el sistema operativo invitado de la máquina virtual es la versión de cliente de Windows (por ejemplo, Windows 10), se deberá configurar manualmente el cortafuegos para permitir el servicio Windows Management Instrumentation (WMI).

Para la máquina virtual de Nutanix



Notas: Para poder crear o escribir archivos en la máquina virtual, tenga en cuenta los siguientes requisitos para la configuración y los permisos de la cuenta de la máquina virtual:

- Firewall debe permitir compartir archivos e impresoras.
- La cuenta es el administrador local integrado, el administrador del dominio integrado o la cuenta del dominio que es miembro del grupo de administradores locales. Si se utilizan otras cuentas:

  Desactive el acceso remoto del Control de cuentas de usuario. Para desactivar el acceso remoto del UAC, consulte Importación de la máquina virtual utilizando una cuenta administrativa adicional.
- Firewall debe permitir Windows Management Instrumentation (WMI).

Restaurar en

Restaura en la ubicación especificada. Se puede hacer clic en el botón de la flecha verde para comprobar la conexión con la ubicación especificada. Si es necesario, también puede escribir las credenciales de nombre de usuario y de contraseña para obtener acceso a dicha ubicación.

2. En **Resolución de conflictos**, especifique la opción correspondiente a la acción que deberá realizar Arcserve UDP si se encuentran conflictos durante el proceso de restauración.

   A continuación se especifican las opciones disponibles:

   Sobrescribir archivos existentes

   Sobrescribe (reemplaza) todos los archivos existentes que se encuentran en el destino de restauración. Todos los objetos se restaurarán desde los archivos de copia de seguridad, independientemente de si actualmente se encuentran en el equipo.

   Reemplazar los archivos activos

   Reemplaza todos los archivos activos después del reinicio. Si durante el intento de restauración, el Agente de Arcserve UDP para Windows detecta que el archivo existente está actualmente en uso o que algún usuario está accediendo al archivo, no sustituye ese archivo de forma inmediata, sino que retrasa la sustitución de los archivos activos hasta que se reinicie de nuevo el equipo con el fin de evitar problemas. (La restauración ocurrirá de forma inmediata pero los archivos activos se sustituirán a partir del reinicio siguiente).

   Esta opción solamente está disponible si selecciona la opción **Sobrescribir archivos existentes**.

   Nota: Si no se selecciona esta opción, se omite de la restauración cualquier archivo activo.

   Cambiar el nombre de los archivos

Si el nombre de archivo ya existe, crea un archivo nuevo. Al seleccionar esta opción se copiará el archivo de origen en el destino con el mismo nombre de archivo pero con una extensión diferente. A continuación, los datos se restaurarán en un archivo nuevo.

Omitir archivos existentes

Omite y no sobrescribe (reemplaza) ningún archivo existente que se encuentre en el destino de restauración. Solo se restaurarán desde los archivos de copia de seguridad los objetos que no estén en el equipo actualmente.

Valor por omisión: Omitir archivos existentes

3. Especifique la **Estructura de directorios** para crear un directorio raíz durante la restauración.

Crear directorio raíz

Especifica que si existe una estructura de directorio raíz en la imagen de copia de seguridad capturada, Arcserve UDP recreará la misma estructura de directorio raíz en la ruta de destino de la restauración.

Si no se selecciona esta opción, el archivo o carpeta se restaurará directamente en la carpeta de destino.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt" y "C:\Folder1\SubFolder2\B.txt" y durante la restauración ha especificado como destino de la restauración "D:\Restore".

- Si ha seleccionado la restauración de los archivos "A.txt" y "B.txt" de manera individual, el destino de los archivos restaurados será "D:\Restore\A.txt" y "D:\Restore\B.txt" (no se recreará el directorio raíz anterior en el nivel de archivo especificado).
- Si se selecciona la restauración desde el nivel "Subcarpeta2", el destino para los archivos restaurados será "D:\Restore\SubFolder2\A.txt" y "D:\Restore\SubFolder2\B.txt" (el directorio raíz superior al nivel de carpeta especificada no se recreará).

Con esta opción seleccionada, la ruta completa de directorio raíz para los archivos/carpetas (incluyendo el nombre de volumen) se recrea en la carpeta de destino. Si los archivos o carpetas que deben restaurarse provienen del mismo nombre de volumen, la ruta del directorio raíz de destino no incluirá el nombre del volumen. Sin embargo, si los archivos o carpetas que deben restaurarse provienen de diferentes nombres de volúmenes, la ruta del directorio raíz de destino incluirá el nombre de volumen.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", y también

E:\Folder3\SubFolder4\C.txt", y durante la restauración ha especificado el destino de restauración como "D:\Restore".

- Si ha seleccionado la restauración únicamente del archivo "A.txt", el destino para el archivo restaurado será "D:\Restore\ Folder1\SubFolder2\A.txt" (se recreará todo el directorio raíz sin el nombre de volumen).
- Si ha seleccionado la restauración tanto del archivo "A.txt" como del archivo "C.txt", el destino para los archivos restaurados será "D:\Restore\C\ Folder1\SubFolder2\A.txt" y "D:\Restore\ E\Folder3\SubFolder4\C.txt" (se recreará todo el directorio raíz con el nombre de volumen).

4. La **Contraseña de cifrado** para el destino de copia de archivo se cargará automáticamente. Si selecciona un destino alternativo para la restauración, será necesario introducir la contraseña manualmente.
5. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Resumen de la restauración**.

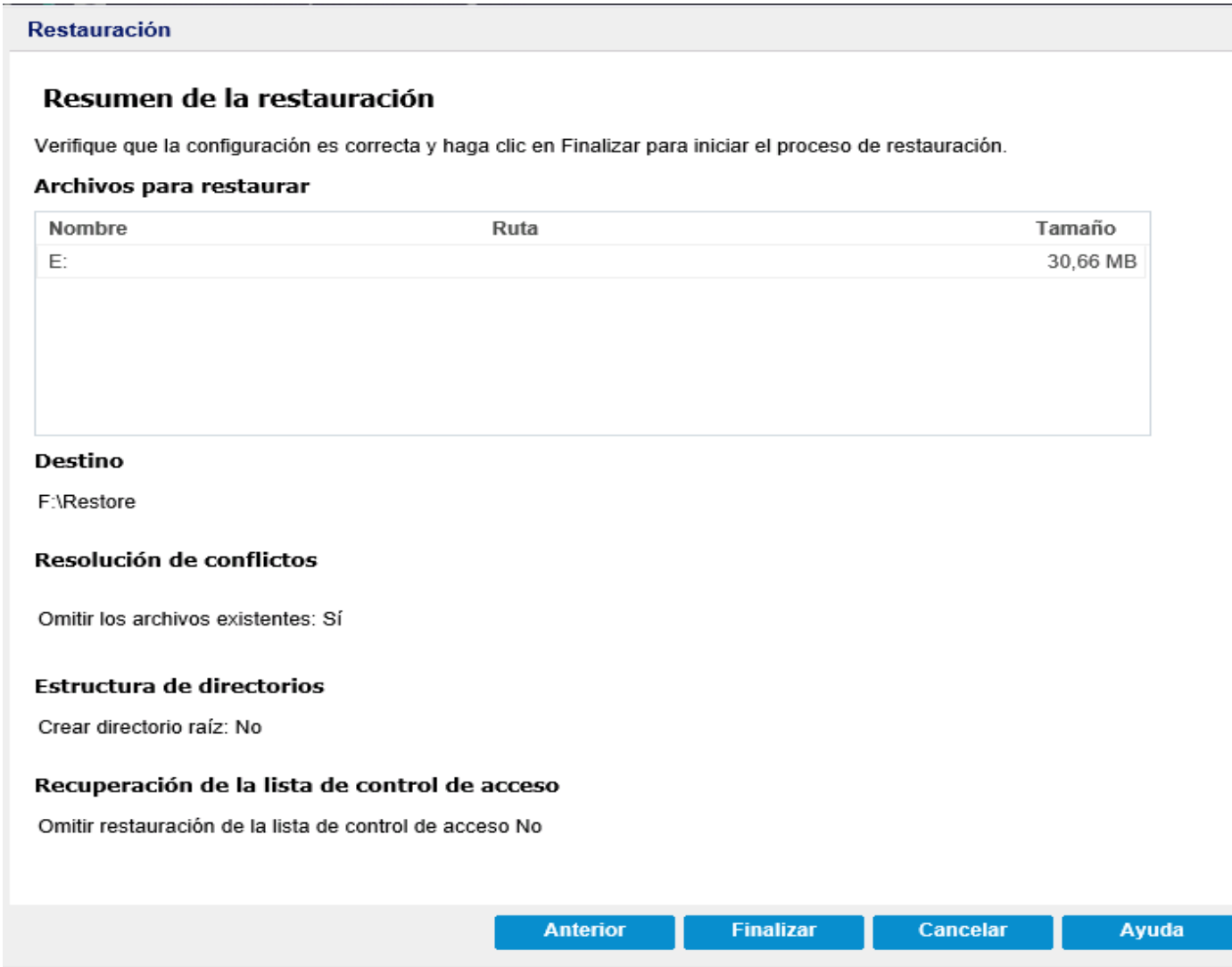
   Las opciones de restauración se han definido para restaurar el archivo o carpeta especificado.

Restauración del archivo y/o carpeta

El **Resumen de la restauración** le ayuda a revisar todas las opciones de la restauración definidas previamente y a modificarlas si es necesario.

Siga estos pasos:

1. En el cuadro de diálogo **Resumen de la restauración**, revise la información que aparece en pantalla para verificar que todos los valores de configuración y las opciones de restauración sean correctos.



- Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para cambiar el valor de configuración incorrecto.
- Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar el proceso de restauración.

El archivo y/o carpeta especificado se restaura.

Verificación de que el archivo y/o carpeta se ha restaurado

Después de la terminación del proceso de restauración, verifique que el archivo y/o carpeta se ha restaurado en el destino especificado.

Siga estos pasos:

1. Vaya al destino de la restauración que se ha especificado.

   Aparecerá una lista de carpetas.

2. Encuentre el archivo en el cual ha restaurado el contenido.

   Por ejemplo, si selecciona restaurar el archivo A.txt en el destino de la restauración D:\Restore, vaya a la ubicación siguiente:

   D:\Restore\A.txt.

3. Verifique el contenido del archivo y/o carpeta restaurado.

   El contenido restaurado se ha verificado correctamente.

Cómo realizar una reconstrucción completa utilizando una máquina virtual de Virtual Standby o instantánea

La reconstrucción completa es el proceso de restaurar un sistema de "reconstrucción completa" incluyendo la reinstalación del sistema operativo y de las aplicaciones de software, además de restaurar los datos y la configuración. El proceso de reconstrucción completa permite restaurar un equipo completo con un esfuerzo mínimo, incluso en un hardware diferente. La reconstrucción completa es posible porque durante el proceso de copia de seguridad de nivel de bloque, el Agente de Arcserve UDP (Windows) no solo captura los datos, sino también toda la información relacionada con las siguientes aplicaciones:

- Sistema operativo
- Aplicaciones instaladas
- Valores de configuración
- Controladores necesarios

  Se realiza una copia de seguridad de toda la información relevante que es necesaria para realizar una compilación completa del sistema desde la reconstrucción completa en una serie de bloques que se almacenan en la misma ubicación que la copia de seguridad.

Para realizar una reconstrucción completa desde una máquina virtual, utilice una de las formas siguientes:

- Conectar con el servidor ESX directamente mediante la dirección IP
- Agregar la configuración de DNS correcta en el equipo de reconstrucción completa y resolver el nombre de host a la dirección IP

Complete las tareas siguientes para realizar una reconstrucción completa mediante una máquina virtual de Virtual Standby o instantánea:

1. Revisión de las consideraciones y requisitos previos de la reconstrucción completa
2. Definición de las opciones de la reconstrucción completa
   - Recuperación mediante una máquina virtual de Virtual Standby para Hyper-V o una máquina virtual instantánea
   - Recuperación mediante una máquina virtual de Virtual Standby para VMware o una máquina virtual instantánea
   - Realización de la reconstrucción completa en el modo expreso
   - Realización de la reconstrucción completa en el modo avanzado
3. Verificación de que la reconstrucción completa ha sido correcta

4. Información de referencia de la reconstrucción completa
5. Solución de problemas relacionados con la recuperación completa

Revisión de las consideraciones y requisitos previos de la reconstrucción completa

Verifique que los requisitos previos siguientes existen antes de realizar una reconstrucción completa:

- Se debe tener una de las imágenes siguientes:
  - Una imagen ISO de BMR creada se graba en un CD/DVD
  - Una imagen ISO de BMR creada se graba en una unidad de USB

  Nota: El Agente de Arcserve UDP (Windows) utiliza una utilidad de kit de arranque para combinar una imagen de WinPE y una imagen del Agente de Arcserve UDP (Windows) a fin de crear una imagen ISO de reconstrucción completa. Esta imagen ISO se graba en un medio de arranque. Se puede utilizar cualesquiera de los medios de arranque siguientes (CD/DVD o unidad de USB) para inicializar el nuevo sistema informático y permitir el inicio del proceso de reconstrucción completa. Para garantizar que la imagen guardada es la versión más reciente, una práctica recomendable es la creación de una nueva imagen ISO cada vez que se actualiza el Agente de Arcserve UDP (Windows).
- Tener al menos una copia de seguridad completa disponible.
- Disponer de 1 GB de memoria RAM instalado en la máquina virtual y en el servidor de origen que está recuperando.
- Para recuperar máquinas virtuales de VMware en otras que estén configuradas para comportarse como servidores físicos, compruebe que las herramientas de VMware estén instaladas en la máquina virtual de destino.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones sobre la restauración:

- Independientemente del método que ha utilizado para crear una imagen de kit de arranque, el proceso de reconstrucción completa es prácticamente el mismo para cada caso.

  Nota: El proceso de reconstrucción completa no puede crear espacios de almacenamiento. Si el equipo de origen ha tenido espacios de almacenamiento durante la reconstrucción completa, no se podrán crear nuevos en el equipo de destino. También se pueden restaurar estos volúmenes en discos/volúmenes regulares o crear espacios de almacenamiento manualmente antes de realizar la reconstrucción completa. A continuación, ya se podrán restaurar los datos en los espacios de almacenamiento creados.

- Los discos dinámicos sólo se restauran en el nivel de disco. Si ha realizado la copia de seguridad de los datos en un volumen local de un disco dinámico, no será posible restaurar este disco dinámico durante la reconstrucción completa. En este escenario, para restaurar durante la reconstrucción completa se debe realizar una de las tareas siguientes y a continuación realizar la reconstrucción completa desde el punto de recuperación copiado:
  - Realizar la copia de seguridad en un volumen de otra unidad.
  - Realizar la copia de seguridad en un recurso compartido remoto.
  - Copiar un punto de recuperación en otra ubicación.

  Nota: Si se realiza una reconstrucción completa con varios discos dinámicos, esta podrá producir un error a causa de algunos errores inesperados (como un error al reiniciar los volúmenes dinámicos desconocidos, entre otros). Si esto ocurre, se debería restaurar solamente el disco del sistema mediante BMR y, a continuación, después de reiniciar el equipo, se podrá realizar una restauración de los otros volúmenes dinámicos en un entorno normal.
- Si intenta realizar una reconstrucción completa en una máquina virtual de Hyper-V con un disco de 4 KB, agregue este disco de 4 KB al controlador de SCSI. Si lo agrega al controlador de IDE, el disco no se detectará en el sistema de Windows PE.
- (Opcional) Revise la información de referencia de la reconstrucción completa. Si desea obtener más información, consulte los siguiente temas:
  - Cómo funciona la reconstrucción completa
  - Sistemas operativos que admiten la conversión de UEFI/BIOS
  - Gestión del menú Operaciones de BMR

Revise las siguientes consideraciones:

- Si se actualiza a una versión más reciente de Arcserve UDP, se tendrá que volver a crear la imagen ISO de reconstrucción completa utilizando el nivel adecuado de Windows ADK o AIK para incluir la compatibilidad con las últimas funciones y correcciones de errores. Sin embargo, una vez que se crea una imagen ISO de reconstrucción completa, el archivo ISO puede utilizarse para el mismo nivel de sistema operativo. Los siguientes niveles de sistema operativo pueden utilizar el mismo ISO:
  - ISO creado con el WAIK Windows 7: Funciona para Windows 2003, Vista, 2008 y 2008 R2
  - ISO creado usando Windows 8/8.1 ADK: Funciona para Windows 8, 8.1, Server 2012 y 2012 Server R2
  - ISO creado usando Windows 10 ADK: Funciona para Windows 10

Definición de las opciones de la reconstrucción completa

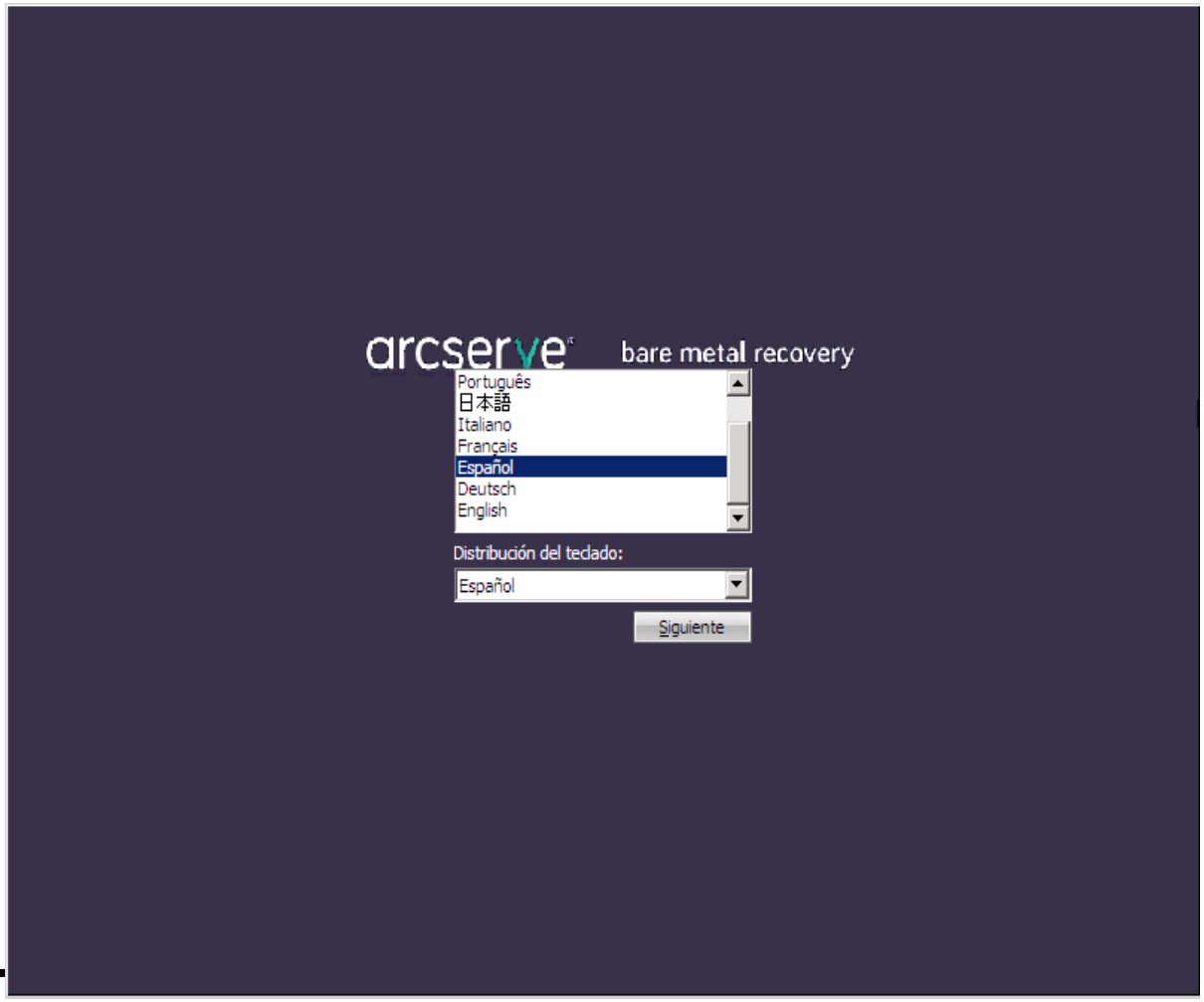
Antes de iniciar el proceso de la reconstrucción completa, se deben especificar algunas opciones de la reconstrucción completa preliminares.

Siga estos pasos:

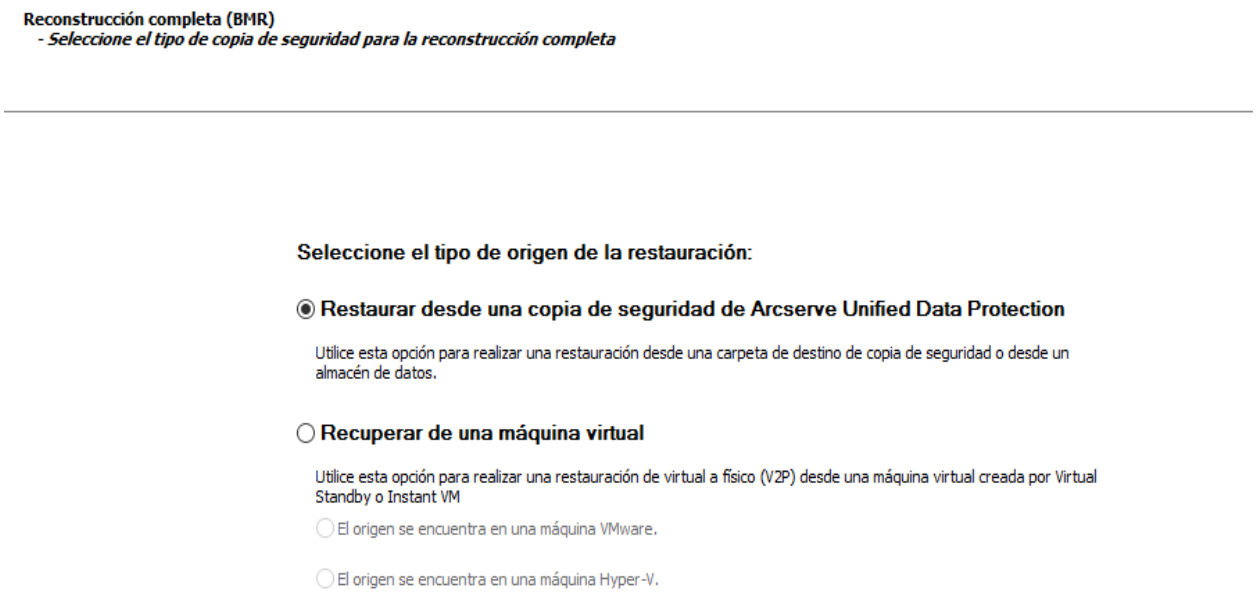
1. Inserte el medio de imagen de kit de arranque guardado y reinicie el equipo.
   - Si se utiliza una imagen ISO de BMR que se ha grabado en un CD/DVD, inserte el CD/DVD guardado.
   - Si se utiliza una imagen ISO de BMR que se ha grabado en una unidad de USB, inserte el USB guardado.

   Aparecerá la pantalla **Utilidad de instalación de BIOS**.
2. Desde la pantalla **Utilidad de instalación de BIOS**, seleccione la opción de unidad de CD-ROM o unidad de USB para iniciar el proceso de arranque. Seleccione una arquitectura (x86/x64) y pulse **Intro** para continuar.

   Aparece la pantalla de selección del idioma del Agente de Arcserve UDP (Windows).
3. Seleccione el idioma y haga clic en **Siguiente** para continuar.



El proceso de reconstrucción completa empezará y se mostrará la pantalla inicial del asistente de reconstrucción completa.



La pantalla del asistente para la reconstrucción completa le permite seleccionar el tipo de reconstrucción completa que se desea realizar:

- **Restauración desde una copia de seguridad de Arcserve Unified Data Protection**

  Utilice esta opción para realizar una restauración desde una carpeta de destino de la copia de seguridad o desde un almacén de datos.

  Esta opción permite recuperar los datos de los cuales se ha realizado una copia de seguridad mediante el Agente de Arcserve UDP (Windows). Esta opción se utiliza en conexión con las sesiones de copia de seguridad realizadas con el Agente de Arcserve UDP para Windows o con la aplicación Arcserve UDP host-based VM backup.

  Para obtener más información, consulte Cómo realizar una reconstrucción completa mediante una copia de seguridad en la Ayuda en línea.

- **Recuperarse de una máquina virtual con Virtual Standby**

  Utilice esta opción para realizar una restauración de virtual a-física (V2P) desde una máquina virtual de Virtual Standby o una máquina virtual instantánea. El término Virtual a física (V2P) hace referencia a la migración de un sistema operativo (SO), los programas de la aplicación y los datos desde una máquina virtual o partición de disco al disco duro principal de un equipo. El destino puede ser un único equipo o varios equipos.

- **El origen está en un equipo de VMware**

  Permite recuperar datos para un equipo para el cual se realiza la conversión virtual en una máquina virtual de VMware. Esta opción se utiliza con la aplicación Arcserve Virtual Standby o máquina virtual instantánea.

  Nota: Para esta opción, solamente se pueden recuperar datos si la conversión virtual a un archivo VMDK (para VMware) se ha realizado mediante Arcserve Central Virtual Standby o máquina virtual instantánea.

  Si se ha seleccionado esta opción, consulte Recuperar mediante una máquina virtual con Virtual Standby para VMware o máquina virtual instantánea para continuar con este procedimiento.

- **El origen está en un equipo de Hyper-V**

  Posibilita la recuperación de datos para un equipo para el cual se realiza la conversión virtual en una máquina virtual de Hyper-V. Esta opción se utiliza con la aplicación Arcserve Virtual Standby o máquina virtual instantánea.

  Nota: Para esta opción, solamente se pueden recuperar datos si la conversión virtual a un archivo VHD (para Hyper-V) se ha realizado mediante Arcserve Central Virtual Standby o máquina virtual instantánea.

  Si se ha seleccionado esta opción, consulte Recuperar mediante una máquina virtual con Virtual Standby para Hyper-V o máquina virtual instantánea para continuar con este procedimiento.

4. Seleccione **Recuperarse de una máquina virtual con Virtual Standby**. A continuación, seleccione uno de los orígenes.

   Si selecciona la opción **El origen está en una opción de equipo VMware**, consulte Recuperación mediante una máquina virtual de Virtual Standby para VMware o máquina virtual instantánea para continuar con este procedimiento.

   Si selecciona la opción **El origen está en una opción de equipo Hyper-V**, consulte Recuperación mediante una máquina virtual de Virtual Standby para Hyper-V o máquina virtual instantánea para continuar con este procedimiento.

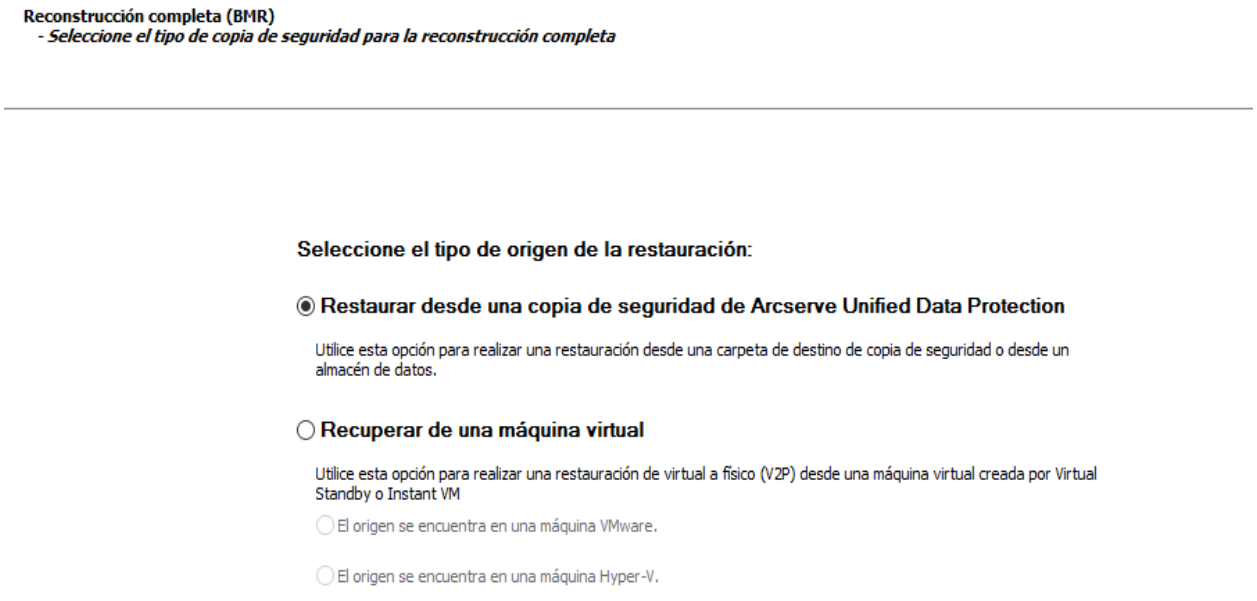
Recuperación mediante una máquina virtual de Virtual Standby para Hyper-V o una máquina virtual instantánea

El Agente de Arcserve UDP (Windows) proporciona la capacidad para realizar reconstrucciones completas para equipos de virtual a físico (V2P). Esta función permite realizar recuperaciones de virtual a físico desde el último estado de una máquina virtual en espera o instantánea y ayuda a reducir la pérdida del equipo de producción.

Siga estos pasos:

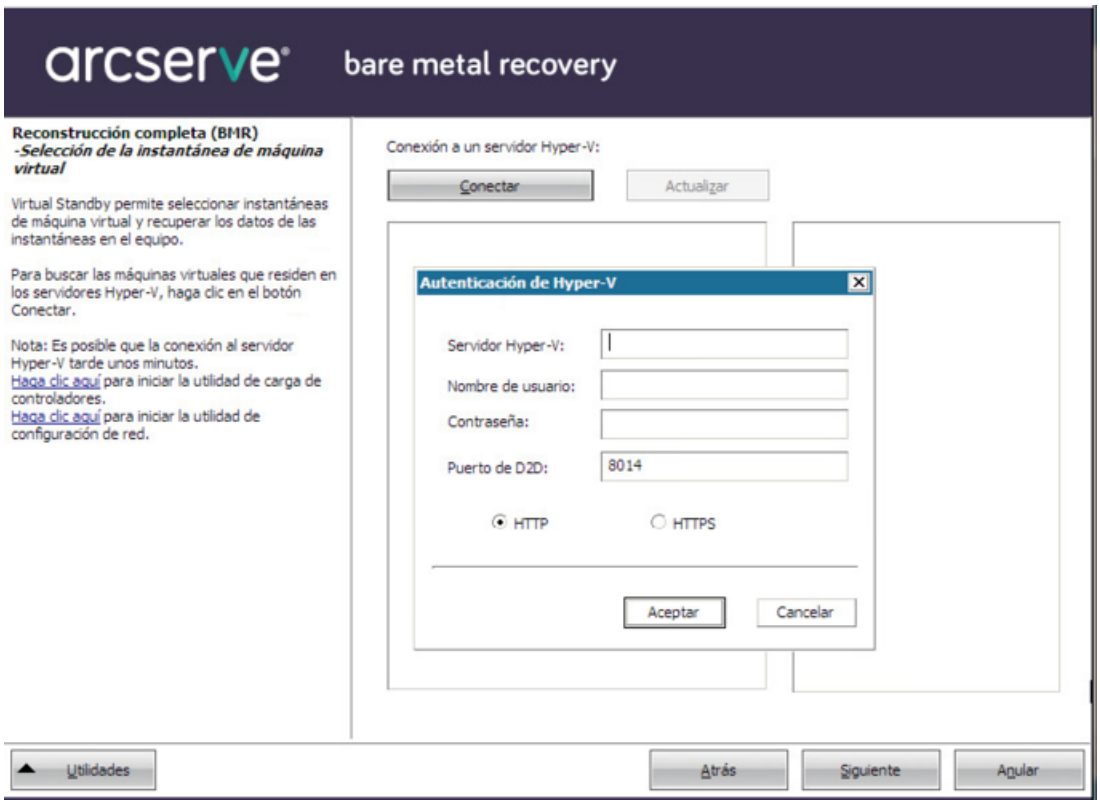
1. Desde la pantalla del asistente Selección del tipo de reconstrucción completa (BMR), seleccione la opción **Recuperar mediante una máquina virtual de Virtual Standby** y la opción **El origen está en un equipo de Hyper-V**.

   Utilice esta opción para realizar una restauración de virtual a-física desde una máquina virtual de Virtual Standby o una máquina virtual instantánea. El término Virtual a física hace referencia a la migración de un sistema operativo (SO), los programas de la aplicación y los datos desde una máquina virtual o partición de disco al disco duro principal de un equipo. El destino puede ser un único equipo o varios equipos.



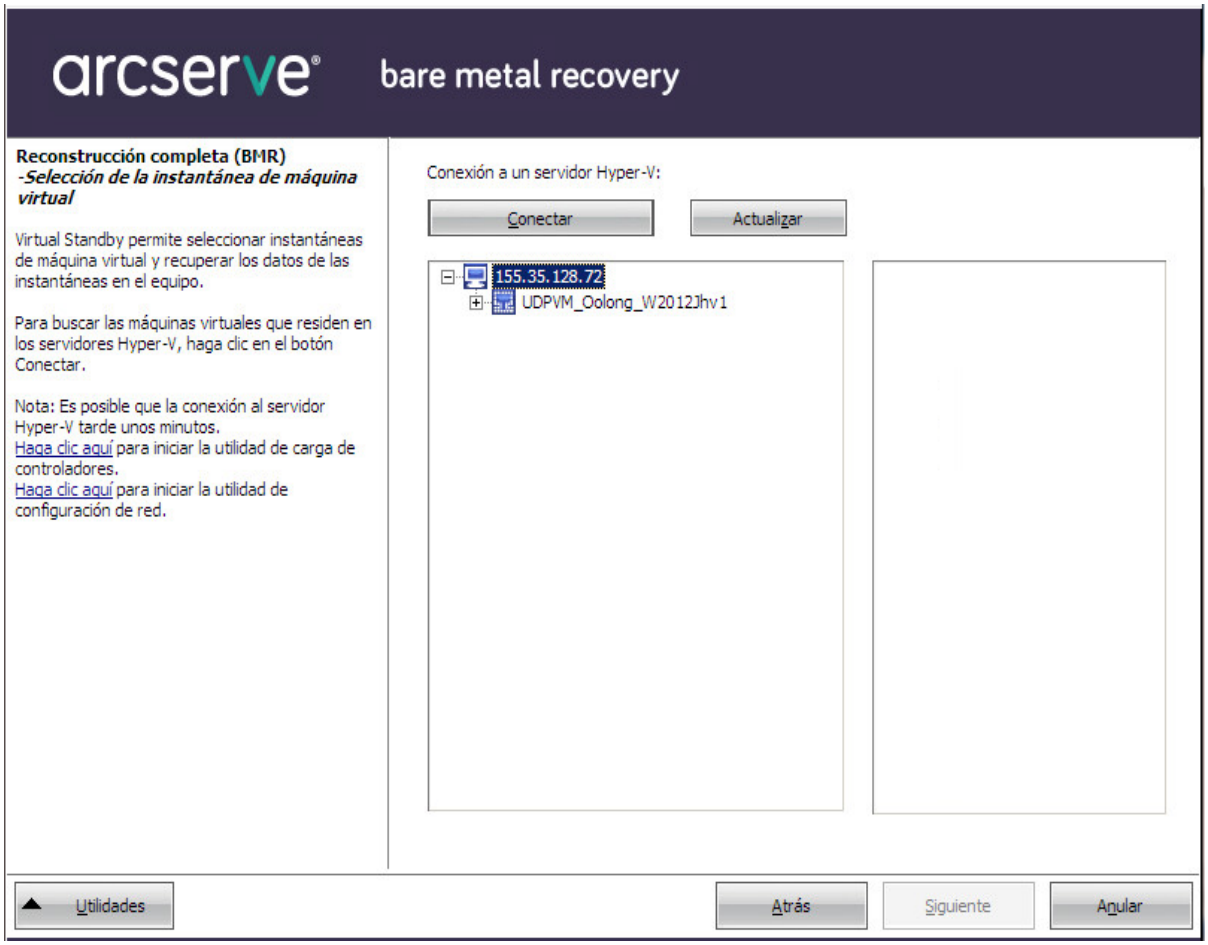
2. Haga clic en **Siguiente**.

Aparecerá la pantalla Seleccione una instantánea de máquina virtual, junto con el cuadro de diálogo Autenticación de Hyper-V, que solicita más detalles acerca del servidor Hyper-V.



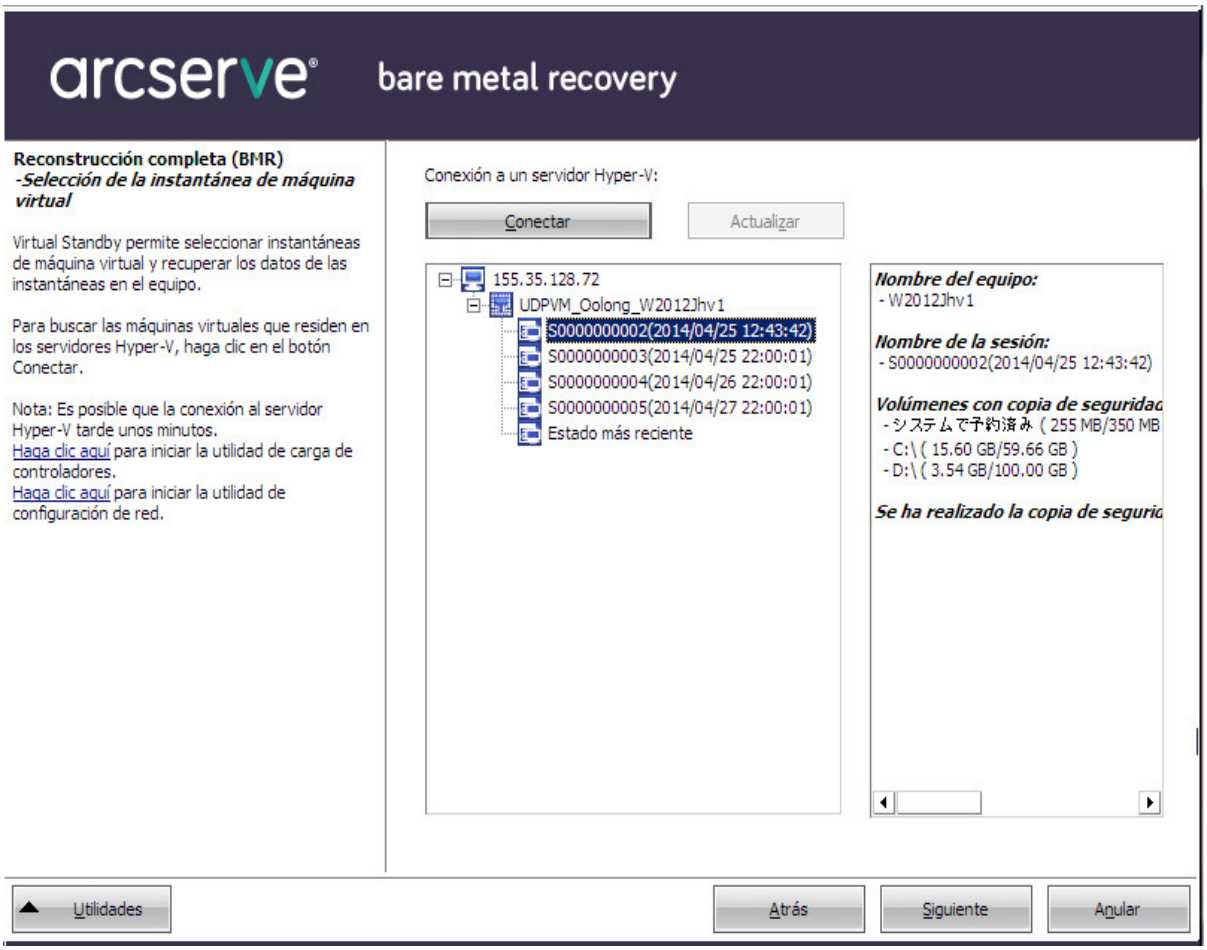
3. Introduzca la información de autenticación y haga clic en **Aceptar**.

   El Agente de Arcserve Unified Data Protection para Windows detecta y muestra el servidor Hyper-V con un listado de todas las máquinas virtuales que se han convertido al servidor Hyper-V especificado mediante Arcserve Central Virtual Standby o la máquina virtual instantánea.



4. Seleccione la máquina virtual que contiene las instantáneas de punto de recuperación para la imagen de copia de seguridad.

   Aparecen las sesiones de copia de seguridad (instantáneas de punto de recuperación) para la máquina virtual seleccionada.



5. Seleccione la sesión de copia de seguridad de la máquina virtual (instantánea de punto de recuperación) que desee recuperar.

   Los detalles correspondientes para la instantánea de punto de recuperación seleccionada (nombre de la máquina virtual, nombre de la sesión de copia de seguridad, volúmenes con copia de seguridad) aparecen en el panel derecho.

   Además de seleccionar uno de los puntos de recuperación enumerados, también tiene la opción de seleccionar el punto de recuperación con **Estado actual** o **Estado más reciente**.

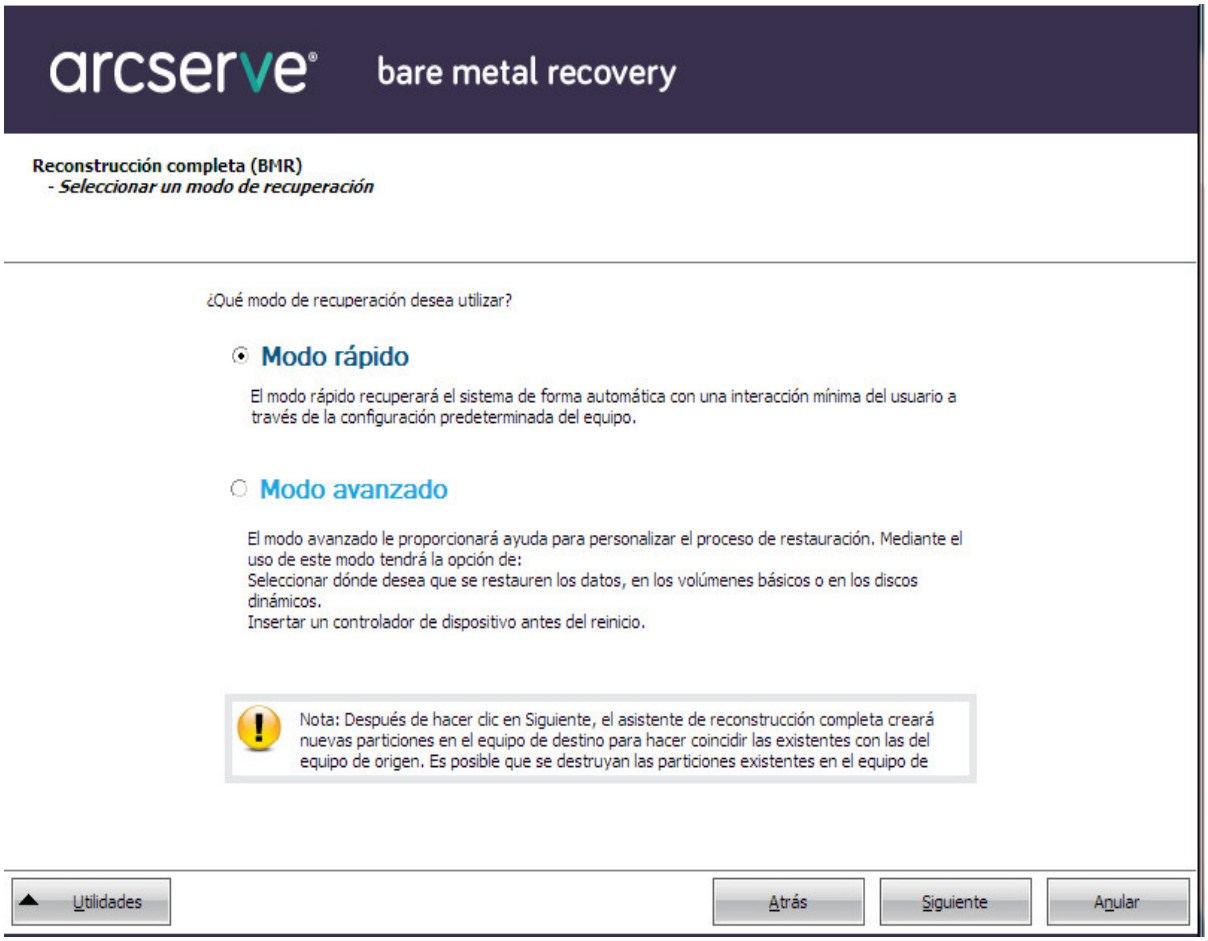
   - Si la máquina virtual que está recuperando está encendida, aparecerá el punto de recuperación en **Estado actual**.

     Nota: Si la máquina virtual está encendida, no se recuperarán los cambios de datos realizados en la máquina virtual una vez que se haya iniciado el proceso de reconstrucción completa.

   - Si la máquina virtual que está recuperando está apagada, aparecerá el punto de recuperación en **Estado más reciente**.

6. Compruebe que se trata del punto de recuperación que desee restaurar y haga clic en **Siguiente**.

   Aparecerá la pantalla del asistente de reconstrucción completa con las opciones de modo de recuperación disponibles.



   Las opciones disponibles son **Modo avanzado** y **Modo rápido**.

   - Seleccione **Modo rápido** si desea una interacción mínima durante el proceso de recuperación. Para obtener más información, consulte Realización de la reconstrucción completa en el modo rápido.
   - Seleccione **Modo avanzado** si desea personalizar el proceso de recuperación. Para obtener más información, consulte a Realización de la reconstrucción completa en el modo avanzado.

   Valor predeterminado: Modo rápido.

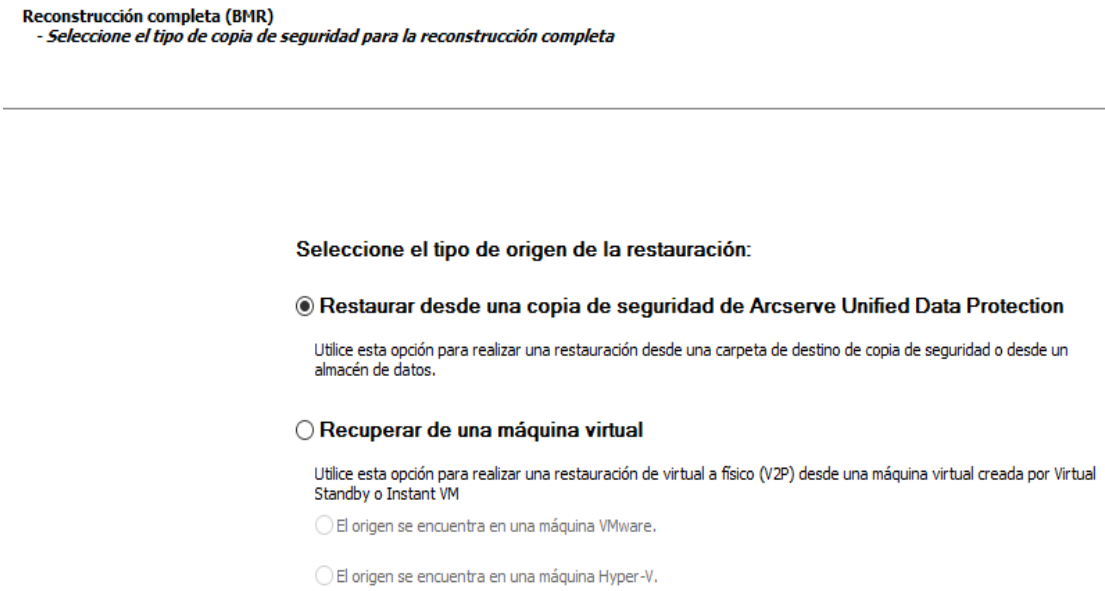
Recuperación mediante una máquina virtual de Virtual Standby para VMware o una máquina virtual instantánea

El Agente de Arcserve UDP (Windows) proporciona la capacidad para realizar reconstrucciones completas para equipos de virtual a físico (V2P). Esta función permite realizar recuperaciones de virtual a físico desde el último estado de una máquina virtual en espera y ayuda a reducir la pérdida del equipo de producción.

Siga estos pasos:

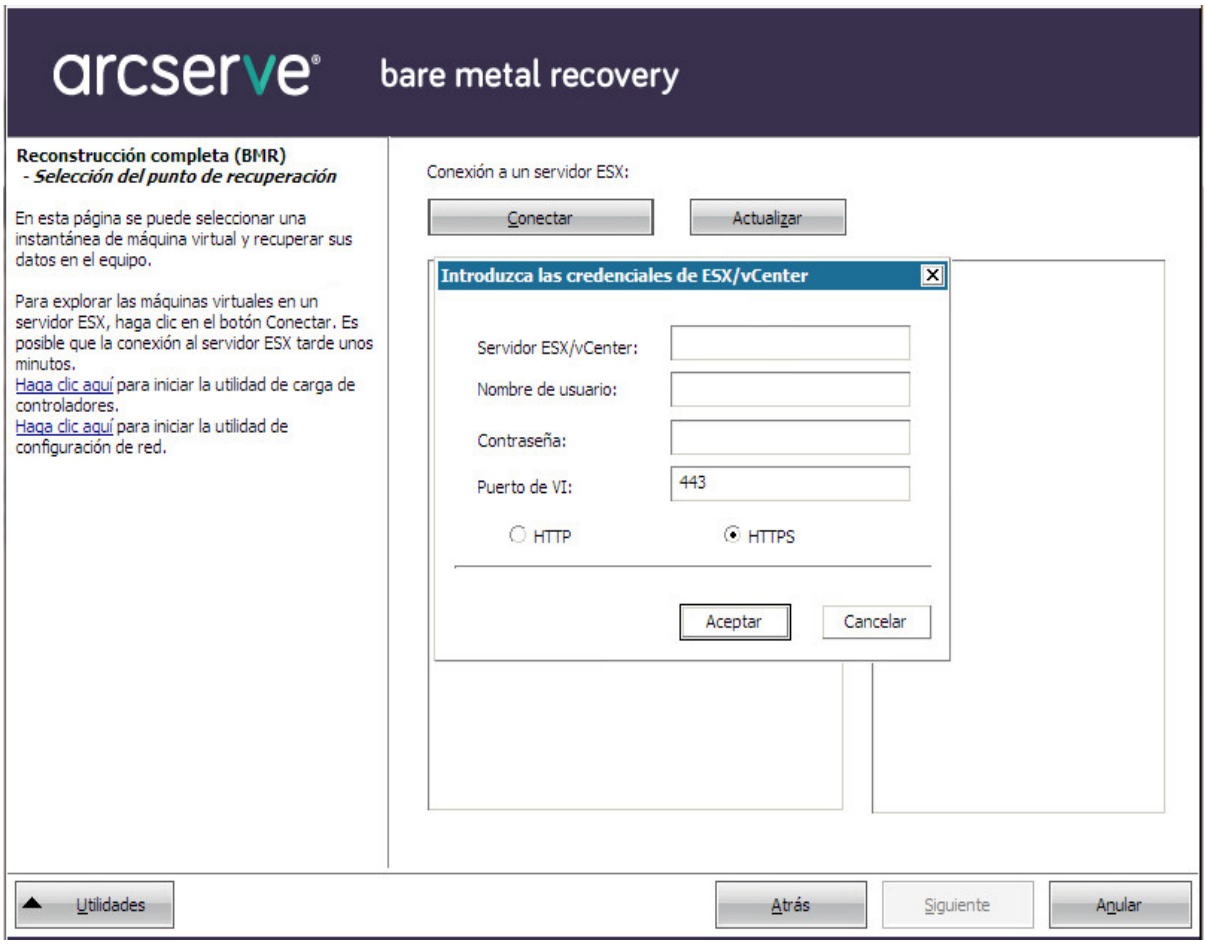
1. Desde la pantalla del asistente Selección del tipo de reconstrucción completa (BMR), seleccione la opción **Recuperar mediante una máquina virtual** y la opción **El origen está en un equipo de VMware**.

   Utilice esta opción para realizar una restauración de virtual a-física desde una máquina virtual de Virtual Standby o una máquina virtual instantánea. El término Virtual a física hace referencia a la migración de un sistema operativo (SO), los programas de la aplicación y los datos desde una máquina virtual o partición de disco al disco duro principal de un equipo. El destino puede ser un único equipo o varios equipos.



2. Haga clic en **Siguiente**.

   La pantalla **Seleccionar un punto de recuperación** aparece junto con el cuadro de diálogo **Credenciales ESX/VC**.



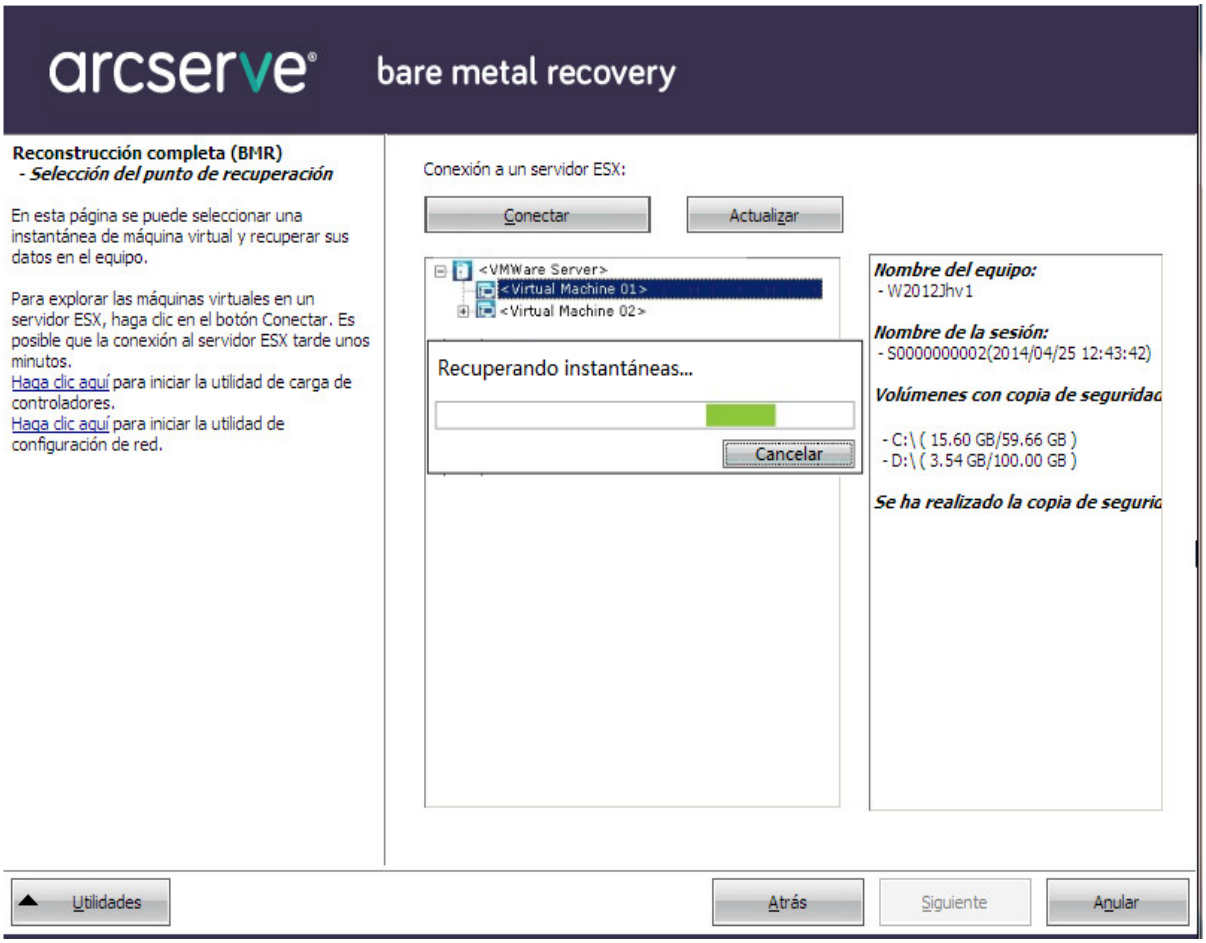
3. Introduzca la información de credenciales correspondiente y haga clic en **Aceptar**.

   Nota: Si se está conectando a vCenter, no necesita un permiso de administrador a nivel del servidor de vCenter pero se debe tener un permiso de administrador a nivel del centro de datos. Además, se deben tener los siguientes permisos a nivel del servidor de vCenter:

   - Global, DisableMethods y EnableMethods
   - Global, licencia

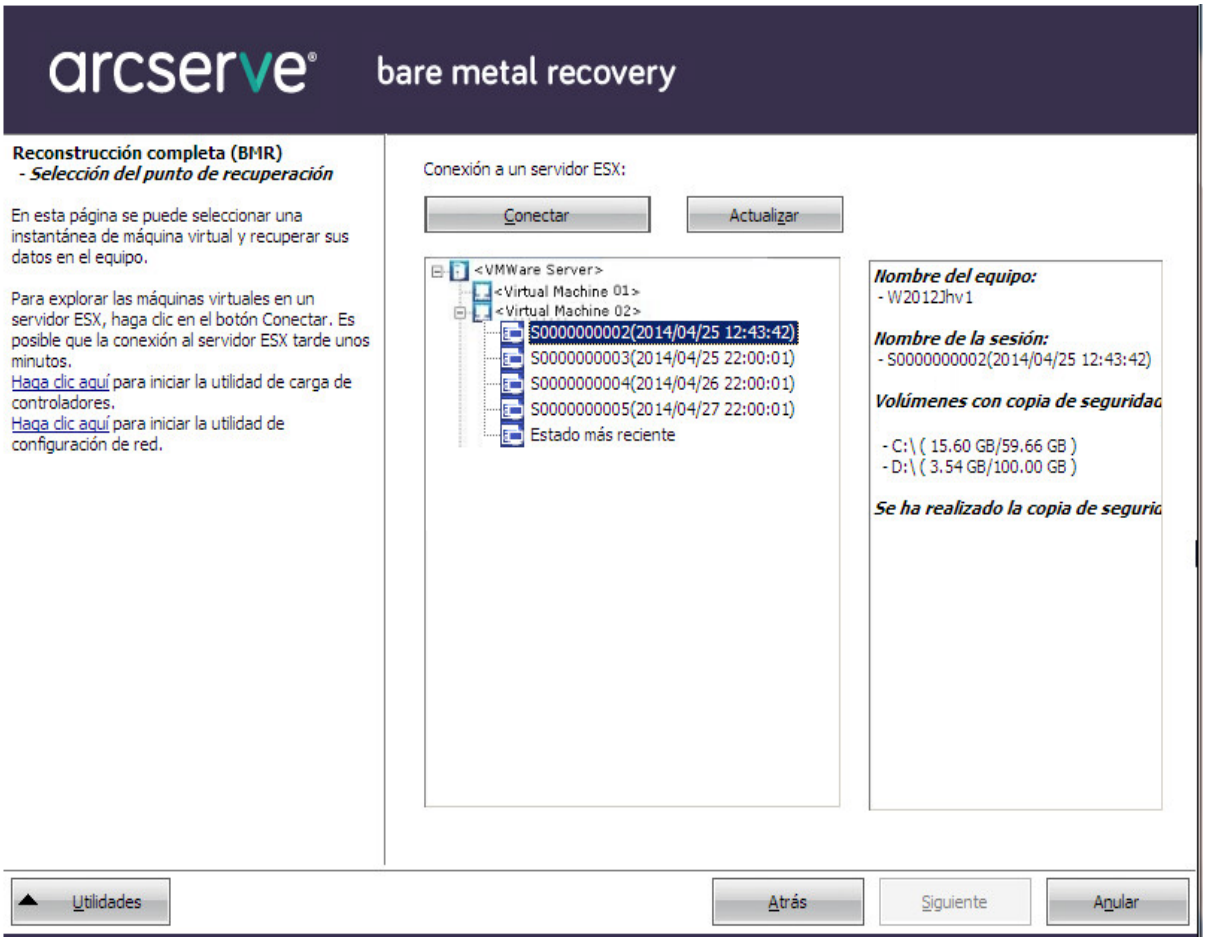
   Aparecerá la pantalla de asistente **Seleccionar un punto de recuperación**.

   A continuación, el Agente de Arcserve Unified Data Protection para Windows recupera todas las instantáneas de punto de recuperación para el servidor VMware seleccionado y muestra el servidor VMware en el panel de la izquierda con un listado de todas las máquinas virtuales que se hospedan en el servidor VMware seleccionado.



4. Seleccione la máquina virtual que contenga los puntos de recuperación para la imagen de copia de seguridad.

   Aparecen las sesiones de copia de seguridad (instantáneas de punto de recuperación) para la máquina virtual seleccionada.



5. Seleccione la sesión de copia de seguridad de la máquina virtual (instantáneas de punto de recuperación) que desee recuperar.

   Los detalles correspondientes para la instantánea de punto de recuperación seleccionada (nombre de la máquina virtual, nombre de la sesión de copia de seguridad, volúmenes con copia de seguridad, discos dinámicos con copia de seguridad) se muestran en el panel de la derecha.

   Además de seleccionar uno de los puntos de recuperación enumerados, también tiene la opción de seleccionar el punto de recuperación con **Estado actual** o **Estado más reciente**.

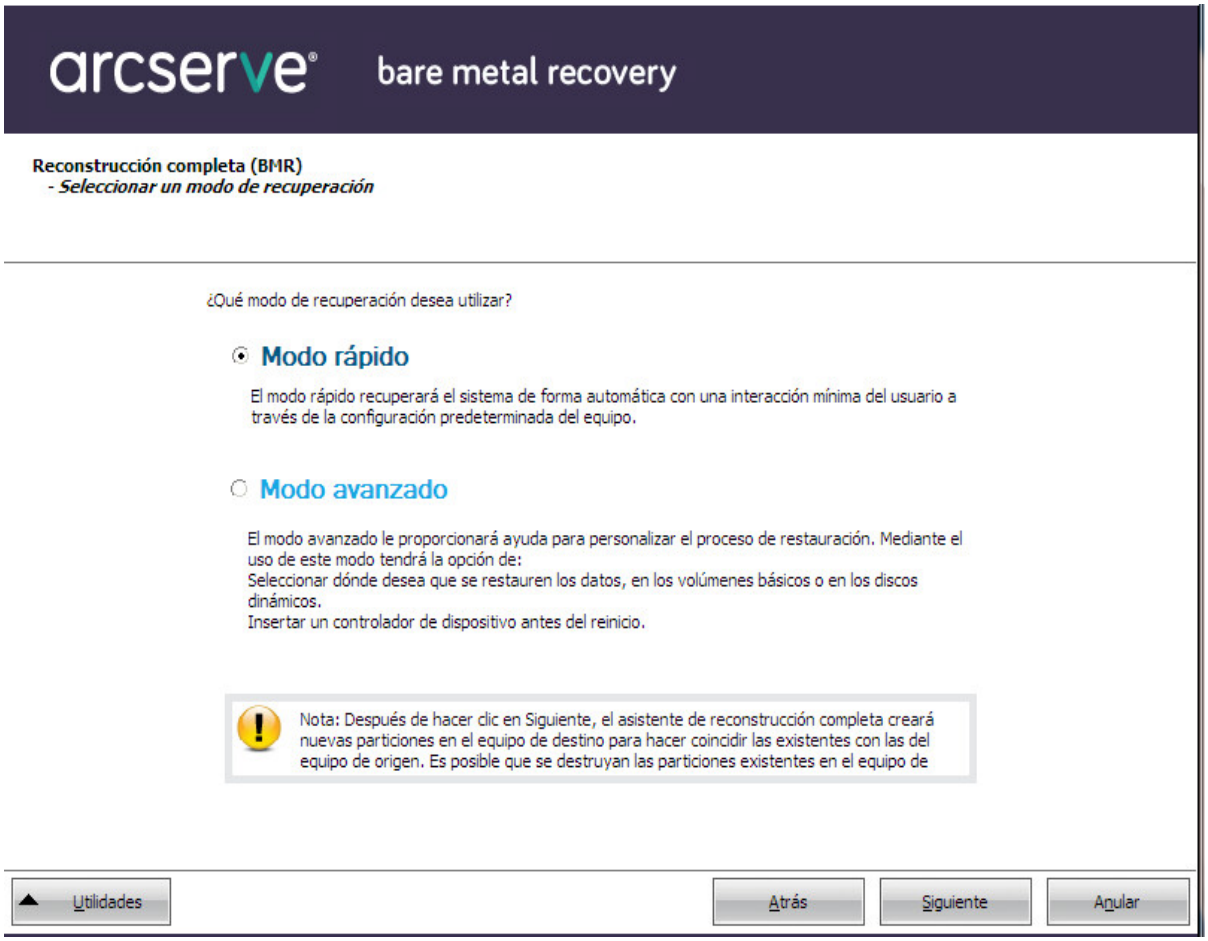
   - Si la máquina virtual que está recuperando está encendida, aparecerá el punto de recuperación en **Estado actual**.

     Nota: Si la máquina virtual está encendida, no se recuperarán los cambios de datos realizados en la máquina virtual una vez que se haya iniciado el proceso de reconstrucción completa.

   - Si la máquina virtual que está recuperando está apagada, aparecerá el punto de recuperación en **Estado más reciente**.

6. Compruebe que se trata del punto de recuperación que desee restaurar y haga clic en **Siguiente**.

   Aparecerá la pantalla del asistente de reconstrucción completa con las opciones de modo de recuperación disponibles.



Las opciones disponibles son **Modo avanzado** y **Modo rápido**.

- Seleccione **Modo rápido** si desea una interacción mínima durante el proceso de recuperación. Para obtener más información, consulte Realización de la reconstrucción completa en el modo rápido.
- Seleccione **Modo avanzado** si desea personalizar el proceso de recuperación. Para obtener más información, consulte a Realización de la reconstrucción completa en el modo avanzado.

Valor predeterminado: Modo rápido.

Realización de la reconstrucción completa en el modo expreso

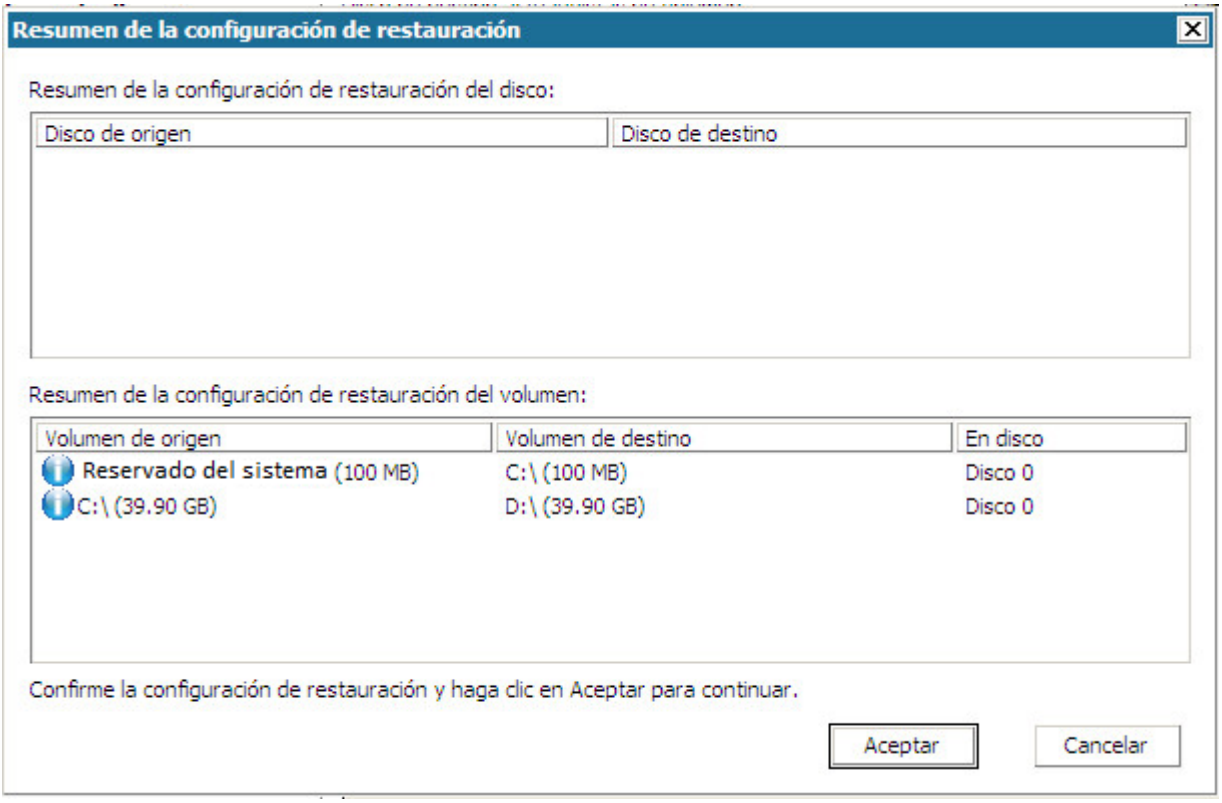
El **Modo rápido** requiere una interacción mínima durante el proceso de recuperación.

Siga estos pasos:

1. En el cuadro de diálogo **Seleccionar un modo de recuperación**, seleccione **Modo rápido** y haga clic en **Siguiente**.

   Aparecerá la pantalla **Resumen de la configuración de restauración del disco** que muestra un resumen de los volúmenes para restaurar.

   Nota: En la parte inferior de la ventana de resumen de restauración, las letras de unidad de la columna **Volumen de destino** se generan de forma automática desde el entorno de preinstalación de Windows (WinPE). Es posible que sean diferentes de las letras de unidad que se enumeran en la columna **Volumen de origen.** Sin embargo, los datos se restaurarán en el volumen adecuado incluso si las letras de unidad son diferentes.



2. Cuando haya comprobado que la información de resumen es correcta, haga clic en **Aceptar**.

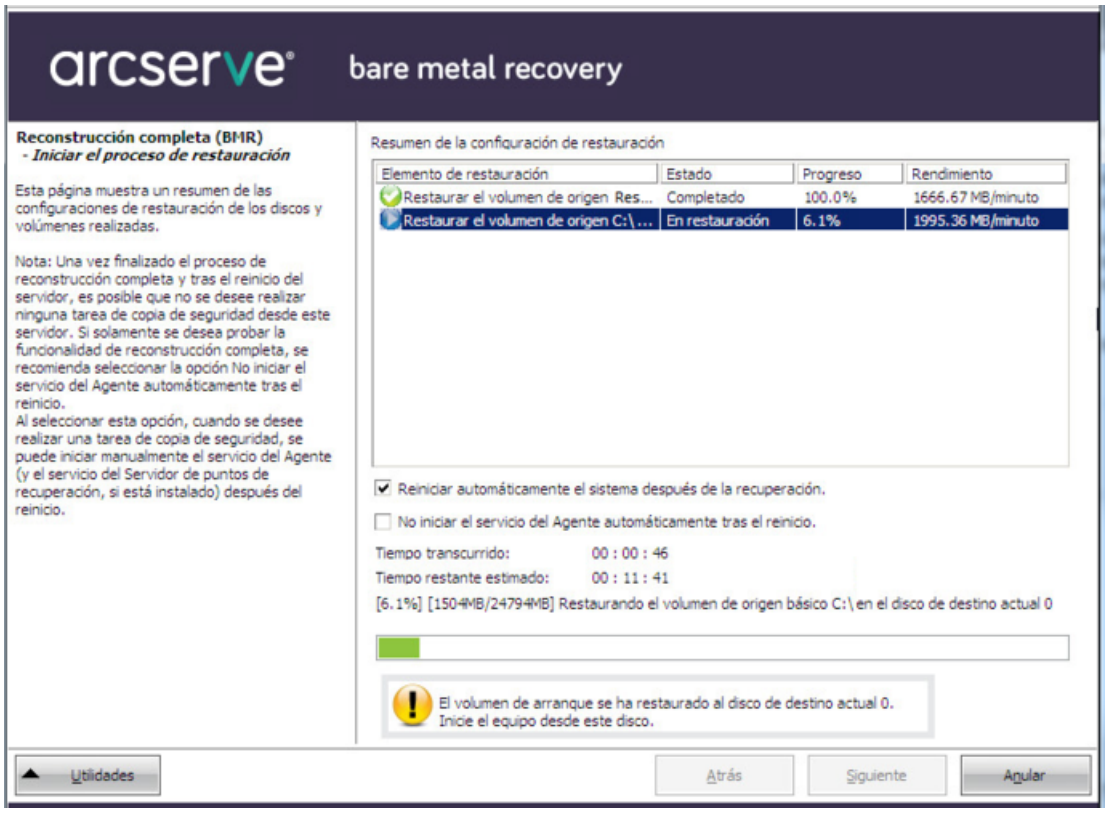
Se iniciará el proceso de restauración. La pantalla del asistente de reconstrucción completa mostrará el estado de restauración para cada volumen.

- Esta operación puede tardar unos minutos, según el tamaño del volumen restaurado.
- En el proceso se restauran por bloques todos los datos de los que había realizado copia de seguridad para el punto de recuperación y se crea, además, una réplica del equipo de origen en el equipo de destino.
- De forma predeterminada, se selecciona la opción de reiniciar el equipo de forma automática después de la recuperación. Si es necesario, es posible deseleccionar la opción y reiniciar el equipo manualmente más tarde.

  Importante: Si se realiza una restauración autoritativa de un Active Directory después de una reconstrucción completa, se debe eliminar la selección de la opción **Reiniciar automáticamente el sistema después de la recuperación** y para obtener más información, consulte Cómo realizar una restauración autoritativa de Active Directory después de una reconstrucción completa.

  - Si es necesario, se puede seleccionar No iniciar el servicio del agente automáticamente después del reinicio.
  - Si es necesario, tiene la opción de cancelar o abortar la operación en

cualquier momento.



3. Desde el menú **Utilidades** podrá acceder al **Registro de actividades** de reconstrucción completa y utilizar la opción **Guardar** para guardar el registro de actividad.

   De forma predeterminada, el registro de actividad se guardará en la ubicación siguiente:

   X:\windows\system32\dr\log.

   Nota: Para evitar obtener un error de Windows, no debe guardar el registro de actividad en el escritorio o crear una carpeta nueva en el escritorio usando la opción **Guardar como** de la ventana de registro de actividad de reconstrucción completa.

4. Si restaura un hardware diferente (el adaptador de SCSI/FC que se ha utilizado para conectar los discos duros puede haberse modificado) y no se ha detectado ningún tipo de controlador compatible en el equipo original, aparecerá la página de inserción de controladores para proporcionar los controladores para los dispositivos.

   Es posible buscar y seleccionar controladores para insertarlos en el sistema recuperado, de modo que incluso al realizar la recuperación en un equipo con un hardware diferente, todavía sea posible recuperar el equipo después de la reconstrucción completa.

5. Al finalizar el proceso de reconstrucción completa, aparecerá una notificación de confirmación.

Realización de la reconstrucción completa en el modo avanzado

El **Modo avanzado** permite personalizar el proceso de recuperación.

Siga estos pasos:

1. En el cuadro de diálogo **Seleccionar un modo de recuperación**, seleccione **Modo avanzado** y haga clic en **Siguiente**.

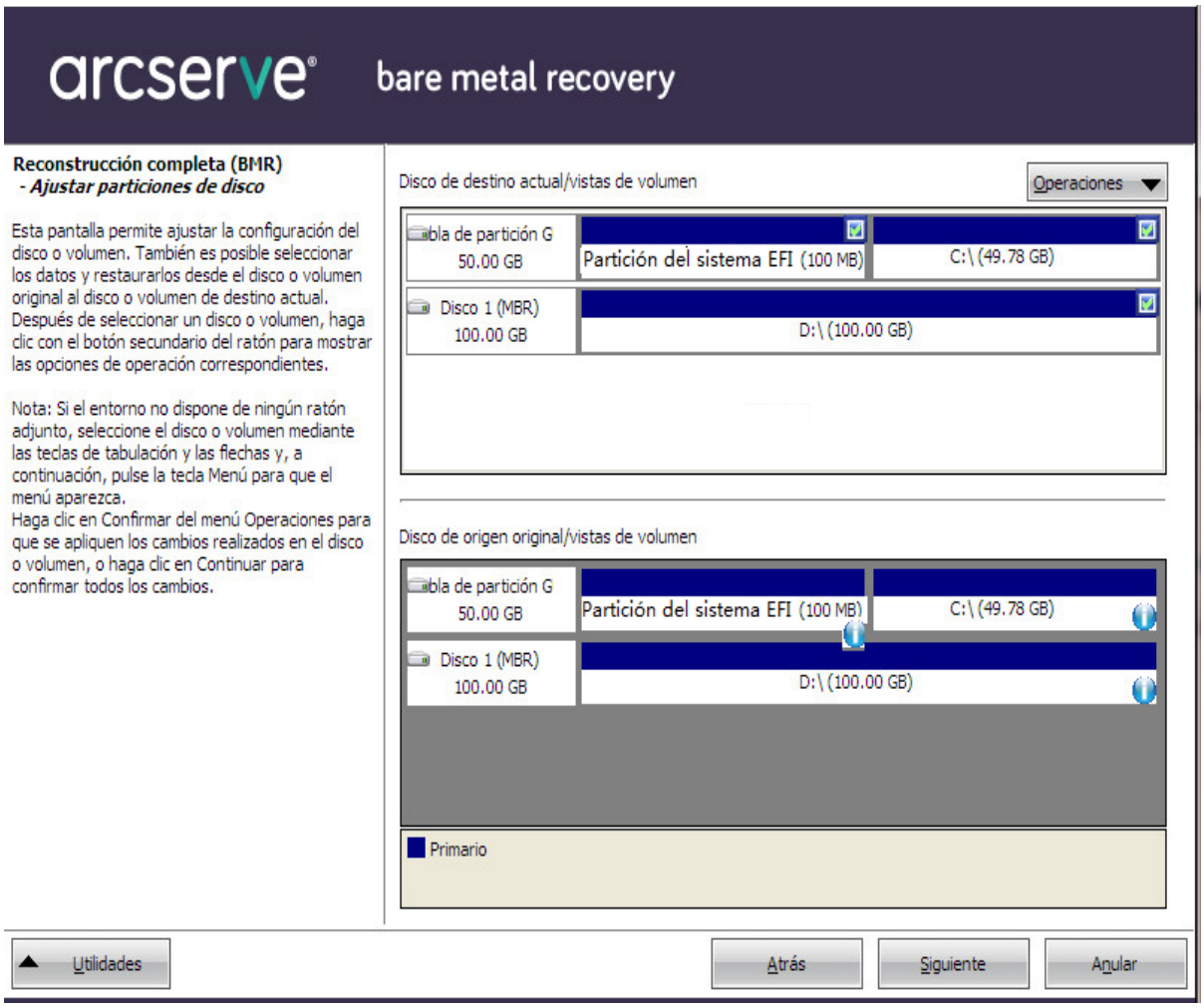
   La utilidad de reconstrucción completa se inicia buscando el equipo para recuperar y mostrará información de la partición de disco correspondiente.

   El panel superior muestra la configuración de disco que tiene en el equipo (de destino) actual y el panel inferior muestra la información de partición de disco que tenía en el equipo (de origen) original.

   Importante: Un icono X rojo que muestra un volumen de origen en el panel inferior indica que este volumen contiene información del sistema y no se ha asignado al volumen de destino. El volumen de información del sistema desde el disco de origen debe asignarse al disco de destino y restaurarse durante la reconstrucción completa o es posible que se produzca un error al reiniciar.

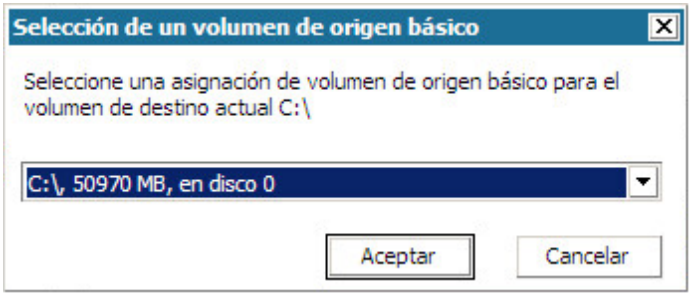
   Nota: Si se realiza la reconstrucción completa y se restaura el volumen del sistema en un disco que no está configurado como el disco de arranque, se producirá un error al inicializar el equipo después de que finalice la reconstrucción completa. Asegúrese de que se restaura el volumen del sistema en un disco de arranque configurado correctamente.

   Nota: Al restaurar en otro disco/volumen, la capacidad del nuevo disco/volumen debe ser del mismo tamaño o mayor que la del disco/volumen original. Además, el cambio de tamaño del disco es únicamente para los discos, no para los discos dinámicos.



2. Si la información de disco actual no es correcta, acceda al menú **Utilidades** y compruebe los posibles controladores que faltan.
3. Si es necesario, en el panel de volumen/disco de destino se puede hacer clic en el menú desplegable **Operaciones** para visualizar las opciones disponibles. Para obtener más información sobre estas opciones, consulte la sección Gestión del menú Operaciones de BMR.
4. Haga clic en todos los volúmenes de destino y, desde el menú emergente, seleccione la opción **Asignar volumen desde** para asignar un volumen de origen en el volumen de destino.

   Aparecerá el cuadro de diálogo **Seleccionar un volumen de origen básico**.

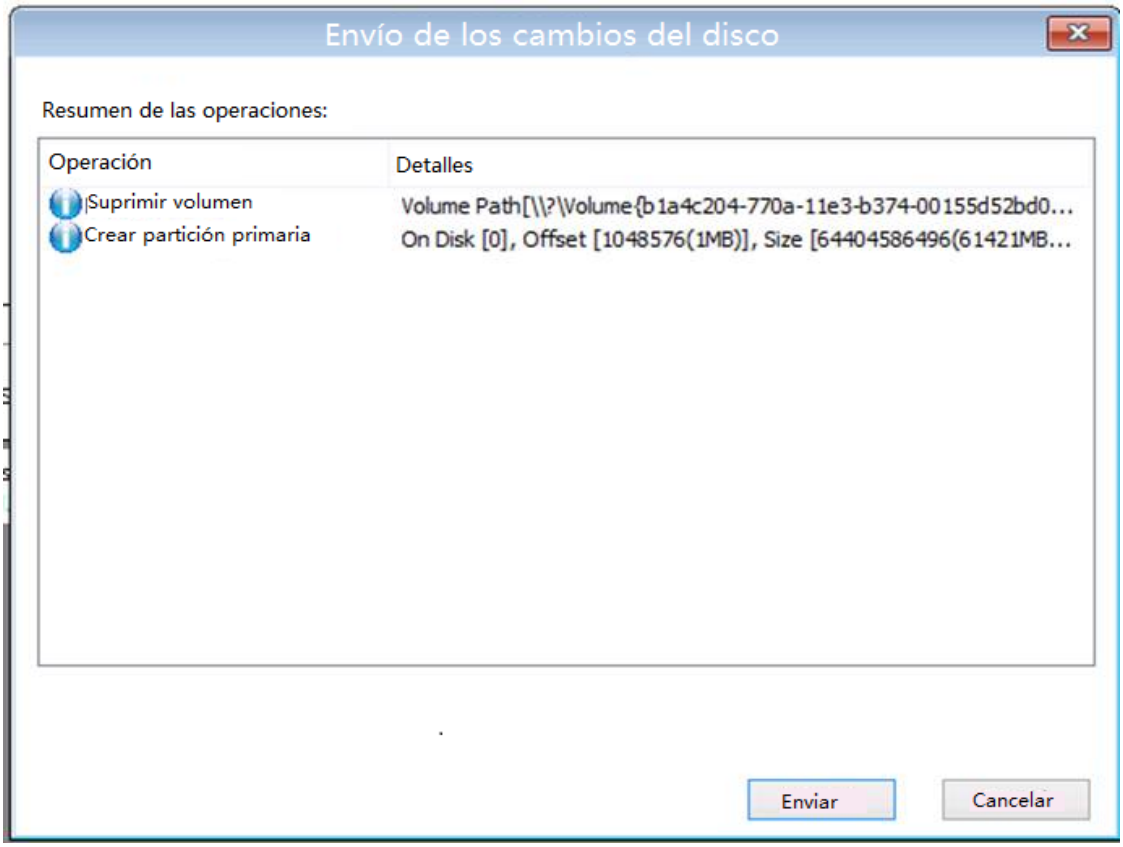


5. Desde el cuadro de diálogo **Seleccionar un volumen de origen básico**, haga clic en el menú desplegable y seleccione el volumen de origen disponible para asignar al volumen de destino seleccionado. Haga clic en **Aceptar**.

   - En el volumen de destino aparecerá una marca de verificación que indica que se ha asignado al volumen de destino.
   - En el volumen de origen, los cambios del icono con una X roja al icono verde indican que el volumen de origen se ha asignado a un volumen de destino.

6. Cuando esté seguro de que todos los volúmenes que desea restaurar y de que todos los volúmenes que contienen información del sistema están asignados a un volumen de destino, haga clic en **Siguiente**.

   Se mostrará la pantalla Enviar cambios de disco, que muestra un resumen de las operaciones seleccionadas. Aparecerá la información correspondiente a cada volumen nuevo creado.



7. Cuando haya comprobado que la información de resumen es correcta, haga clic en **Enviar**. (Si la información no es correcta, haga clic en **Cancelar**).

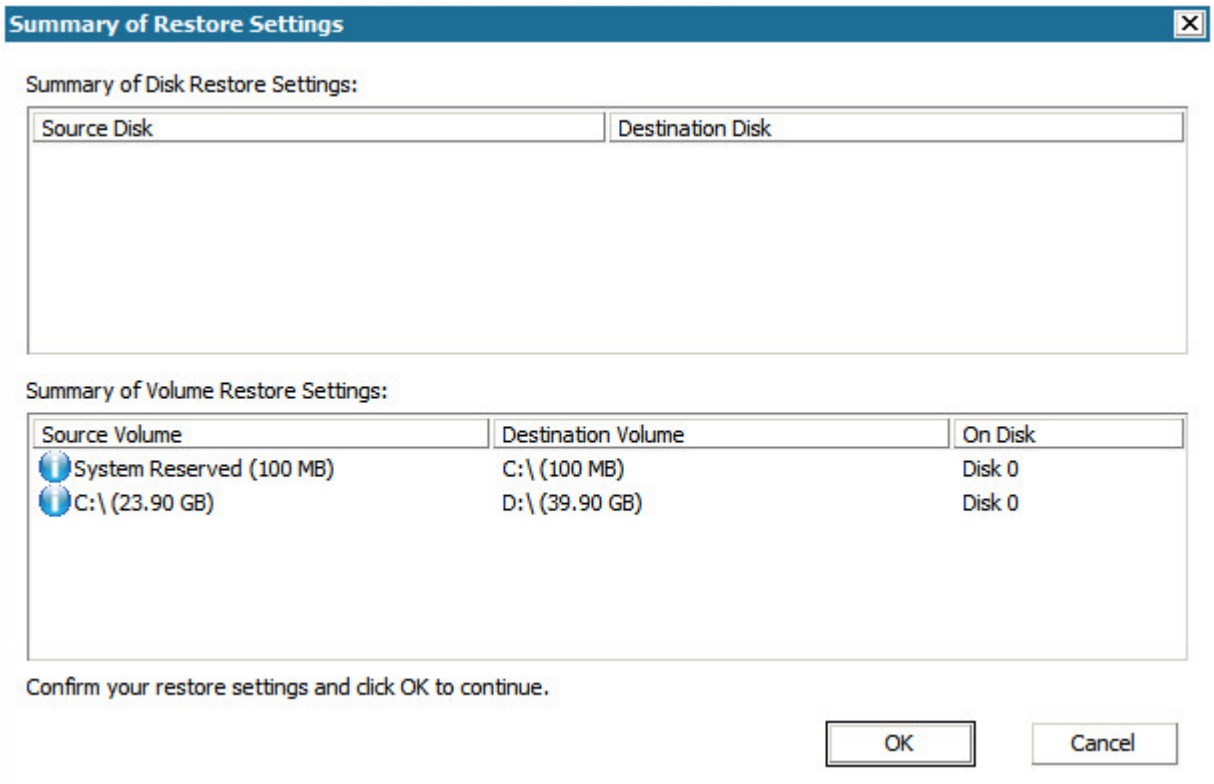
   Nota: Las operaciones en el disco duro no tendrán efecto hasta enviarlas.

   En el equipo de destino, los nuevos volúmenes se crean en el disco de destino y se asignan al equipo de origen correspondiente.

8. Cuando los cambios finalicen, haga clic en **Aceptar**.

   Aparecerá la pantalla Resumen de la configuración de restauración del disco que muestra un resumen de los volúmenes para restaurar.

   Nota: En la parte inferior de la ventana de resumen de restauración, las letras de unidad de la columna "Volumen de destino" se generan de forma automática desde el entorno de preinstalación de Windows (WinPE). Es posible que sean diferentes de las letras de unidad que se enumeran en la columna "Volumen de origen". Sin embargo, los datos se restaurarán en el volumen adecuado incluso si las letras de unidad son diferentes.

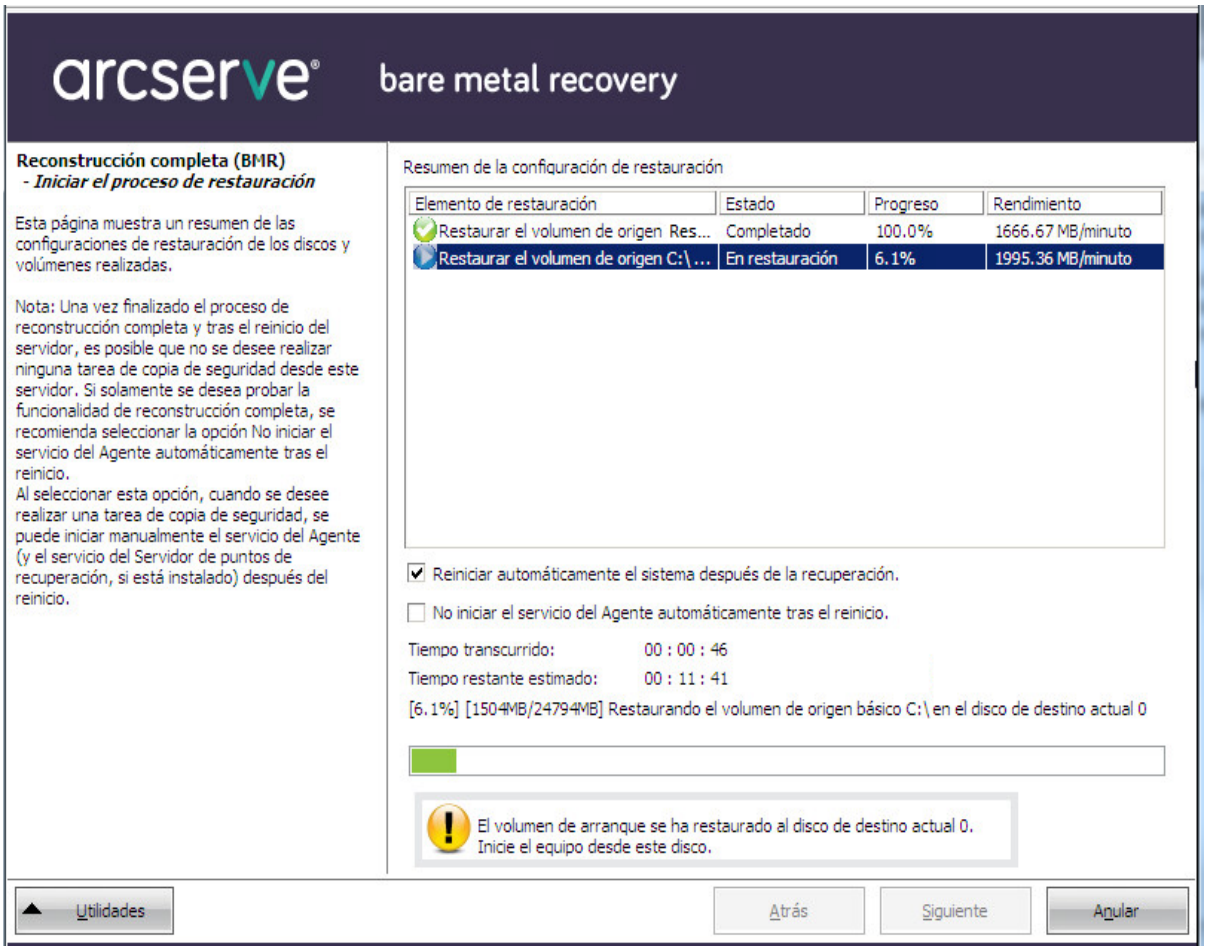


9. Cuando haya comprobado que la información de resumen es correcta, haga clic en **Aceptar**.

   Se iniciará el proceso de restauración. La pantalla del asistente de reconstrucción completa mostrará el estado de restauración para cada volumen.

- Esta operación puede tardar unos minutos, según el tamaño del volumen restaurado.
- En el proceso se restauran por bloques todos los datos de los que había realizado copia de seguridad para el punto de recuperación y se crea, además, una réplica del equipo de origen en el equipo de destino.
- De forma predeterminada, se selecciona la opción de reiniciar el equipo de forma automática después de la recuperación. Si es necesario, es posible deseleccionar la opción y reiniciar el equipo manualmente más tarde.

  Importante: Si se realiza una restauración autoritativa de un Active Directory después de una reconstrucción completa, se debe eliminar la selección de la opción **Reiniciar automáticamente el sistema después de la recuperación**. Para obtener más información, consulte Cómo realizar una restauración autoritativa de Active Directory después de una reconstrucción completa.
- Si es necesario, se puede seleccionar No iniciar el servicio del agente automáticamente después del reinicio.
- Si es necesario, tiene la opción de cancelar o abortar la operación en cualquier momento.



10. Desde el menú **Utilidades** podrá acceder al **Registro de actividades** de reconstrucción completa y utilizar la opción **Guardar** para guardar el registro de actividad.

    De forma predeterminada, el registro de actividad se guardará en la ubicación siguiente:

    X:\windows\system32\dr\log

    Nota: Para evitar obtener un error de Windows, no debe guardar el registro de actividad en el escritorio o crear una carpeta nueva en el escritorio usando la opción **Guardar como** de la ventana de registro de actividad de reconstrucción completa.

11. Si restaura un hardware diferente (el adaptador de SCSI/FC que se ha utilizado para conectar los discos duros puede haberse modificado) y no se ha detectado ningún tipo de controlador compatible en el equipo original, aparecerá la página de inserción de controladores para proporcionar los controladores para los dispositivos.

    Es posible buscar y seleccionar controladores para insertarlos en el sistema recuperado, de modo que incluso al realizar la recuperación en un equipo con un hardware diferente, todavía sea posible recuperar el equipo después de la reconstrucción completa.

12. Al finalizar el proceso de reconstrucción completa, aparecerá una notificación de confirmación.

Verificación de que la reconstrucción completa ha sido correcta

Para verificar si la reconstrucción completa ha sido correcta, realice las tareas siguientes:

- Reinicie el sistema operativo.
- Verifique que todos los sistemas y las aplicaciones funcionan correctamente.
- Verifique que todos los valores de configuración de la red están configurados correctamente.
- Verifique que la BIOS se ha configurado para arrancar desde el disco en el que se ha restaurado el volumen de arranque.
- Cuando se completa la reconstrucción completa, tenga en cuenta las siguientes condiciones:
  - La primera copia de seguridad que se realiza después de una reconstrucción completa es una copia de seguridad de verificación.
  - Una vez que el equipo haya reiniciado, es posible que sea necesario configurar los adaptadores de redes de manera manual si se ha realizado la restauración en un hardware diferente.

    Nota: Cuando se reinicia el equipo, aparecerá la pantalla Recuperación de errores de Windows indicando que Windows no se ha apagado correctamente. Si esto ocurre, se podrá ignorar esta advertencia de forma segura y continuar con el inicio de Windows del modo habitual.
  - Para discos dinámicos, si el estado del disco es sin conexión, éste se puede cambiar a en línea de forma manual desde la interfaz de usuario de gestión de discos (a la cual se accede mediante la ejecución de la utilidad de control Diskmgmt.msc).
  - Para discos dinámicos, si los volúmenes dinámicos están en estado de redundancia con errores, es posible volver a sincronizar los volúmenes de forma manual desde la interfaz de usuario de gestión de discos (a la cual se accede mediante la ejecución de la utilidad de control Diskmgmt.msc).

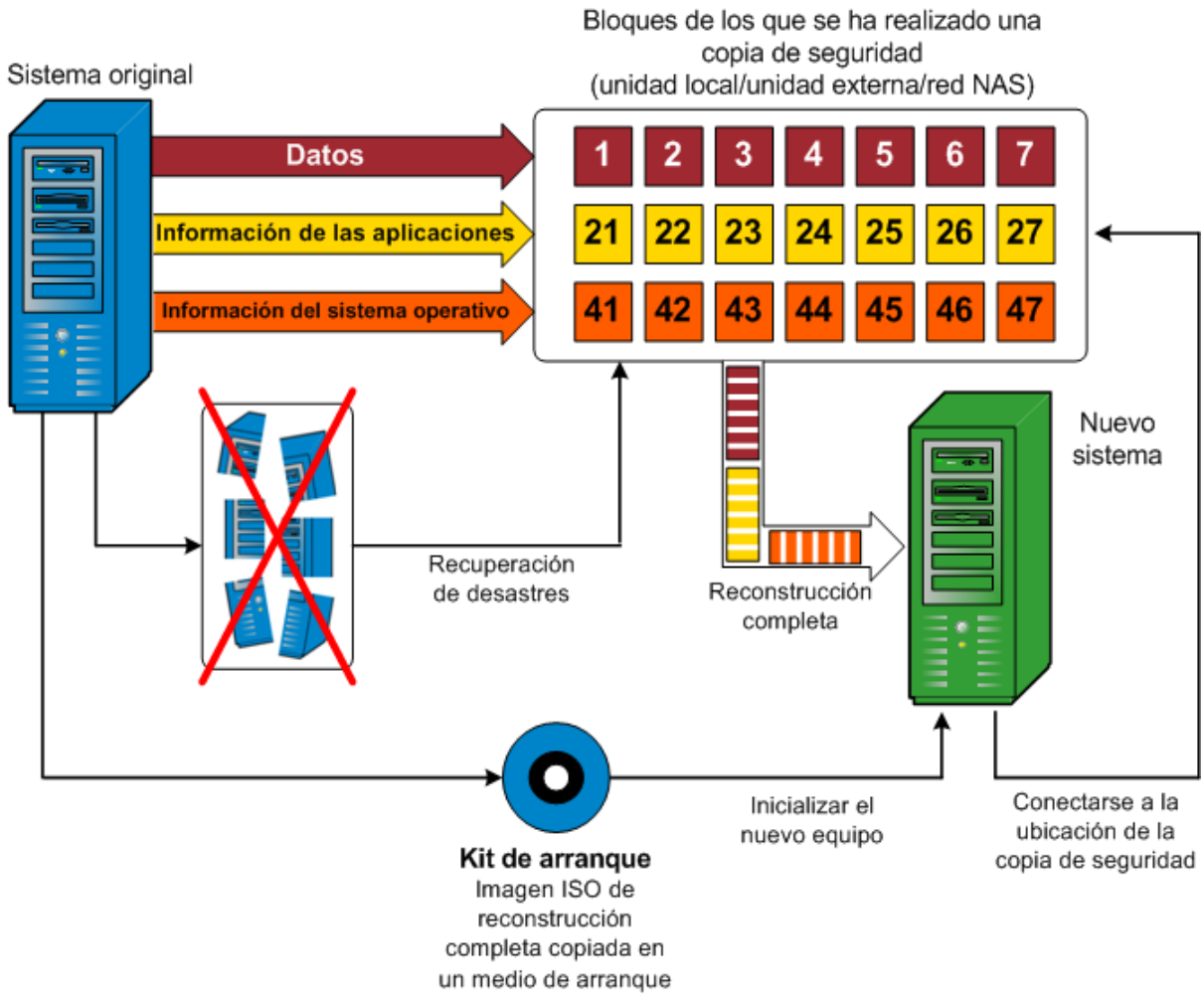
Información de referencia de la reconstrucción completa

- Cómo funciona la reconstrucción completa
- Sistemas operativos que admiten la conversión de UEFI/BIOS
- Gestión del menú Operaciones de BMR

Cómo funciona la reconstrucción completa

La reconstrucción completa es el proceso de restauración de un sistema desde la "reconstrucción completa" incluyendo la reinstalación del sistema operativo y de las aplicaciones de software, además de restaurar los datos y la configuración. Los motivos más comunes para realizar una reconstrucción completa son porque se produce un error en el disco duro o se llena y se desea actualizar (migrar) a una unidad mayor o migrar a un equipo de hardware más reciente. La reconstrucción completa es posible porque durante el proceso de copia de seguridad de nivel de bloque el Agente de Arcserve UDP (Windows) no solo captura los datos, sino toda la información relacionada con el sistema operativo, las aplicaciones instaladas, la configuración, los controladores necesarios, entre otros. Se realiza una copia de seguridad de toda la información relevante que es necesaria para realizar una compilación completa del sistema desde la reconstrucción completa en una serie de bloques que se almacenan en la misma ubicación que la copia de seguridad.

Nota: Los discos dinámicos sólo se restaurarán en el nivel de disco. Si se ha realizado la copia de seguridad de los datos en un volumen de un disco dinámico, no será posible restaurar este disco dinámico (incluidos sus volúmenes) durante la reconstrucción completa.



Cuando se realiza una reconstrucción completa se utiliza el disco de arranque del Agente de Arcserve UDP (Windows) para iniciar el sistema y permitir que comience el proceso de recuperación completa. Al iniciar la reconstrucción completa, el Agente de Arcserve UDP (Windows) solicitará que se seleccione o proporcione una ubicación válida desde la cual se podrán recuperar los bloques con copia de seguridad y también un punto de recuperación para la restauración. Si es necesario, también se solicitarán los controladores válidos para el nuevo sistema. Cuando se proporciona información de conexión y configuración, el Agente de Arcserve UDP (Windows) empieza a sacar la imagen de copia de seguridad específica desde la ubicación de copia de seguridad y a restaurar todos los bloques con copia de seguridad al nuevo sistema (los bloques vacíos no se restaurarán). Una vez se ha restaurado por completo la imagen de la reconstrucción completa en el nuevo sistema, el equipo volverá a estar en el estado en que se encontraba en el momento en que se realizó la última copia de seguridad y se podrán continuar las copias de seguridad del Agente de Arcserve UDP (Windows) según lo programado. (Después de la reconstrucción completa, la primera copia de seguridad será una Copia de seguridad de verificación).

Sistemas operativos que admiten la conversión de UEFI/BIOS

Si se detecta que el sistema operativo del equipo de origen no es el mismo firmware que el del sistema, se solicitará al usuario si desea convertir UEFI en un sistema compatible con BIOS-compatible o BIOS en sistema compatible con UEFI. La tabla siguiente clasifica todos los sistemas operativos y el tipo de conversión compatible:

Usuario del sistema operativo (SO)	CPU	uEFI a BIOS	BIOS a uEFI
Microsoft Windows (ningún SP)	x86	No	No
Microsoft Windows (ningún SP)	x64	No	No
Windows Vista SP1	x86	No	No
Windows Vista SP1	x64	Sí	Sí
Windows Server 2008	x86	No	No
Windows Server 2008	x64	Sí	Sí
Windows Server 2008 R2	x64	Sí	Sí
Windows 7	x86	No	No
Windows 7	x64	Sí	Sí
Windows 8	x86	No	No
Windows 8	x64	Sí	Sí
Windows Server 2012	x64	Sí	Sí
Windows 8.1	x86	No	No
Windows 8.1	x64	Sí	Sí
Windows 10	x86	No	No
Windows 10	x64	Sí	Sí
Windows Server 2012 R2	x64	Sí	Sí
Windows Server 2016	x64	Sí	Sí
Windows Server 2019	x64	Sí	Sí

Gestión del menú Operaciones de BMR

El menú Operaciones de BMR está formado por los tres tipos de operaciones siguientes:

- Operaciones específicas del disco
- Operaciones específicas de Volume/Partition
- Operaciones específicas de reconstrucción completa

Operaciones específicas del disco:

Para realizar operaciones específicas del disco, seleccione el encabezado de disco y haga clic en **Operaciones**.

Limpiar disco

Esta operación se utiliza y es para limpiar todas las particiones de un disco y es

- un método alternativo para suprimir todos los volúmenes de un disco. Con la operación **Limpiar disco** no es necesario suprimir cada volumen uno a uno.
- Se utiliza para suprimir las particiones que no sean de Windows. Debido a una limitación de VDS, no se puede suprimir la partición que no es de Windows de la IU, pero se puede utilizar esta operación para limpiarlas todas.

  Nota: Durante la reconstrucción completa, cuando el disco de destino tiene particiones que no son de Windows o particiones de OEM, no se puede seleccionar esta partición y suprimirla de la IU de reconstrucción completa. Normalmente esto ocurriría cuando se instalaba Linux/Unix en el disco de destino. Para solucionar este problema, se deben realizar las tareas siguientes:
- Seleccione el encabezado de disco en la IU de reconstrucción completa, haga clic en **Operaciones** y utilice la operación **Limpiar disco** para borrar todas las particiones del disco.
- Abra un símbolo del sistema y escriba **Diskpart** para abrir la consola de comandos de Diskpart. Después escriba "seleccionar disco X" , donde "X" es el número del disco, y "limpiar" para borrar todas las particiones del disco.

Convertir en MBR

Esta operación se utiliza para convertir un disco en MBR (registro de arranque maestro). Está disponible solamente cuando el disco seleccionado es un

disco de tabla de partición GUID (GPT) y no hay ningún volumen en este disco.

Convertir en tabla de partición GUID

Esta operación se utiliza para convertir un disco en una tabla de partición GUID. Está disponible solamente cuando el disco seleccionado es un disco de MBR y no hay ningún volumen en este disco.

Convertir en básico

Esta operación se utiliza para convertir un disco en básico. Está disponible solamente cuando el disco seleccionado es un disco dinámico y no hay ningún volumen en este disco.

Convertir en dinámico

Esta operación se utiliza para convertir un disco en un disco dinámico. Está disponible solamente cuando el disco seleccionado es un disco básico.

Disco en línea

Esta operación se utiliza para conectar el disco. Está disponible solamente cuando el disco seleccionado está en estado sin conexión.

Propiedades de disco

Esta operación se utiliza para ver las propiedades detalladas del disco. Está siempre disponible, y cuando se selecciona esta operación aparece un cuadro de diálogo **Propiedades de disco**.

Operaciones específicas de Volume/Partition:

Para realizar operaciones de volumen/partición, seleccione el área del cuerpo de disco y haga clic en **Operaciones**. Desde este menú se pueden crear nuevas particiones para que se correspondan con las particiones de disco en el volumen de origen.

Crear partición primaria

Esta operación se utiliza para crear una partición en un disco básico. Está disponible solamente cuando el área seleccionada es un espacio en disco no adjudicado.

Crear partición lógica

Esta operación se utiliza para crear una partición lógica en un disco básico de MBR. Está disponible solamente cuando el área seleccionada es una partición extendida.

Crear partición extendida

Esta operación se utiliza para crear una partición extendida en un disco básico de MBR. Está disponible solamente cuando el disco es un disco de MBR y el área seleccionada es un espacio en disco no adjudicado.

Crear una partición reservada del sistema

Esta operación se utiliza para crear la partición reservada del sistema en un sistema de firmware de BIOS y construye una relación de asignación con la partición del sistema de EFI de origen. Está disponible solamente cuando se restaura un sistema de UEFI en un sistema de BIOS.

Nota: Si ha realizado la conversión previamente de UEFI a un sistema compatible con BIOS, utilice la opción operación Crear una partición reservada del sistema para cambiar el tamaño del disco de destino.

Crear partición del sistema de EFI

Esta operación se utiliza para crear la partición del sistema de EFI en un disco básico de GPT. Está disponible solamente cuando el firmware del equipo de destino es UEFI y el disco seleccionado es un disco básico de GPT.

Nota: Si ha realizado la conversión previamente de BIOS a un sistema compatible con BIOS, utilice la operación Crear partición del sistema de EFI para cambiar el tamaño del disco de destino.

Nota: Los sistemas compatibles con UEFI también requieren que la partición de arranque resida en un disco de GPT (tabla de particiones GUID). Si utiliza un disco de MBR (registro de arranque maestro), se debe convertir este disco en un disco de GPT y, a continuación, utilizar la operación Crear partición del sistema de EFI para cambiar el tamaño del disco.

Cambiar el tamaño del volumen

Esta operación se utiliza para cambiar el tamaño de un volumen. Es un método alternativo de Windows "Extender volumen/Reducir volumen". Está disponible solamente cuando el área seleccionada es una partición de disco válida.

Suprimir el volumen

Esta operación se utiliza para suprimir un volumen. Está disponible solamente cuando el área seleccionada es un volumen válido.

Suprimir la partición extendida

Esta operación se utiliza para suprimir la partición extendida. Está disponible solamente cuando el área seleccionada es una partición extendida.

Propiedades del volumen

Esta operación se utiliza para ver las propiedades detalladas del volumen. Cuando se selecciona esta operación, aparece el cuadro de diálogo **Propiedades del volumen**.

Operaciones específicas de BMR:

Estas operaciones son específicas de BMR. Para realizar operaciones de reconstrucción completa, seleccione el encabezado de disco o el área del cuerpo de disco y haga clic en **Operaciones**.

Asignar disco desde

Esta operación se utiliza para construir una relación de asignación entre los discos dinámicos de origen y de destino. Está disponible solamente cuando el disco seleccionado es un disco dinámico.

Nota: Al asignar a otro disco, la capacidad de cada volumen de destino asignado debe ser del mismo tamaño o mayor que la del volumen de origen correspondiente.

Asignar volumen desde

Esta operación se utiliza para construir una relación de asignación entre el volumen básico de origen y de destino. Está disponible solamente cuando el volumen seleccionado es un volumen básico.

Nota: Al asignar a otro disco, la capacidad de cada volumen de destino asignado debe ser del mismo tamaño o mayor que la del volumen de origen correspondiente.

Confirmar

Esta operación está siempre disponible. Todas las operaciones se guardan en la memoria caché y no modifican los discos de destino hasta que se selecciona la operación **Confirmar**.

Restablecer

Esta operación está siempre disponible. La operación **Restablecer** se utiliza para cancelar las operaciones y restaurar el diseño del disco a su estado predeterminado. Esta operación limpia todas las operaciones guardadas en la memoria caché. Restablecer significa volver a cargar la información de diseño del disco de destino y de origen desde el archivo de configuración y el sistema operativo actual, y rechazar cualquier información de diseño del disco modificado por el usuario.

Solución de problemas relacionados con la recuperación completa

Al detectar un problema, el Agente de Arcserve UDP (Windows) genera un mensaje para ayudarle a identificar y resolver el problema. El **registro de actividades** del Agente de Arcserve UDP (Windows) contiene estos mensajes. Se puede acceder a él a través de la opción **Ver registros** que se encuentra en la interfaz de usuario de la página principal. Además, cuando se intenta llevar a cabo una acción incorrecta, el Agente de Arcserve UDP (Windows) suele mostrar un mensaje emergente que le ayuda a identificar el problema y resolverlo de forma rápida.

- Rendimiento lento durante la reconstrucción completa
- Después de la reconstrucción completa, el sistema operativo no reconoce volúmenes dinámicos.
- Imposibilidad de reiniciar la máquina virtual de Hyper-V después de la reconstrucción completa
- Imposibilidad de reiniciar la máquina virtual de VMware después de la reconstrucción completa
- No se puede iniciar el servidor después de realizar una reconstrucción completa.
- Se ha producido un error al enviar la tarea de reconstrucción completa al servidor de punto de recuperación

Rendimiento lento durante la reconstrucción completa

Este problema puede estar causado porque los controladores de SATA tienen AHCI activado.

Durante la reconstrucción completa, el Agente de Arcserve UDP (Windows) instalará controladores para dispositivos desconocidos importantes. Si el dispositivo ya tiene un controlador instalado, el Agente de Arcserve UDP (Windows) no actualizará el controlador de nuevo. Para algunos dispositivos, Windows 7PE puede disponer de controladores, pero estos controladores pueden no ser los mejores y provocar que la reconstrucción completa se ejecute de manera lenta.

Para solucionar este problema, se deben realizar las tareas siguientes:

- Compruebe si la carpeta de agrupación de controlador contiene los controladores de disco más nuevos. Si es así y realiza una restauración en el equipo original, instale el controlador nuevo desde la carpeta de agrupación de controlador. Si se realiza una restauración en un equipo alternativo, descargue los últimos controladores de disco de Internet y cárguelos antes de iniciar la recuperación de datos. Para cargar el controlador, puede utilizar la utilidad "drvload.exe", que se incluye en PE de Windows.
- Cambie el modo operativo del dispositivo de Interfaz avanzada de controlador de host (AHCI) a modo de compatibilidad. (El modo de compatibilidad proporciona un mejor rendimiento).

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Después de la reconstrucción completa, el sistema operativo no reconoce los volúmenes dinámicos

Para guardar discos dinámicos de forma coherente, el sistema operativo de Windows sincroniza automáticamente los metadatos del Administrador de discos lógicos (LDM) en cada disco dinámico. De modo que cuando la reconstrucción completa restaura un disco dinámico y lo conecta, el sistema operativo actualizará automáticamente los metadatos de LDM en este disco. Esto puede dar lugar a que el sistema operativo no reconozca un volumen dinámico y que falte después del reinicio.

Para solucionar este problema, al realizar la reconstrucción completa con discos dinámicos múltiples, no deben realizarse operaciones de disco previas de reconstrucción completa como la limpieza, la supresión de un volumen, etc.

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Imposibilidad de reiniciar la máquina virtual de Hyper-V después de la reconstrucción completa

Si ha realizado una reconstrucción completa en un equipo de Hyper-V formado por más de un disco conectado a un controlador de Electrónica de Dispositivo Integrada (IDE), y el servidor no se reinicia, realice el siguiente procedimiento de solución de problemas:

1. Compruebe que el disco que contiene el volumen del sistema es el disco principal.

   La BIOS Hyper-V busca el volumen del sistema en el disco principal (disco 1) que está conectado al canal principal. Si el volumen del sistema no está ubicado en el disco principal, la máquina virtual no se reiniciará.

   Nota: Verifique que el disco que contiene el volumen del sistema esté conectado a un controlador de IDE. Hyper-V no puede reiniciarse desde un disco de SCSI.

2. Si es necesario, modifique la configuración de Hyper-V para conectarse al disco que contiene el volumen del sistema al canal principal de IDE y reinicie de nuevo la máquina virtual.

   Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Imposibilidad de reiniciar la máquina virtual de VMware después de la reconstrucción completa

Si ha realizado una reconstrucción completa en un equipo de VMware formado por más de un disco conectado a un controlador de Electrónica de Dispositivo Integrada (IDE) o un adaptador de SCSI y el servidor no se reinicia, realice el siguiente procedimiento de resolución de problemas:

1. Compruebe que el disco que contiene el volumen del sistema es el disco principal.

   La BIOS VMware busca el volumen del sistema en el disco principal (disco 0) que está conectado al canal principal. Si el volumen del sistema no está ubicado en el disco principal, la máquina virtual no se reiniciará.

2. Si es necesario, modifique la configuración de VMware para conectarse al disco que contiene el volumen del sistema al canal principal de IDE y reinicie de nuevo la máquina virtual.

3. Si el disco es SCSI, compruebe que el disco que contiene el volumen de arranque sea el primer disco que se conecte al adaptador de SCSI. Si no, asigne al disco de arranque desde la BIOS de VMware.

4. Asegúrese de que el disco que contiene el volumen de arranque sea uno de los ocho primeros, dado que la BIOS de VMware sólo detecta 8 discos durante el arranque. Si existen más de 7 discos en el disco que contienen volúmenes del sistema conectados al adaptador de SCSI, la máquina virtual no podrá reiniciarse.

   Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

No se puede iniciar el servidor después de realizar una reconstrucción completa.

Síntoma

Cuando el equipo de origen es un servidor Active Directory que realiza una reconstrucción completa en una máquina física con un hardware distinto o a una máquina virtual en un servidor Hyper-V, el servidor no se inicia y aparecerá una pantalla azul con el siguiente mensaje:

DETENCIÓN: los servicios del directorio c00002e2 no podrán iniciarse a causa del error siguiente: no funciona el dispositivo adjunto al sistema. Estado del error: 0xc0000001.

Solución

Reinicie el sistema en el entorno PE de BMR, cambie el nombre de todos los archivos *.log en la carpeta C:\Windows\NTDS y reinicie el sistema. Por ejemplo, renombre el archivo edb.log a edb.log.old y reinicie el sistema.

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Se ha producido un error al enviar la tarea de reconstrucción completa al servidor de punto de recuperación

Solamente se es compatible con una tarea de reconstrucción completa cuando se restaura desde el mismo servidor de punto de recuperación para el mismo nodo (copia de seguridad del agente o copia de seguridad basada en host). El controlador de tareas controla esta acción en el servidor de punto de recuperación.

Si el equipo donde la tarea de reconstrucción completa se está ejecutando se cierra o reinicia inesperadamente, el controlador de tareas del servidor de punto de recuperación esperará 10 minutos y, a continuación, se excederá el tiempo de espera. Durante este tiempo no se puede iniciar otra reconstrucción completa para el mismo nodo del mismo servidor de punto de recuperación.

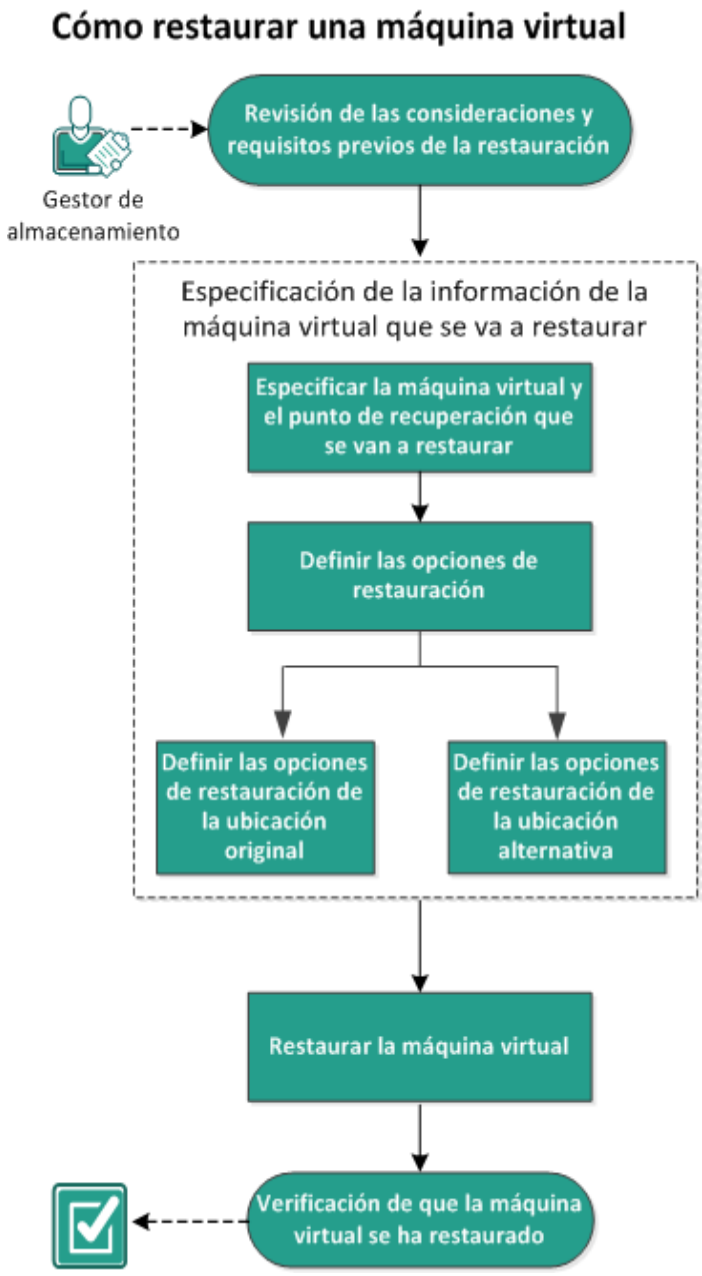
Si se anula la reconstrucción completa desde la interfaz de usuario de la reconstrucción completa, este problema no existe.

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Cómo restaurar una máquina virtual

Arcserve UDP permite utilizar la opción **Recuperar máquina virtual** para restaurar una máquina virtual de la cual se ha realizado la copia de seguridad previamente utilizando la copia de seguridad sin agente basada en el host. Este método le ayudará a restaurar toda la máquina virtual a la ubicación original o a una ubicación de ESX o Hyper-V alternativa. Se pueden explorar los puntos de recuperación de máquinas virtuales disponibles en una vista de calendario y seleccionar qué punto de recuperación desea restaurar.

El diagrama siguiente muestra el proceso para restaurar desde una máquina virtual:



Realice las tareas siguientes para restaurar una máquina virtual:

1. Revisión de las consideraciones y requisitos previos de la restauración
2. Especificación de la información de la máquina virtual que se va a restaurar
    a. Especificación de la máquina virtual y del punto de recuperación que se van a restaurar
    b. Definición de las opciones de restauración
        - Definición de las opciones de restauración de la ubicación original
        - Definición de las opciones de restauración de la ubicación alternativa
3. Restauración de la máquina virtual
4. Verificación de que la máquina virtual se ha restaurado

Revisión de las consideraciones y requisitos previos de la restauración

Verifique que los requisitos previos siguientes existen antes de realizar una restauración:

- Tiene un punto de recuperación válido disponible desde el cual llevar a cabo la restauración.
- Tiene un destino válido y accesible en el servidor de Virtual Center/ESX o Hyper-V para recuperar la máquina virtual.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones sobre la restauración:

- Si el destino Recuperar máquina virtual es Windows Server 2008 R2, entonces la máquina virtual de la copia de seguridad de origen no debe contener discos de VHDx, que no se admiten en el servidor Hyper-V (Windows Server 2008 R2).
- Si el destino Recuperar máquina virtual es Windows Server 2008 R2 o Win2012, entonces el tipo subsistema de la máquina virtual de la copia de seguridad de origen no debe ser de la generación 2 (que se ha introducido en Windows Server 2012 R2) y no se admite en el servidor Hyper-V (Windows Server 2012/2008 R2).

Especificación de la información de la máquina virtual que se va a restaurar

Se puede restaurar toda una máquina virtual a partir de un punto de recuperación.

El proceso implicado en la restauración de la máquina virtual es el siguiente:

1. Especificación de la máquina virtual y del punto de recuperación que se van a restaurar
2. Definición de las opciones de restauración
   - Definición de las opciones de restauración de la ubicación original
   - Definición de las opciones de restauración de la ubicación alternativa

Especificación de la máquina virtual y del punto de recuperación que se van a restaurar

Utilice la opción **Recuperar máquina virtual** para restaurar una máquina virtual de la cual se ha realizado una copia de seguridad previamente. Este método crea rápida y coherentemente una máquina virtual a partir de un punto de recuperación de Arcserve UDP en un servidor ESX o Hyper-V. La máquina virtual recuperada se puede iniciar a continuación para completar el proceso de recuperación.

Siga estos pasos:

1. Acceda al cuadro de diálogo Selección del método de recuperación de una de las formas siguientes:

   Desde Arcserve UDP:

   a. Inicie sesión en Arcserve UDP.

   b. Haga clic en la ficha **recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos agregados en el panel central.

   d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   e. Haga clic en **Restaurar** de la opción desplegable **Acción**.

      El cuadro de diálogo Selección del método de restauración se abre.

      Nota: Se inicia sesión automáticamente en el nodo del Agente y el cuadro de diálogo Selección del método de restauración se abre desde el nodo del Agente.

   Desde el Agente de Arcserve UDP (Windows):

   a. Inicie sesión en el Agente de Arcserve UDP (Windows).

   b. En la página principal, seleccione **Restaurar**.

   El cuadro de diálogo Selección del método de restauración se abre.

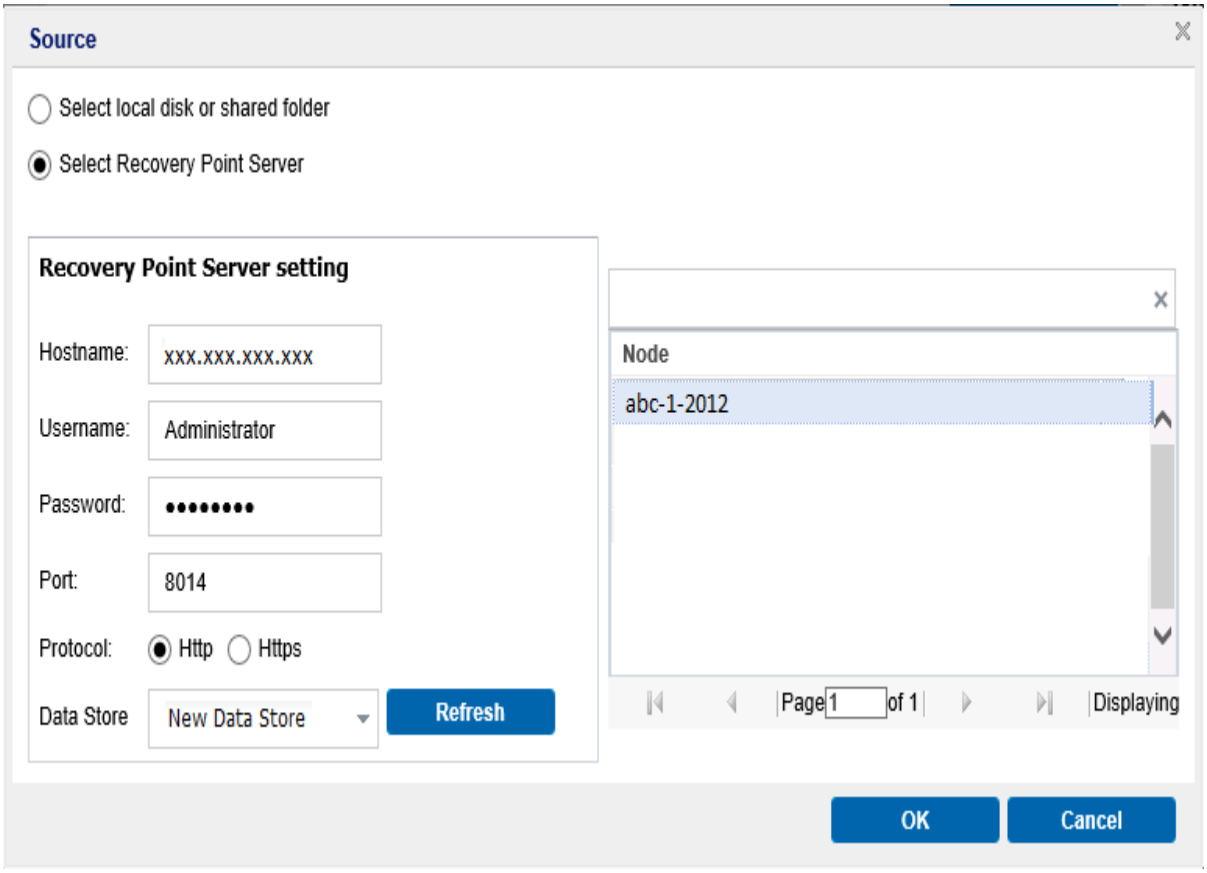
2. Haga clic en la opción **Recuperar máquina virtual**.

   Se abre el cuadro de diálogo **Recuperar máquina virtual**.



3. Haga clic en **Cambiar** para cambiar la ubicación de la copia de seguridad.

   Se abrirá el cuadro de diálogo **Origen.** Se puede seleccionar la ubicación de la copia de seguridad en este cuadro de diálogo.



4. Seleccione una de las opciones siguientes:

   Seleccionar disco local o carpeta compartida

   a. Especifique o vaya a la ubicación donde se almacenan las imágenes de copia de seguridad y seleccione el origen de la copia de seguridad adecuado.

      Se puede hacer clic en el botón de la flecha verde para comprobar la conexión con la ubicación especificada. Si es necesario, también puede escribir las credenciales de Nombre de usuario y Contraseña para obtener acceso a dicha ubicación de origen.

      El cuadro de diálogo **Selección de la ubicación de la copia de seguridad** se abre.

   b. Seleccione la carpeta en la cual se almacenan los puntos de recuperación y haga clic en **Aceptar**.

El cuadro de diálogo **Selección de la ubicación de la copia de seguridad** se cierra y se puede ver la ubicación de la copia de seguridad en el cuadro de diálogo **Origen**.

c. Haga clic en **Aceptar**.

Los puntos de recuperación se enumeran en el cuadro de diálogo **Recuperar máquina virtual**.

Seleccionar servidor de puntos de recuperación

a. Especifique los detalles del valor de configuración del servidor de puntos de recuperación y haga clic en **Actualizar**.

Todos los nodos (agentes/máquinas virtuales) se enumeran en la columna Nodo en el cuadro de diálogo **Origen.**

b. Seleccione el nodo (agente/máquina virtual) de la lista mostrada y haga clic en **Aceptar**.

Los puntos de recuperación se enumeran en el cuadro de diálogo **Recuperar máquina virtual**.

5. Desde el menú desplegable **Máquina virtual**, seleccione la máquina virtual que se debe recuperar.

La vista de calendario aparece y todas las fechas que contienen puntos de recuperación para el origen de la copia de seguridad especificado se resaltan en verde.

6. Seleccione la fecha de calendario para la imagen de la máquina virtual que desee restaurar.

Aparecerán los puntos de recuperación correspondientes para la fecha, junto con la hora de la copia de seguridad, el tipo de copia de seguridad que se realiza y el nombre de la copia de seguridad.

7. Seleccione un punto de recuperación para restaurar.

Se muestra el contenido de la copia de seguridad (incluyendo cualquier aplicación) del punto de recuperación seleccionado. Al restaurar una máquina virtual, se restaurará todo el sistema. Como resultado, se pueden ver, aunque no seleccionar, volúmenes, carpetas o archivos de dentro de la máquina virtual seleccionada.

Nota: El icono de un reloj con el símbolo de un candado indica que el punto de recuperación contiene información cifrada y que puede requerir una contraseña para realizar la restauración.

8. Haga clic en **Siguiente**.

Se abrirá el cuadro de diálogo **Opciones de restauración**.

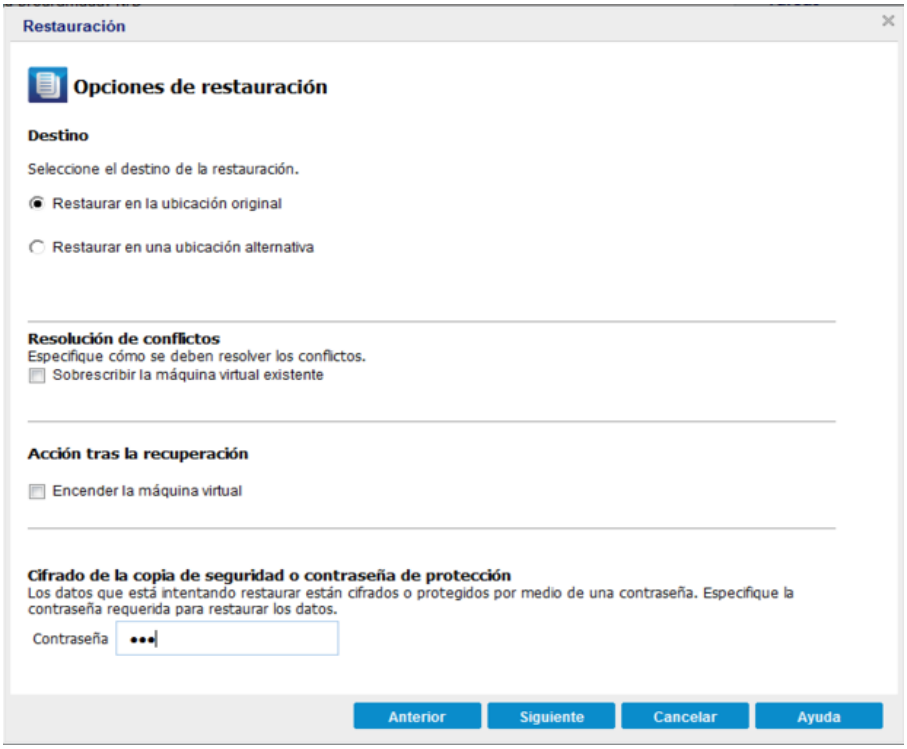
Se especifican la máquina virtual y el punto de recuperación que se van a restaurar.

Definición de las opciones de restauración

Después de especificar la máquina virtual y el punto de recuperación que se deben restaurar, defina las opciones de restauración para la imagen de la máquina virtual seleccionada.

Siga estos pasos:

1. En el cuadro de diálogo Opciones de restauración, seleccione el destino para la restauración.



A continuación se especifican las opciones de destino disponibles:

Restauración en la ubicación original

Restaura la máquina virtual en la ubicación original desde la que se ha capturado la imagen de la copia de seguridad. De forma predeterminada, esta opción está activada.

Para obtener más información, consulte Definición de las opciones de restauración de la ubicación original.

Restaurar en una ubicación alternativa

Restaura la máquina virtual en una ubicación distinta de la ubicación en la cual se capturó la imagen de la copia de seguridad.

Para obtener más información, consulte Definición de las opciones de restauración de la ubicación alternativa.

2. (Opcional) Seleccione la casilla de verificación **Utilizar la red del servidor de puntos de recuperación seleccionada para el tráfico de la restauración** y, a continuación, realice lo siguiente:

   a. Para activar la comunicación entre el servidor proxy de Windows y el servidor de puntos de recuperación, seleccione la red CIDR en el menú desplegable.

   b. Para definir la restricción en la función SMB multicanal para que los datos se transfieran solo a través de la red seleccionada, seleccione la casilla de verificación **Utilizar una red Ethernet dedicada si el equipo actual permite SMB multicanal**.

      Notas:

      - Esta opción no se encuentra disponible de forma determinada. Para activar esta opción, cree el registro de la cadena *UseDedicatedEthernet* en la ruta siguiente y, a continuación, establezca el valor del registro en 1:

        SOFTWARE\Arcserve\Unified Data Protection\Engine

      - Cuando realice una tarea de restauración desde la página Nodos, cree una clave de registro en el proxy de la copia de seguridad.
      - Cuando se realiza una tarea de restauración desde el agente normal mediante la sesión de la copia de seguridad del servidor de puntos de recuperación, cree una clave de registro en el agente normal.

3. (Opcional) Seleccione la casilla de verificación **Utilizar la red del servidor proxy seleccionada para el tráfico de la restauración** y, a continuación, realice lo siguiente:

   a. Para activar la comunicación entre el servidor proxy de Windows y el hipervisor, seleccione la red CIDR en el menú desplegable.

   b. Para definir la restricción en la función SMB multicanal para que los datos se transfieran solo a través de la red seleccionada, seleccione la casilla de verificación **Utilizar una red Ethernet dedicada si el equipo actual permite SMB multicanal**.

      Notas:

      - Esta opción no se encuentra disponible de forma determinada. Para activar esta opción, cree el registro de la cadena *UseDedicatedEthernet* en la ruta siguiente y, a continuación, establezca el valor del registro en 1:

        SOFTWARE\Arcserve\Unified Data Protection\Engine

- Cuando realice una tarea de restauración desde la página Nodos, cree una clave de registro en el proxy de la copia de seguridad.
- Cuando se realiza una tarea de restauración desde el agente normal mediante la sesión de la copia de seguridad del servidor de puntos de recuperación, cree una clave de registro en el agente normal.

4. En Resolución de conflictos, especifique las opciones correspondientes a la acción que deberá realizar Arcserve UDP si se encuentran conflictos durante el proceso de restauración

Sobrescribir la máquina virtual existente

Esta opción es para especificar si se sobrescribe la máquina virtual existente. De forma predeterminada, esta opción no está seleccionada.

Nota: Para la opción Sobrescribir la máquina virtual existente, se define una "máquina virtual existente" como una máquina virtual que tiene el mismo nombre de máquina virtual y que reside en el mismo host de ESXi (para la máquina virtual de VMware), o en una máquina virtual que tiene el mismo nombre de máquina virtual y el mismo UUID de instancia y que reside en el mismo host de Hyper-V (para la máquina virtual de Hyper-V). Para la máquina virtual de VMware, si hay una máquina virtual que tiene el mismo nombre de máquina virtual pero que reside en un host de ESXi diferente (que se encuentra en el mismo vCenter), esta opción para sobrescribir no funcionará. En este caso, la interfaz gráfica de usuario de recuperación de la máquina virtual detecta dicha máquina virtual, muestra un mensaje de error y no permite que se pueda continuar para evitar que una máquina virtual no se sobrescriba por error. Como solución temporal, se debe cambiar el nombre de la máquina virtual existente o utilizar la opción Restaurar en una ubicación alternativa y, a continuación, especificar un nombre diferente de la máquina virtual.

- Si selecciona esta opción, el proceso de restauración sobrescribirá (reemplazará) cualquier imagen existente de esta máquina virtual que se encuentra en el destino de restauración especificado. La imagen de la máquina virtual se restaurará a partir de los archivos de copia de seguridad sin tener en cuenta la presencia actual en el destino de la restauración.
- Si no se selecciona esta opción, la interfaz gráfica de usuario de recuperación de la máquina virtual muestra un mensaje de error y le impedirá continuar si la máquina virtual original todavía existe en la ubicación original. Como solución temporal, se debe cambiar el nombre de la máquina virtual existente o utilizar la opción Restaurar en una ubicación alternativa y, a continuación, especificar un nombre diferente de la máquina virtual.

Generar un UUID de la nueva instancia de la máquina virtual

Esta opción es para especificar si se desea generar un UUID de la nueva instancia para la máquina virtual restaurada o mantener el UUID de la instancia original.

Nota: Si no se selecciona esta opción, se establecerá el UUID de la instancia original en la máquina virtual restaurada. Sin embargo, en caso de que el destino de vCenter/ESX o que el host de Hyper-V ya tenga una máquina virtual con el mismo UUID de la instancia, se utilizará el UUID nuevo en su lugar y se mostrará un mensaje de advertencia en el registro de actividad de la tarea de recuperación de la máquina virtual.

5. Especifique la opción Recuperación posterior.

Encender la máquina virtual

Seleccione si se aplicará el encendido a la máquina virtual al final del proceso de restauración. De forma predeterminada, esta opción no está activada.

Marcar como plantilla de máquina virtual (disponible solamente para la máquina virtual de VMware)

Seleccione si se desea convertir la máquina virtual restaurada en la plantilla. Si el nodo de origen es una máquina virtual cuando se realiza la copia de seguridad, esta opción no estará seleccionada de forma predeterminada. Si el nodo de origen es una plantilla cuando se realiza la copia de seguridad, esta opción estará seleccionada de forma predeterminada.

Las opciones de restauración se han definido para restaurar una máquina virtual.

Definición de las opciones de restauración de la ubicación original

Durante el proceso de configuración de Recuperar máquina virtual, es necesario seleccionar la opción de dónde se desea restaurar la máquina virtual. Las selecciones disponibles son **Restauración en la ubicación original** y **Restauración en una ubicación alternativa**.

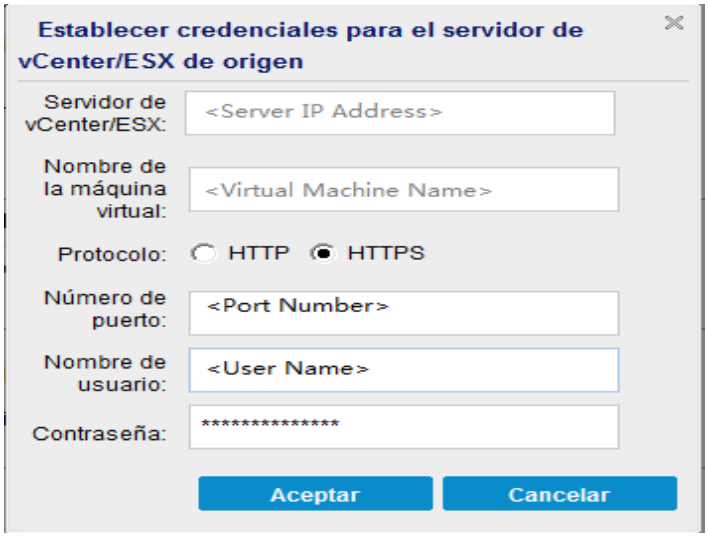
Este procedimiento explica cómo restaurar una máquina virtual en una ubicación original.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, después de especificar las opciones **Resolución de conflictos** y **Acción tras la recuperación**, seleccione **Restaurar en la ubicación original** y haga clic en **Siguiente**.

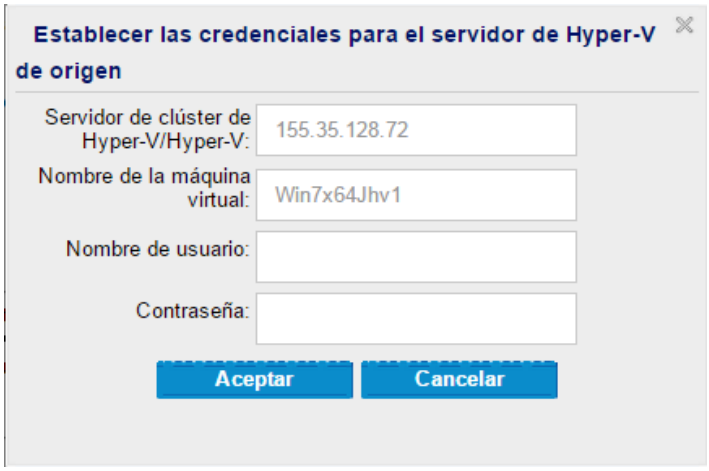
   Se muestra el cuadro de diálogo adecuado para VMware o Hyper-V.

   - Aparece el cuadro de diálogo **Establecer credenciales para el servidor vCenter/ESX de origen**.



   - Para Hyper-V, se muestra el cuadro de diálogo **Establecer las credenciales**

para el servidor Hyper-V de origen.



2. Especifique las credenciales para acceder a la máquina virtual.
   - Para VMware, rellene los campos siguientes.

     Servidor vCenter/ESX

     Muestra el nombre de host o la dirección IP para el sistema del servidor de vCenter o de ESX.

     Nota: Este campo no se puede editar. Únicamente puede consultar los detalles.

     Nombre de máquina virtual

     Muestra el nombre de la máquina virtual que se está restaurando.

     Nota: Este campo no se puede editar. Únicamente puede consultar los detalles.

     Protocolo

     Especifica el protocolo que se desea utilizar para la comunicación con el servidor de destino. Las selecciones disponibles son HTTP y HTTPS.

     Número de puerto

     Especifica el puerto que se desea utilizar para la transferencia de datos entre el servidor de origen y el destino.

     Predeterminado: 443.

     Nombre de usuario

     Especifica el nombre de usuario que tiene derechos de acceso para iniciar sesión en el servidor ESX/vCenter en el que desee restaurar la máquina virtual.

     Contraseña

Especifica la contraseña correspondiente para el nombre de usuario.

- Para Hyper-V, rellene los campos siguientes.

  Servidor de clúster de Hyper-V/Hyper-V

  Muestra el nombre de host o la dirección IP para el sistema del servidor de clúster de Hyper-V o el servidor de Hyper-V.

  Nota: Este campo no se puede editar. Únicamente puede consultar los detalles.

  Nombre de máquina virtual

  Muestra el nombre de la máquina virtual que se está restaurando.

  Nota: Este campo no se puede editar. Únicamente puede consultar los detalles.

  Nombre de usuario

  Especifica el nombre de usuario que tiene derechos de acceso para iniciar sesión en el servidor Hyper-V en el que desee restaurar la máquina virtual. Para la máquina virtual del clúster de Hyper-V se debe especificar la cuenta de dominio que dispone de privilegios administrativos del clúster.

  Contraseña

  Especifica la contraseña correspondiente para el nombre de usuario.

3. Haga clic en **Aceptar**.

   Se abrirá el cuadro de diálogo **Resumen de la restauración**.

   Se han definido las opciones de restauración para la ubicación original.

Definición de las opciones de restauración de la ubicación alternativa

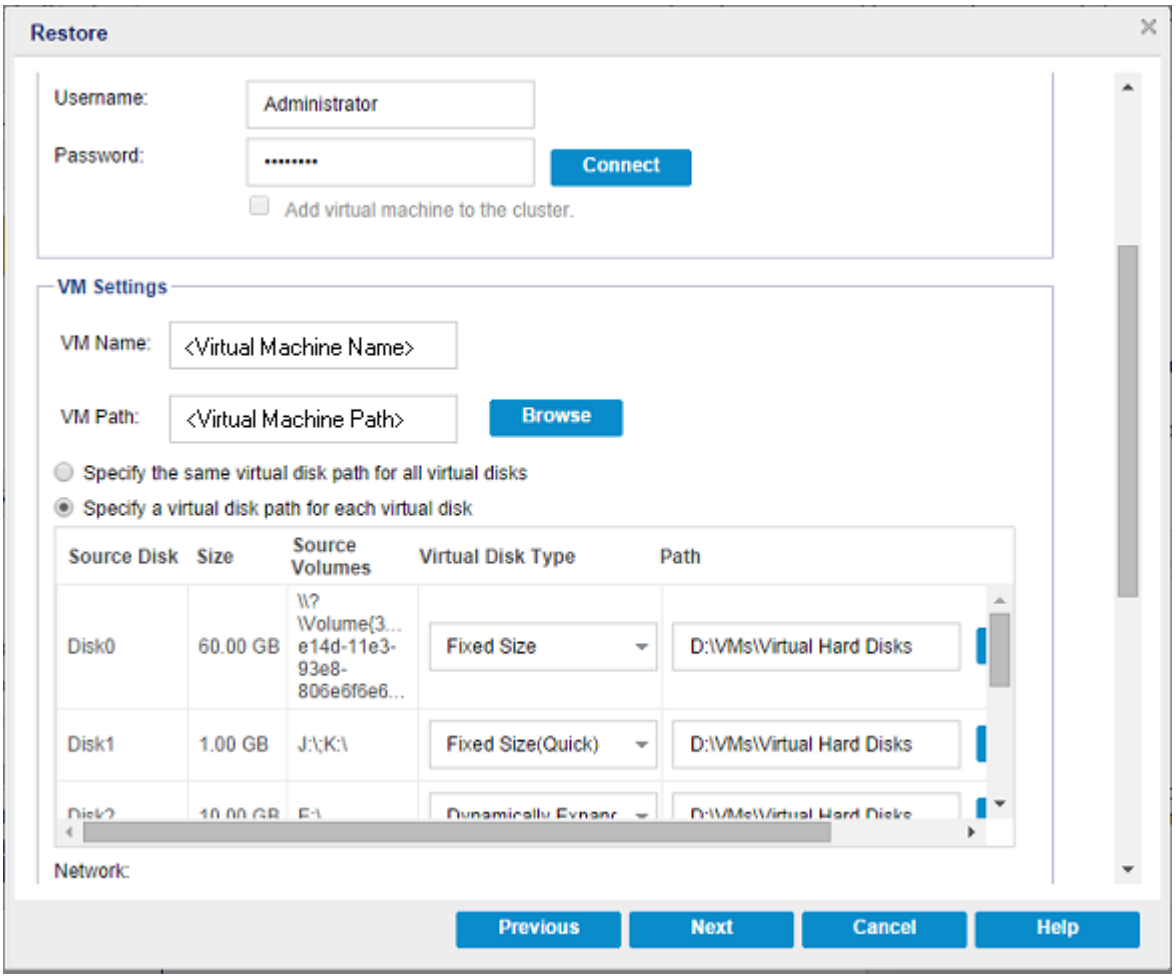
Durante el proceso de configuración de Restaurar máquina virtual, se debe especificar dónde se desea almacenar la máquina virtual recuperada. Las selecciones disponibles son **Restauración en la ubicación original** y **Restauración en una ubicación alternativa**.

Este procedimiento explica cómo restaurar una máquina virtual en una ubicación alternativa o en un almacén de datos distinto.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, después de especificar las opciones **Resolución de conflictos** y **Acción tras la recuperación**, seleccione **Restaurar en una ubicación alternativa**.
   - Para VMware, el cuadro de diálogo **Opciones de restauración** se amplía para mostrar una restauración adicional a las opciones alternativas.
   - Para Hyper-V, el cuadro de diálogo **Opciones de restauración** se amplía para mostrar una restauración adicional a las opciones alternativas.

   Si se selecciona la opción **Especifique la ruta de disco virtual para cada disco virtual,** aparecerá el cuadro de diálogo siguiente:



2. Especifique la información del servidor adecuada.

   - Para VMware, introduzca los campos siguientes:

     Servidor vCenter/ESX

     Especifica el nombre de host o dirección IP para el sistema del servidor ESX o vCenter de destino.

     Nombre de usuario

     Especifica el nombre de usuario que tiene derechos de acceso para iniciar sesión en el servidor ESX/vCenter en el que desee restaurar la máquina virtual.

     Contraseña

     Especifica la contraseña correspondiente para el nombre de usuario.

     Protocolo

     Especifica el protocolo que se desea utilizar para la comunicación con el servidor de destino. Las selecciones disponibles son HTTP y HTTPS.

     Valor predeterminado: HTTPS.

Nota: VMware Virtual Disk Development Kit (VDDK) 6.x.x está integrado en Arcserve UDP 6.5 pero VDDK 6.x.x no es compatible con HTTP. Asegúrese de seleccionar HTTPS, a menos que desee sustituir manualmente la versión integrada VDDK 6.x.x por otra versión de VDDK.

Número de puerto

Especifica el puerto que se desea utilizar para la transferencia de datos entre el servidor de origen y el destino.

Valor predeterminado: 443

- Para Hyper-V, introduzca los campos siguientes:

servidor Hyper-V

Muestra el nombre de host o la dirección IP para el sistema del servidor Hyper-V.

Nombre de usuario

Especifica el nombre de usuario que tiene derechos de acceso para iniciar sesión en el servidor Hyper-V en el que desee restaurar la máquina virtual. Para la máquina virtual del clúster de Hyper-V se debe especificar la cuenta de dominio que dispone de privilegios administrativos del clúster.

Contraseña

Especifica la contraseña correspondiente para el nombre de usuario.

Adición de una máquina virtual al clúster

Seleccione esta opción si desea agregar al clúster la máquina virtual que ha restaurado Arcserve UDP. Tenga en cuenta una de las siguientes opciones:

- Si se ha proporcionado el nombre del nodo de clúster como el nombre del servidor Hyper-V, la casilla de verificación se desactiva y se selecciona de forma predeterminada. Como resultado, la máquina virtual se agrega automáticamente en el clúster.
- Si se proporciona el nombre de host de un servidor Hyper-V que forma parte del clúster, la casilla de verificación se activa y podrá seleccionar la opción para agregar la máquina virtual en el clúster.
- Si se proporciona el nombre de host de un servidor Hyper-V independiente, el cual no forma parte del clúster, la casilla de verificación se desactiva y, en consecuencia, no se selecciona.

3. Cuando se especifica la Información del servidor vCenter/ESX o la Información del servidor Hyper-V, haga clic en el botón **Conectar a este servidor vCenter/ESX** o haga clic en el botón **Conectar a este servidor Hyper-V.**

   Si la información de credenciales de acceso del servidor alternativo es correcta, los campos **Configuración de la máquina virtual** se activan.

4. Especifique la **Configuración de la máquina virtual**.

   - Para VMware, introduzca los campos siguientes.

     Nombre de VM

     Especifica el nombre de la máquina virtual que se está restaurando.

     Servidor ESX

     Especifica el servidor ESX de destino. El menú desplegable contendrá un listado de todos los servidores de ESX asociados al servidor de vCenter.

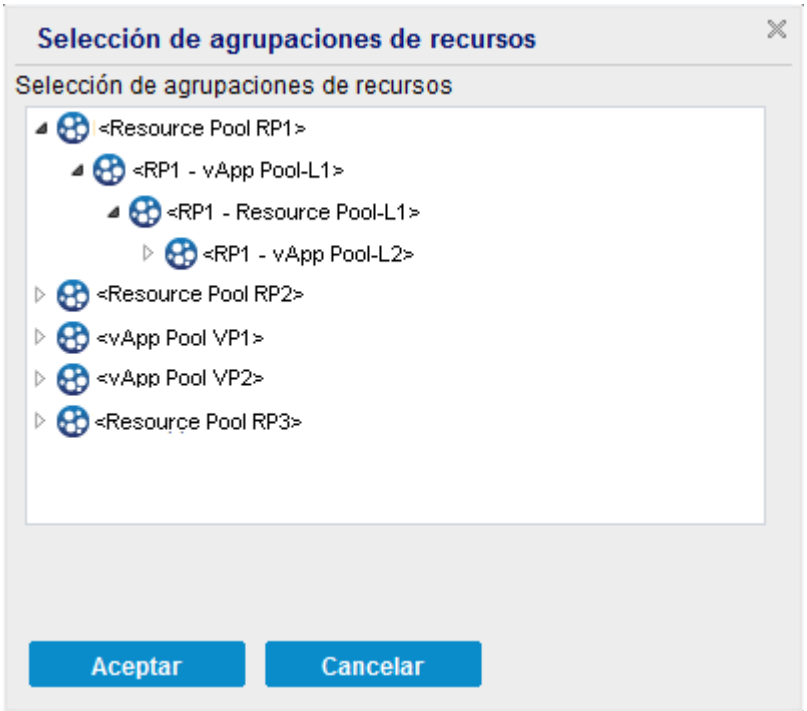
     Agrupación de recursos

     Selecciona la **Agrupación de recursos** o la **Agrupación de vApp** que se desea utilizar para la recuperación de la máquina virtual.

     Nota: una agrupación de recursos es una recopilación configurada de CPU y recursos de memoria. Una agrupación de vApp es una recopilación de una o más máquinas virtuales que se puede gestionar como un solo objeto.

     Predeterminado: vacío.

     Haga clic el botón **Explorar agrupaciones de recursos** para mostrar el cuadro de diálogo **Selección de agrupaciones de recursos.** Este cuadro de diálogo contiene un listado de todas las agrupaciones de recursos y las agrupaciones de vApp disponibles para el servidor ESX de destino. Seleccione la agrupación que se utilizará para la recuperación de la máquina virtual. Puede dejar este campo en blanco cuando no se desea asignar una agrupación de recursos o una agrupación de vApp a esta recuperación de la máquina virtual.



Política de almacenamiento

Especifique la política de almacenamiento de la máquina virtual que se aplica a la máquina virtual principal de la máquina virtual restaurada. Si no desea aplicar la política de almacenamiento de la máquina virtual, seleccione Almacén de datos predeterminado.

Nota: Si solo puede ver un almacén de datos predeterminado, pero en realidad hay otras políticas de almacenamiento definidas en vCenter, la cuenta utilizada para conectarse a vCenter no tiene permisos suficientes para obtener la política de almacenamiento desde vCenter. Compruebe si la cuenta tiene la vista del almacenamiento controlado por el perfil del privilegio en el nivel de vCenter.

Almacén de datos de máquina virtual

Especifique el almacén de datos de destino para la máquina virtual principal de la máquina virtual restaurada.

Nota: De forma predeterminada, se muestran solo los almacenes de datos que son compatibles con la política de almacenamiento seleccionada. Si desea ver todos los almacenes de datos, desactive la selección de la casilla de verificación **Mostrar solo los almacenes de datos admitidos para la política de almacenamiento seleccionada** que se encuentra en la tabla Almacén de datos del disco.

Almacén de datos del disco

Especifique Tipo de disco virtual, Política de almacenamiento y Almacén de datos de destino para cada disco virtual de la máquina virtual, respectivamente.

- Tipo de disco virtual: Seleccione una de las siguientes opciones: Fino, Pesado - diferido - ajustado a cero o Pesado - diligente - ajustado a cero.
- Política de almacenamiento: Seleccione la política de almacenamiento de la máquina virtual que se aplica a este disco virtual. Si no desea aplicar la política de almacenamiento de la máquina virtual, seleccione Almacén de datos predeterminado.
- Almacén de datos de destino: Seleccione el almacén de datos donde se ha restaurado el disco virtual.

Nota: De forma predeterminada, se muestran solo los almacenes de datos que son compatibles con la política de almacenamiento seleccionada. Si desea ver todos los almacenes de datos, desactive la selección de la casilla de verificación **Mostrar solo los almacenes de datos admitidos para la política de almacenamiento seleccionada** que se encuentra en la tabla Almacén de datos del disco.

Red

Especifica los detalles de configuración del Conmutador estándar de vSphere/Conmutador distribuido de vSphere.

- Para Hyper-V, introduzca los campos siguientes.

Nombre de VM

Especifica el nombre de la máquina virtual que se está restaurando.

Ruta de VM

Especifica la ruta de destino (en el servidor Hyper-V) donde guardar el archivo de configuración de la máquina virtual de Hyper-V. La carpeta predeterminada del archivo de configuración de la máquina virtual para el servidor Hyper-V se muestra de forma predeterminada. Se puede modificar la ruta directamente en el campo o hacer clic en **Examinar** para seleccionar una.

Nota: Si se restaura la máquina virtual en un clúster de Hyper-V y desea que la máquina virtual migre entre los nodos de clúster, se debe especificar el volumen compartido de clúster (CSV) tanto para la ruta a la máquina virtual como para la ruta al disco virtual.

Especifique la misma ruta de disco virtual para todos los discos virtuales

Especifica una ruta (en el servidor Hyper-V) donde guardar todos los discos virtuales de la máquina virtual juntos. La carpeta predeterminada del archivo de disco de la máquina virtual para el servidor Hyper-V se muestra de forma predeterminada. Se puede modificar la ruta directamente en el campo o hacer clic en **Examinar** para seleccionar una.

Nota: Si se restaura la máquina virtual en un clúster de Hyper-V y desea que la máquina virtual migre entre los nodos de clúster, se debe especificar el volumen compartido de clúster (CSV) tanto para la ruta a la máquina virtual como para la ruta al disco virtual.

Especifique la ruta de disco virtual para cada disco virtual

Especifique la ruta (en el servidor Hyper-V) para cada uno de los discos virtuales de la máquina virtual respectivamente. La carpeta predeterminada del archivo de disco de la máquina virtual para el servidor Hyper-V se muestra de forma predeterminada. Se puede modificar la ruta directamente en el campo o hacer clic en **Examinar** para seleccionar una. Para asignar el tipo de disco virtual, seleccione una de las opciones siguientes: Tamaño fijo Tamaño fijo (rápido), Expansión dinámica y Mantener el mismo que el disco de origen.

Notas:

- Si se restaura la máquina virtual en un clúster de Hyper-V y desea que la máquina virtual migre entre los nodos del clúster, se debe especificar el volumen compartido de clúster (CSV) tanto para la ruta a la máquina virtual como para la ruta al disco virtual.
- No utilice la opción Tamaño fijo (rápido) a menos que esté seguro de que no se ha guardado información importante en el dispositivo de almacenamiento donde reside el archivo de disco virtual.

Tamaño fijo (rápido)

Mediante esta opción, se puede restaurar el disco de tamaño fijo más rápidamente. No es necesario borrar los bloques de disco sin utilizar mientras se restaura el disco. Sin embargo, como consecuencia, algunos fragmentos de datos originales se han quedado en el almacenamiento subyacente. Esta situación crea riesgos de pérdidas de información. Después de montar el disco en la máquina virtual, el usuario de la máquina virtual puede usar algunas herramientas de disco para analizar los datos sin formato en el disco y obtener los datos originales en el dispositivo de almacenamiento del servidor Hyper-V donde reside el archivo de disco virtual.

Red

Especifica los detalles de la configuración de red para la máquina virtual.

5. Haga clic en **Aceptar**.

   Se abrirá el cuadro de diálogo **Resumen de la restauración**.

   Se han definido las opciones de restauración para la ubicación alternativa.

Restauración de la máquina virtual

El **Resumen de la restauración** le ayuda a revisar todas las opciones de la restauración definidas y a modificarlas si es necesario.

En el cuadro de diálogo **Resumen de la restauración**, revise la información que aparece en pantalla para verificar que todas las opciones de restauración y los valores de configuración sean correctos.

- Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para cambiar el valor de configuración incorrecto.
- Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar el proceso de restauración.

Se restaura la máquina virtual.

Verificación de que la máquina virtual se ha restaurado

Después de la terminación del proceso de restauración, verifique que la máquina virtual se ha restaurado en el destino especificado.

Siga estos pasos:

1. Vaya al destino de la restauración que se ha especificado.

   Por ejemplo, si selecciona que se restaure la máquina virtual al destino de la restauración como ubicación original, inicie sesión en el servidor vCenter/ESX o Hyper-V original y compruebe si la máquina virtual existe.

   Si selecciona que se restaure la máquina virtual a la ubicación alternativa, inicie sesión en el servidor vCenter/ESX o Hyper-V alternativo proporcionado en las opciones de restauración y compruebe si la máquina virtual existe.

2. Verifique que la máquina virtual se ha restaurado.

   Se restaura la máquina virtual satisfactoriamente.

Cómo restaurar SQL Filestream

Esta sección incluye los siguientes temas:

Cómo aplicar el parche T00002266

Esta sección proporciona información sobre cómo aplicar el parche T00002266.

Antes de instalar el parche *T00002266*, asegúrese de que tiene el archivo *SqlRestore.ini* en *C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\Configuration* para realizar las restauraciones.

Para instalar el parche, haga lo siguiente:

1. Descargue y extraiga el archivo **T00002266.zip**.
2. Para instalarlo, haga clic en el archivo **T00002266.exe**.

Para abrir y editar el archivo SqlRestore.ini, haga lo siguiente:

1. En el equipo de origen, vaya a la siguiente ubicación:

   C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\Configuration
2. Abra el archivo *SqlRestore.ini* en un editor de texto e incluya la siguiente información:

   RestoreInstanceName = {Nombre de instancia de SQL Server de destino}

   MDF-restore-folder = {ubicación del archivo MDF}

   LDF-restore-folder = {ubicación del archivo LDF}

   NDF-restore-folder = {ubicación del archivo NDF}

   FILESTREAM-restore-folder = {ubicación del archivo FileStreams}
3. En función de dónde desee restaurar las bases de datos, edite el contenido entre llaves con las ubicaciones de las carpetas.

   Por ejemplo, reemplace:

   MDF-restore-folder = {ubicación del archivo MDF}

   con

   MDF-restore-folder = C:\Rest\MDF1

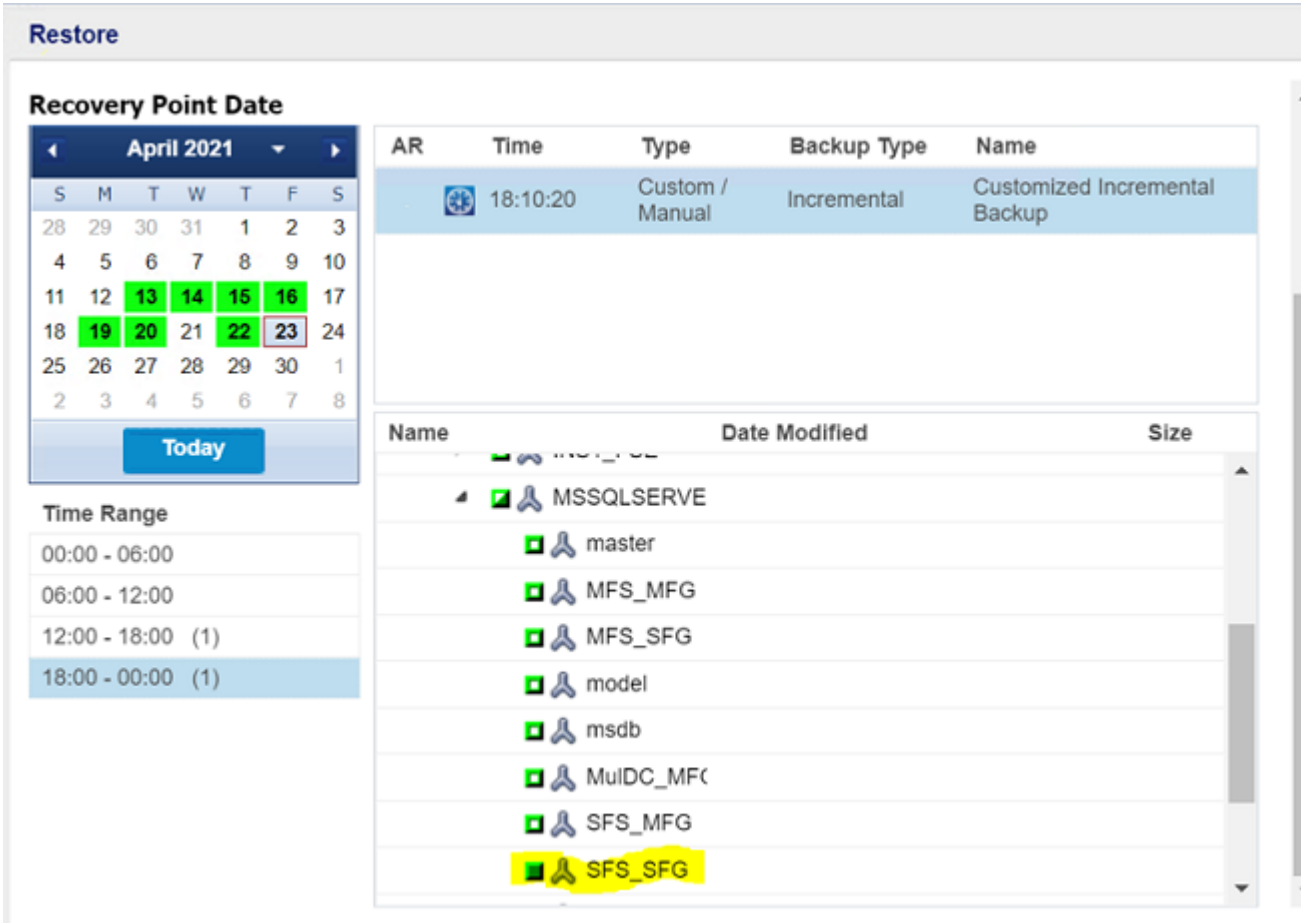
   Nota: El contenido entre llaves indica marcadores de posición para el nombre y las ubicaciones, y las llaves no son necesarias cuando se utilizan datos reales.
4. Realice la restauración de una base de datos SQL según sea necesario.

Restauración de la base de datos SQL a la ubicación original

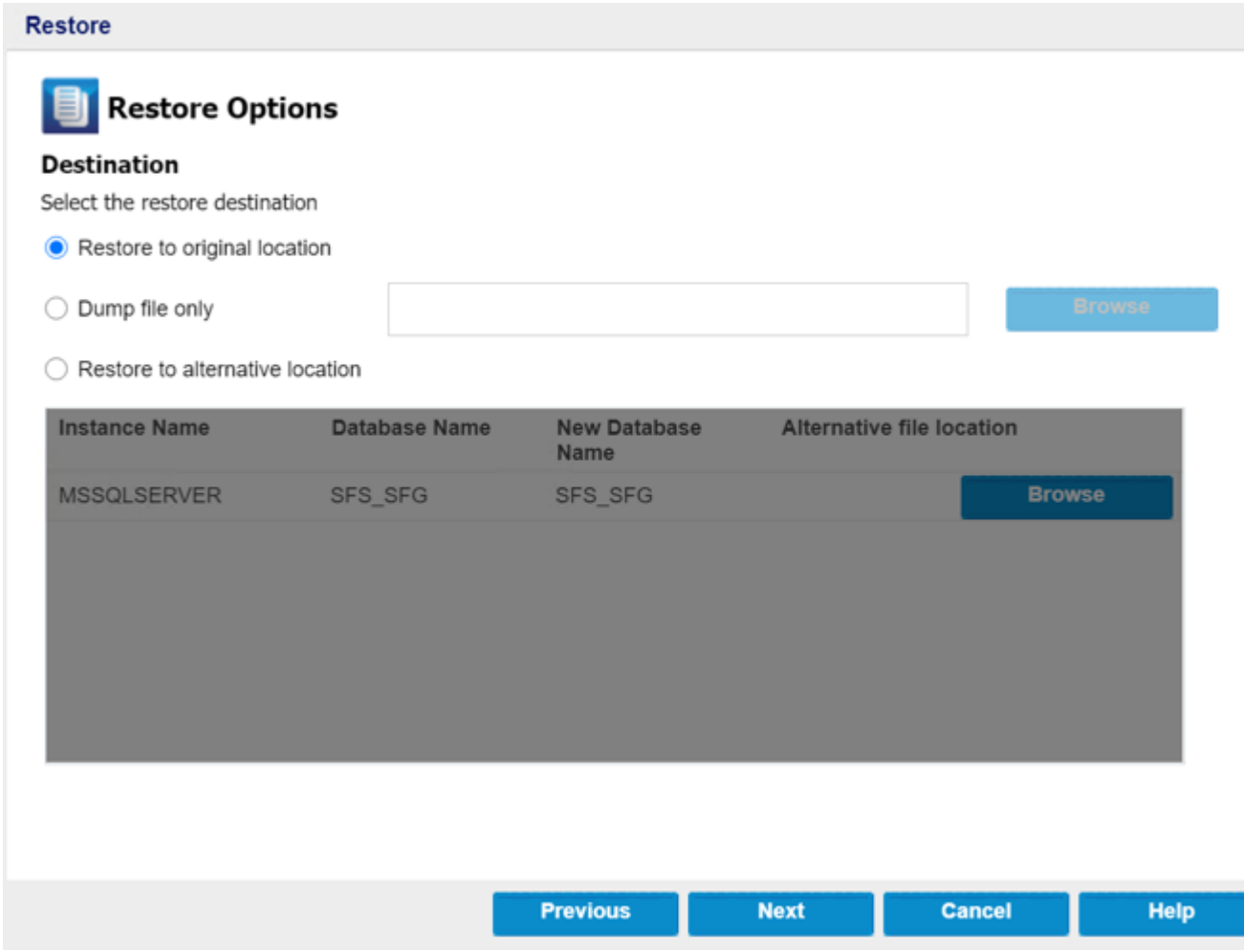
Esta sección proporciona información sobre cómo restaurar la base de datos SQL con Filestream activado a una ubicación original.

Siga estos pasos:

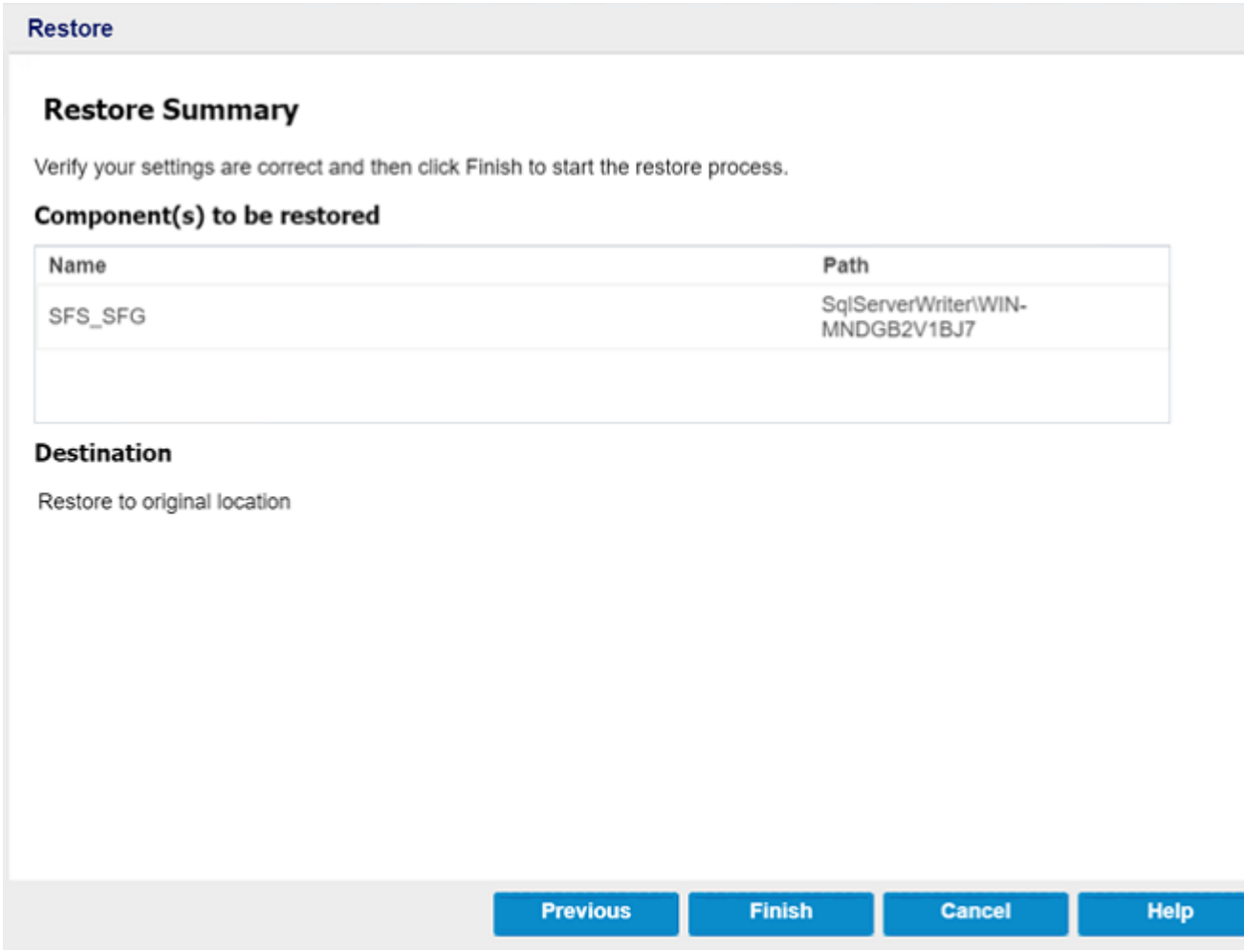
1. En la pantalla Restaurar, seleccione la Fecha del punto de recuperación, el Intervalo de tiempo y la Base de datos SQL y, a continuación, haga clic en **Siguiente**.



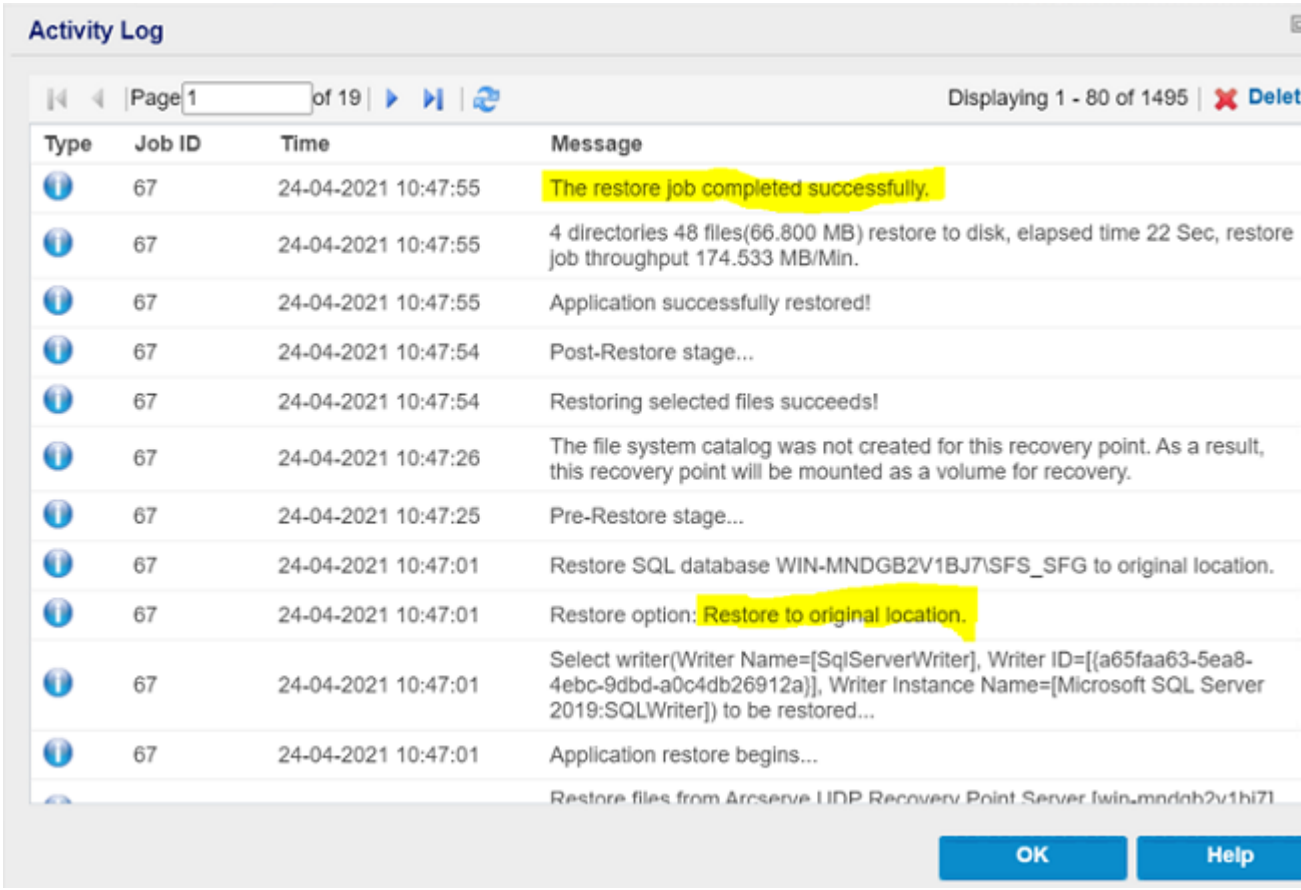
2. En la pantalla Opciones de restauración, en Destino, seleccione **Restaurar en la ubicación original** y, a continuación, haga clic en el botón **Examinar** para seleccionar la instancia.



3. Seleccione la instancia y, a continuación, haga clic en **Siguiente**.
4. Compruebe si los valores de configuración son los correctos y, a continuación, haga clic en **Finalizar** para iniciar el proceso de restauración en la ubicación original.



Consulte los registros de actividad para verificar que el estado de la restauración sea correcto.



Restauración de la base de datos SQL a una instancia alternativa en el mismo servidor

Esta sección proporciona información sobre cómo restaurar la base de datos SQL con Filestream activado a una instancia alternativa de la base de datos con Filestream activado en la que ambas instancias están en el mismo servidor SQL.

Siga estos pasos:

1. Para cambiar el nombre de la instancia, abra el archivo **SqlRestore.ini** y, a continuación, edite **RestoreInstanceName**.

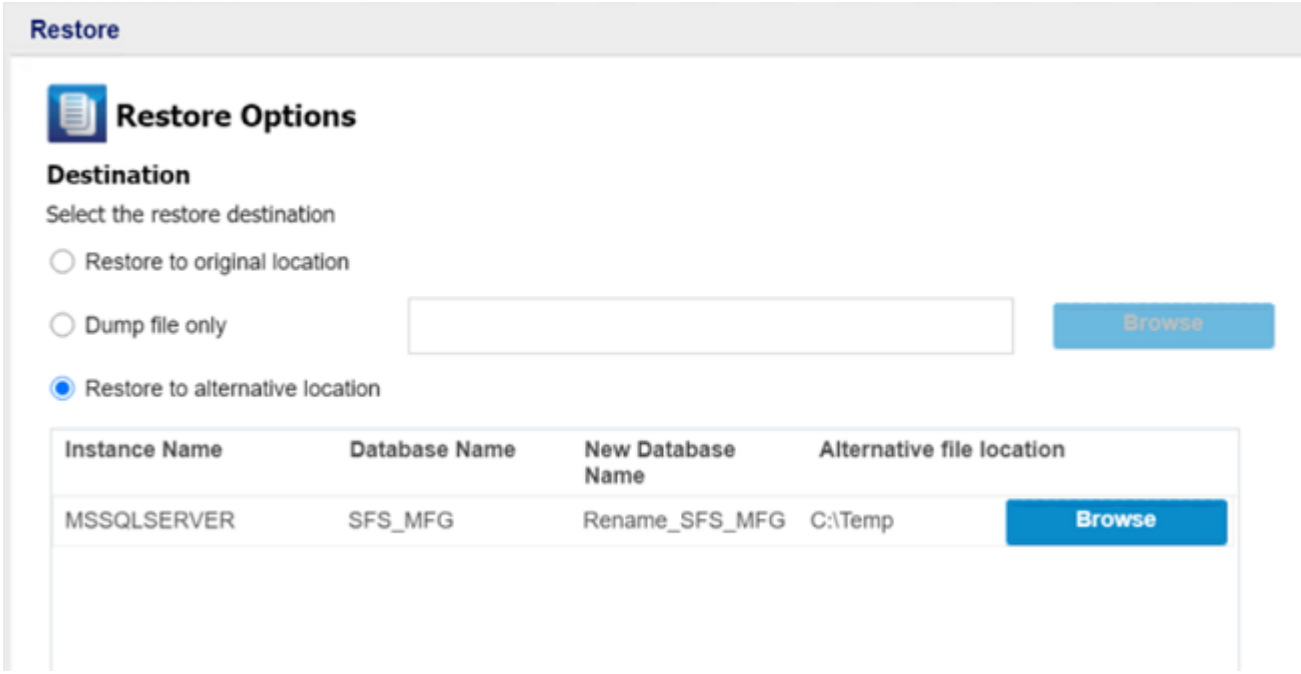
   Por ejemplo, cambie el nombre de la instancia de *WIN-MNDGB2V1BJ7\MSSQLSERVER* a *WIN-MNDGB2V1BJ7\INS1_FSE*.

   Nota: WIN-MNDGB2V1BJ7 indica el servidor SQL.



Nota: También se puede proporcionar el campo *RestoreInstanceName* sin el servidor SQL. Por ejemplo, *RestoreInstanceName = INS1_FSE*.

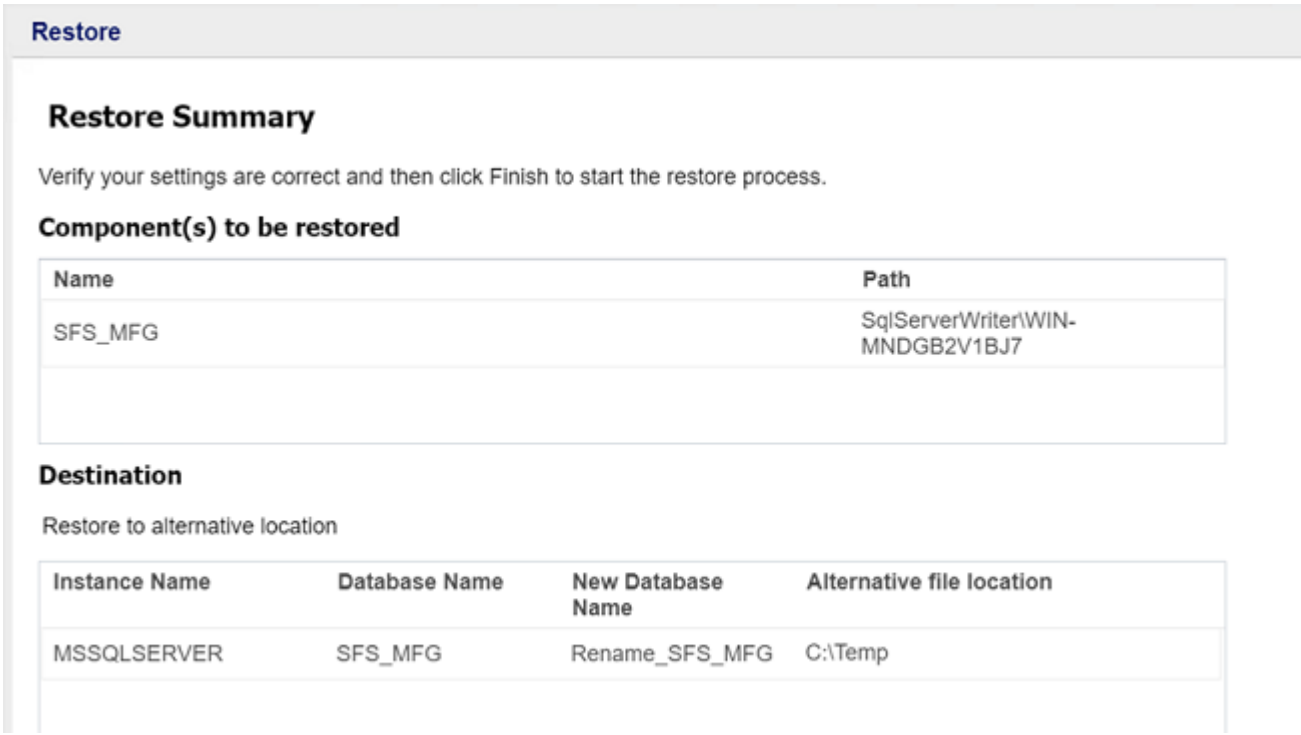
2. En el Agente, en la página Restaurar, seleccione la base de datos que desea restaurar y, a continuación, haga clic en **Siguiente**.
3. En la pantalla Opciones de restauración, seleccione **Restaurar en una ubicación alternativa** y explore la instancia.



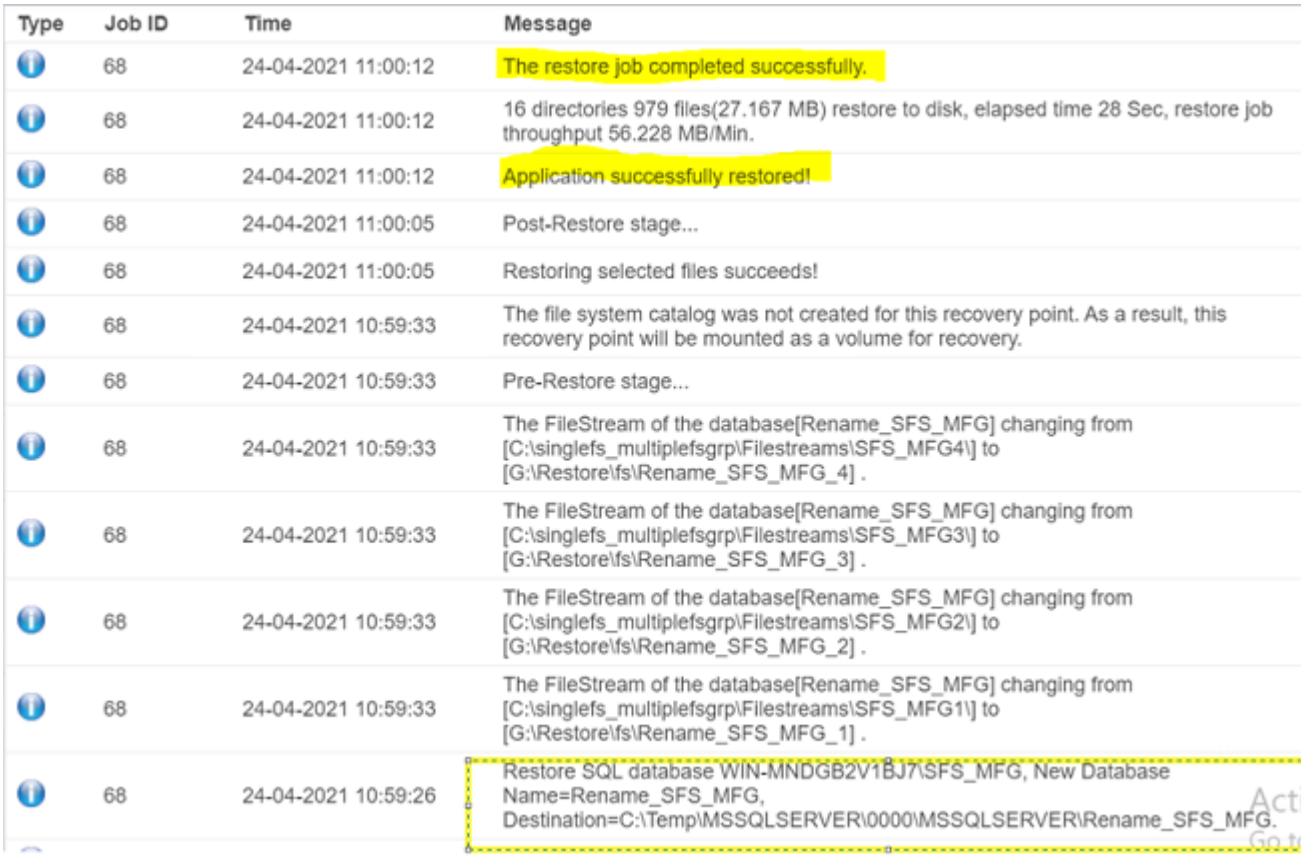
Para renombrar el nombre de la base de datos, haga clic en el área de texto **Nuevo nombre de la base de datos** y especifique el nuevo nombre. Por ejemplo, *SFS_MFG* se renombra como *Rename_SFS_MFG*.

Nota: En Ubicación alternativa del archivo, se selecciona una carpeta temporal. Esta ubicación procesa la restauración de archivos a la ubicación definida en el archivo SqlRestore.ini.

4. Compruebe si la configuración es correcta y, a continuación, haga clic en **Finalizar** para iniciar el proceso de restauración.

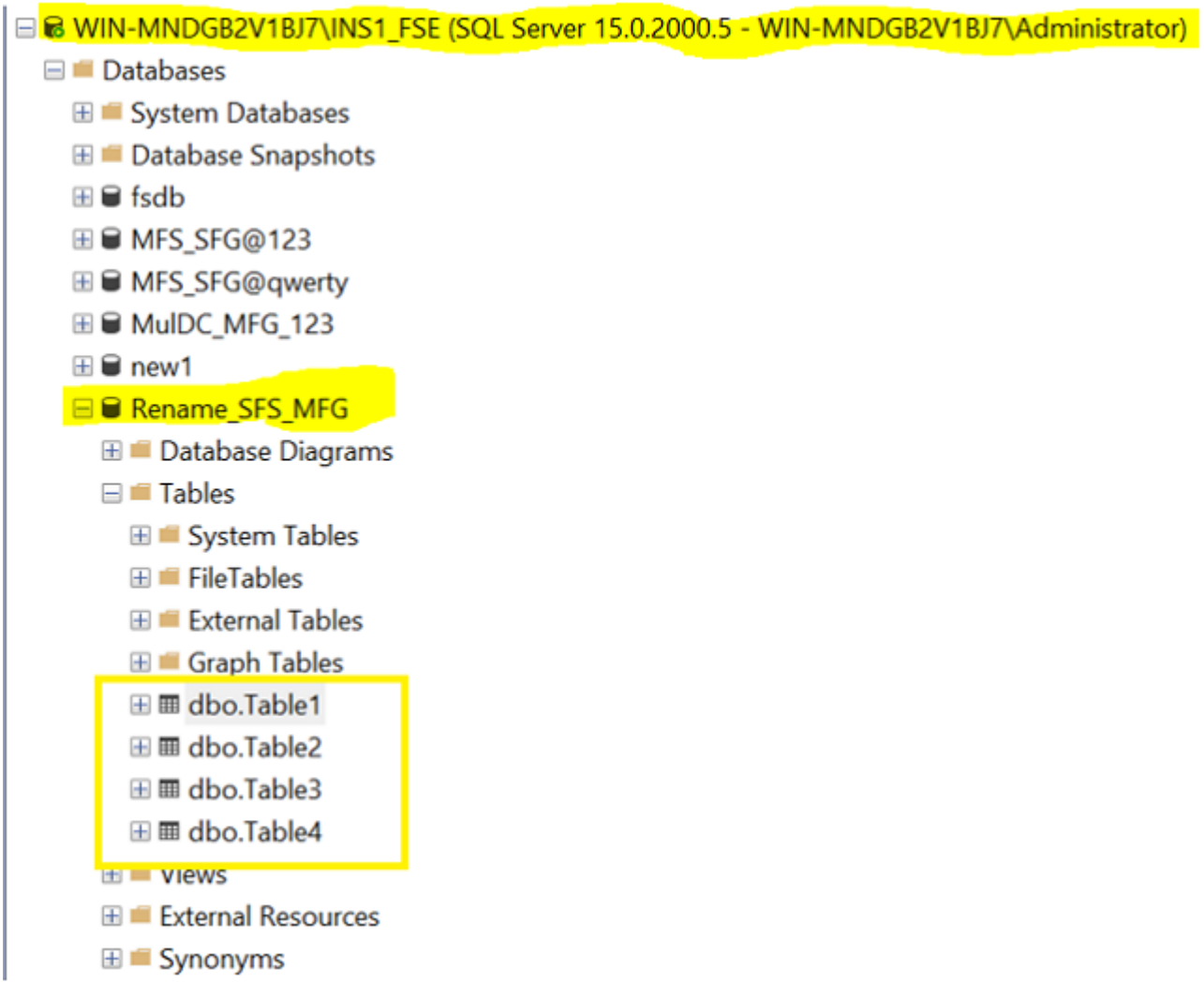


El registro de actividad muestra el estado de la restauración junto con el cambio de nombre de la base de datos.

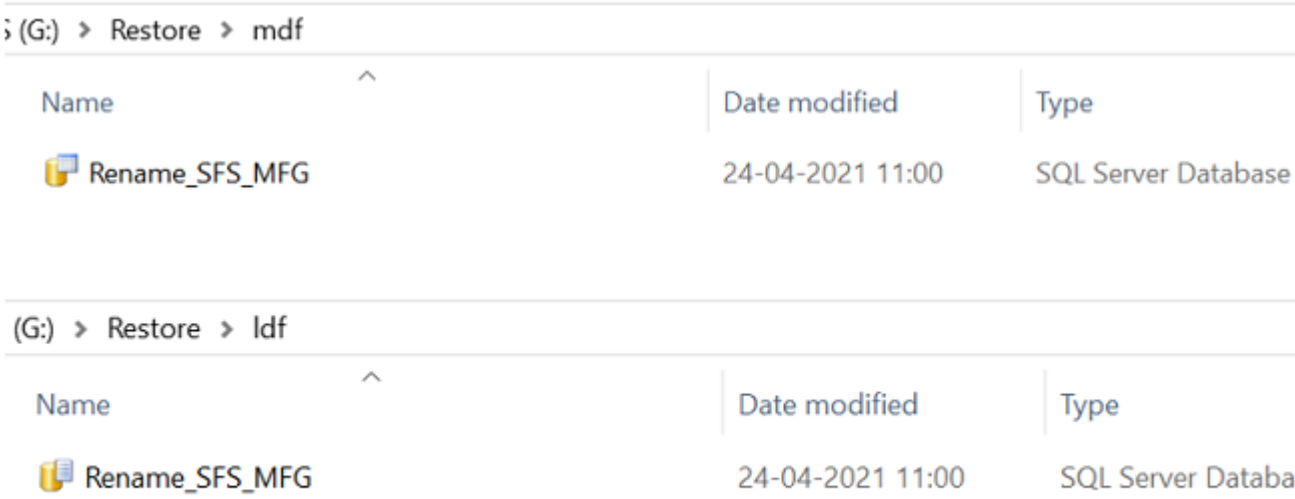


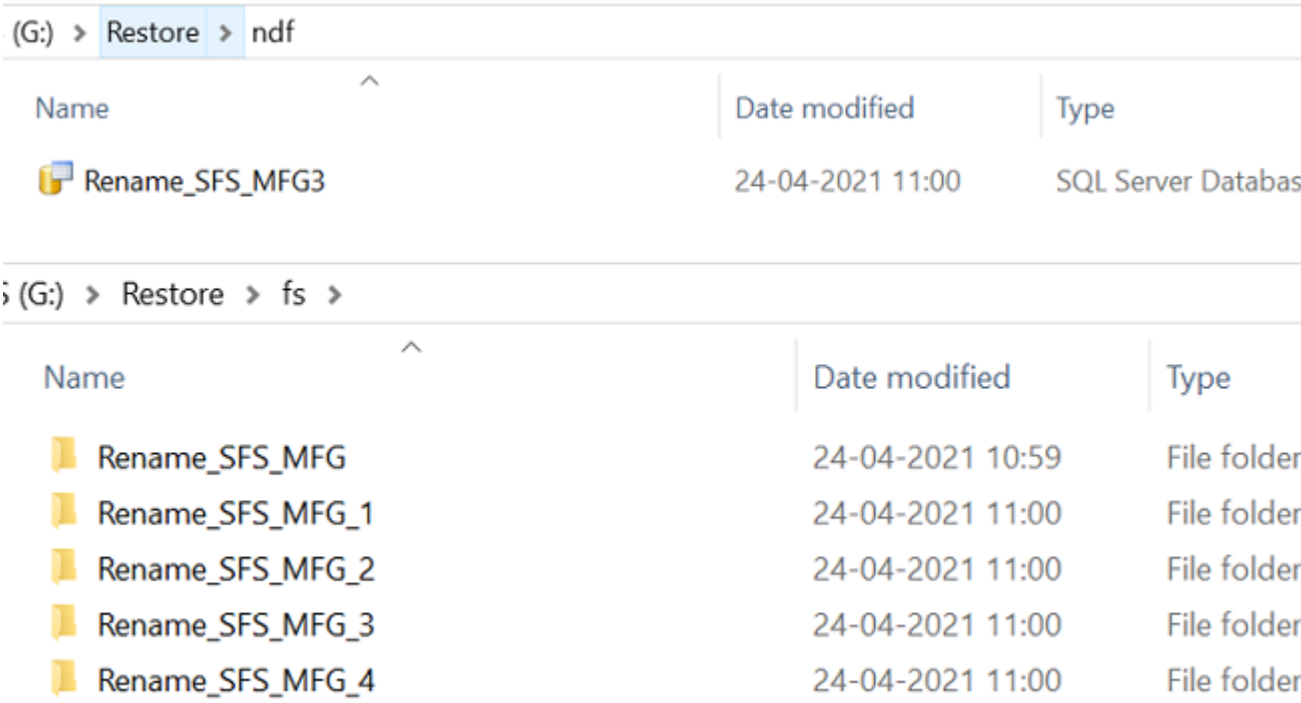
Type	Job ID	Time	Message
	68	24-04-2021 11:00:12	The restore job completed successfully.
	68	24-04-2021 11:00:12	16 directories 979 files(27.167 MB) restore to disk, elapsed time 28 Sec, restore job throughput 56.228 MB/Min.
	68	24-04-2021 11:00:12	Application successfully restored!
	68	24-04-2021 11:00:05	Post-Restore stage...
	68	24-04-2021 11:00:05	Restoring selected files succeeds!
	68	24-04-2021 10:59:33	The file system catalog was not created for this recovery point. As a result, this recovery point will be mounted as a volume for recovery.
	68	24-04-2021 10:59:33	Pre-Restore stage...
	68	24-04-2021 10:59:33	The FileStream of the database[Rename_SFS_MFG] changing from [C:\singlefs_multiplefsgrp\Filestreams\SFS_MFG4\] to [G:\Restore\fs\Rename_SFS_MFG_4] .
	68	24-04-2021 10:59:33	The FileStream of the database[Rename_SFS_MFG] changing from [C:\singlefs_multiplefsgrp\Filestreams\SFS_MFG3\] to [G:\Restore\fs\Rename_SFS_MFG_3] .
	68	24-04-2021 10:59:33	The FileStream of the database[Rename_SFS_MFG] changing from [C:\singlefs_multiplefsgrp\Filestreams\SFS_MFG2\] to [G:\Restore\fs\Rename_SFS_MFG_2] .
	68	24-04-2021 10:59:33	The FileStream of the database[Rename_SFS_MFG] changing from [C:\singlefs_multiplefsgrp\Filestreams\SFS_MFG1\] to [G:\Restore\fs\Rename_SFS_MFG_1] .
	68	24-04-2021 10:59:26	Restore SQL database WIN-MNDGB2V1BJ7\SFS_MFG, New Database Name=Rename_SFS_MFG, Destination=C:\Temp\MSSQLSERVER\0000\MSSQLSERVER\Rename_SFS_MFG.

Los cambios de nombre de la instancia y de la base de datos se reflejan en SQL Management Studio.



Tal y como se define en el archivo SqlRestore.ini, los archivos LDF, MDF y Filestream se almacenan en sus respectivas carpetas.



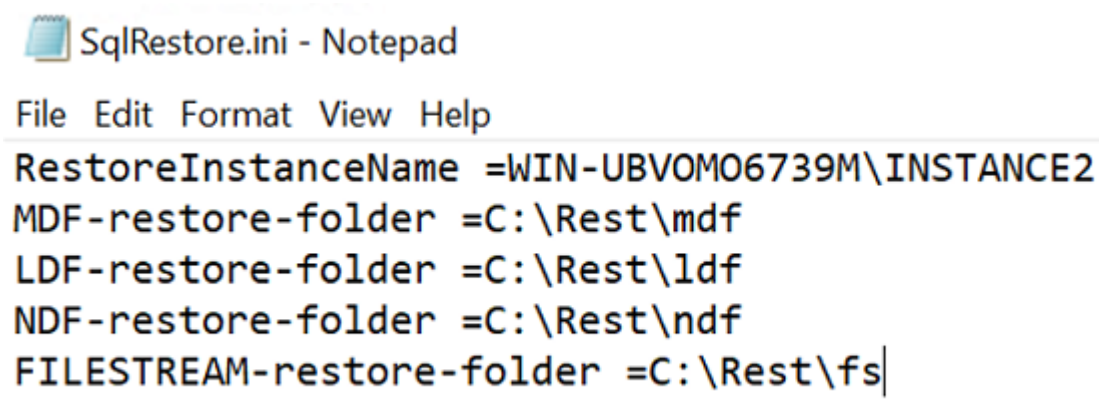


Restauración de la base de datos SQL a una instancia alternativa en un servidor diferente

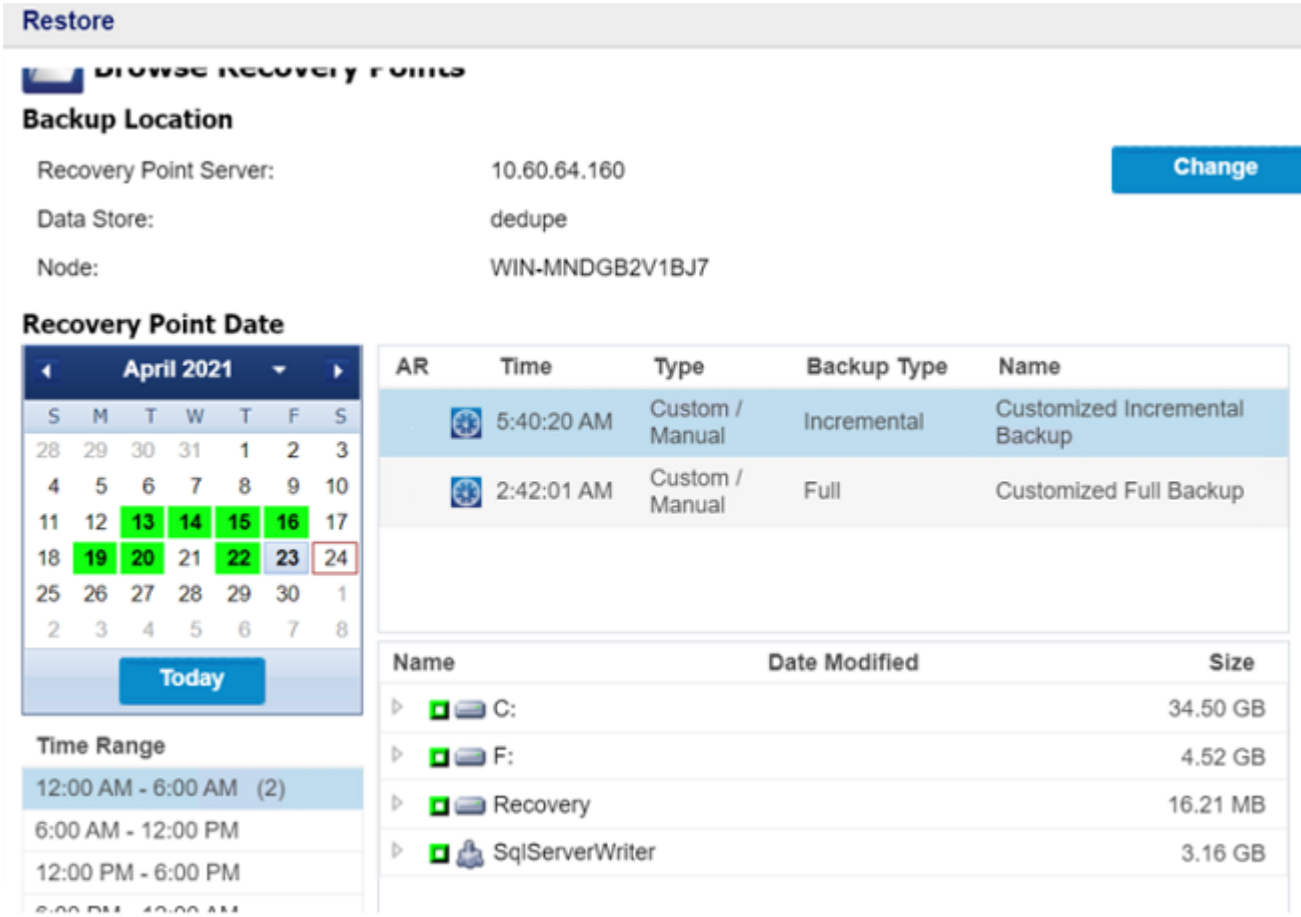
Esta sección proporciona información sobre cómo restaurar la base de datos SQL con Filestream activado a una instancia alternativa de la base de datos con Filestream activado en la que ambas instancias están en un servidor SQL diferente. Por ejemplo, si la base de datos está en el servidor de origen WIN-MNDGB2V1BJ7 y en la instancia de origen MSSQLSERVER, se puede restaurar en el servidor de destino WIN-UBVOMO6739M y en la instancia de destino INSTANCE2.

Siga estos pasos:

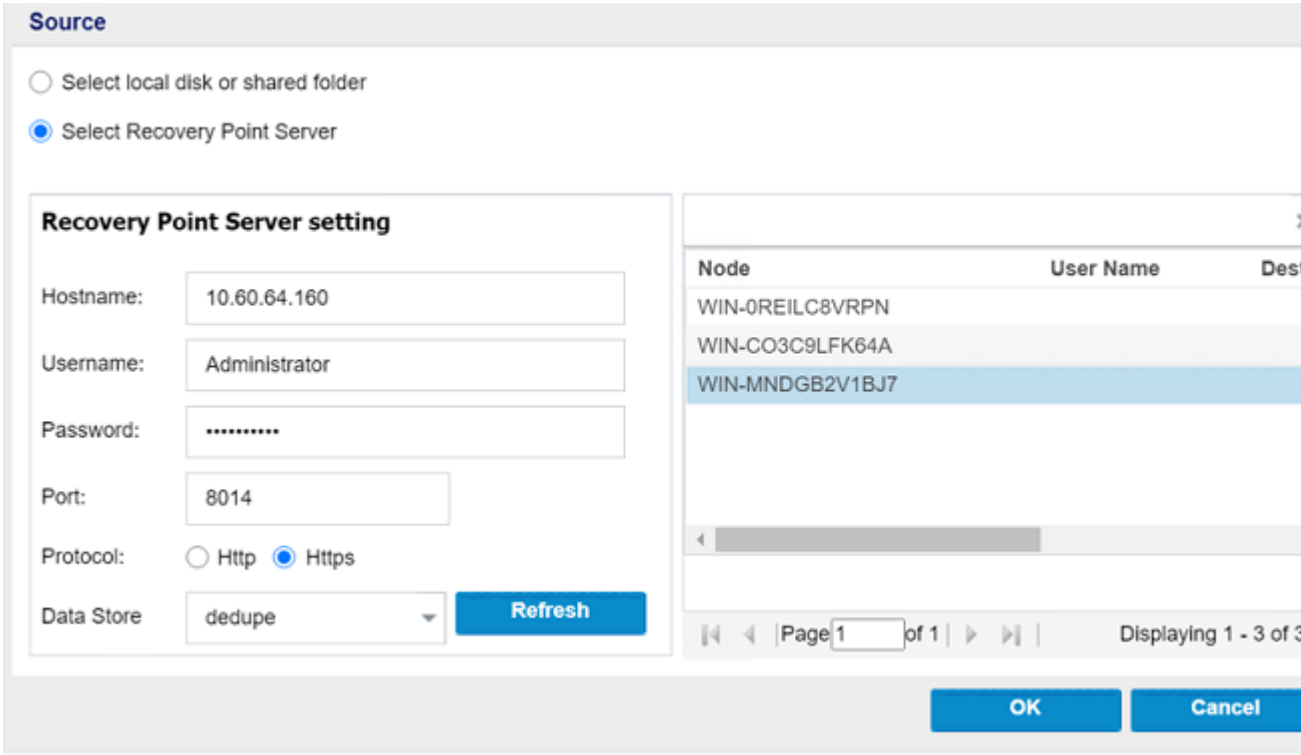
1. Para restaurar la base de datos en el servidor (WIN-UBVOMO6739M) y en la instancia (INSTANCE2) alternativos, modifique el archivo SqlRestore.ini.



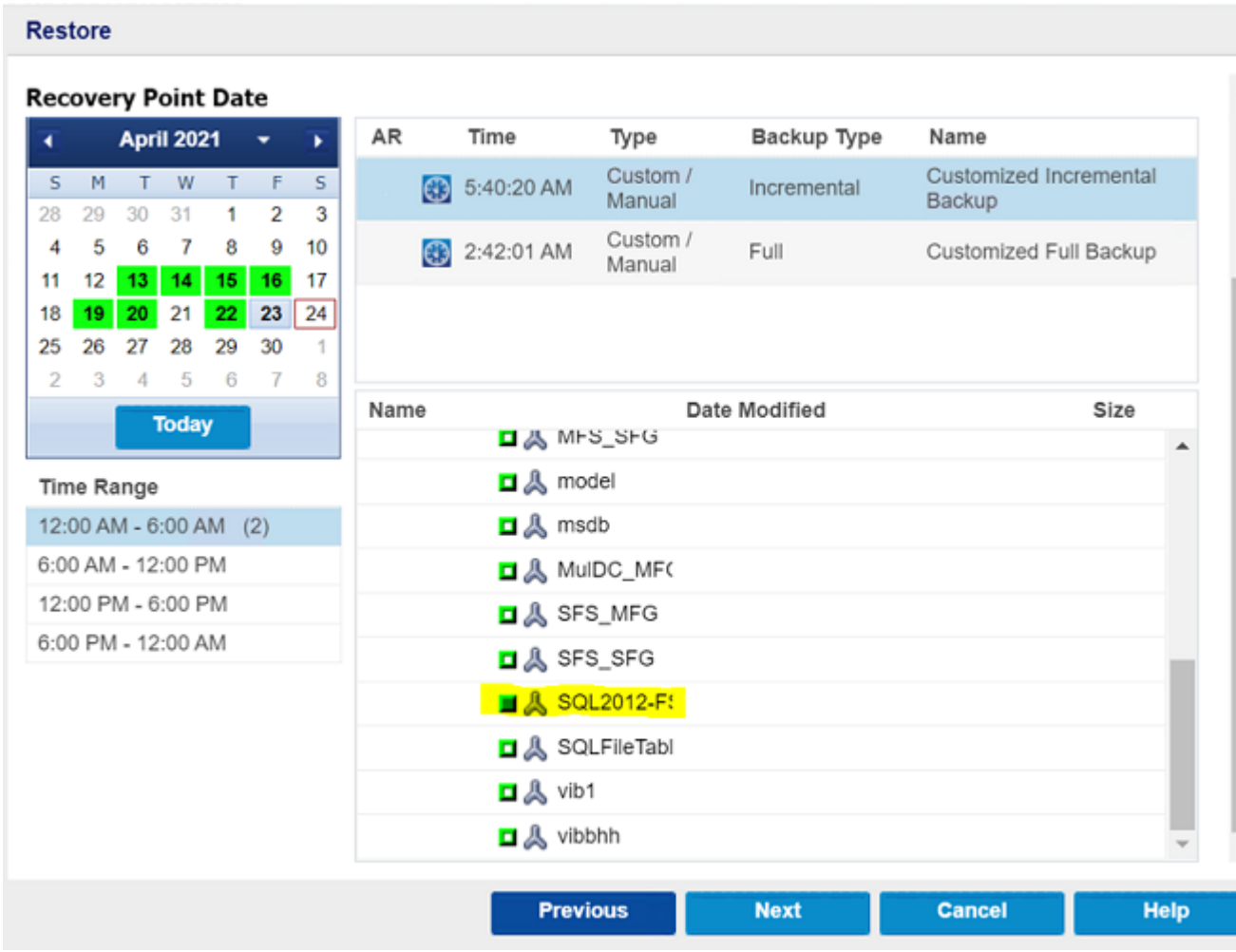
2. Para cambiar la ubicación del servidor de puntos de recuperación (RPS) para restaurar los servidores y las instancias en un servidor alternativo, haga clic en el botón **Cambiar** y, a continuación, proporcione los detalles del nuevo servidor de puntos de recuperación.



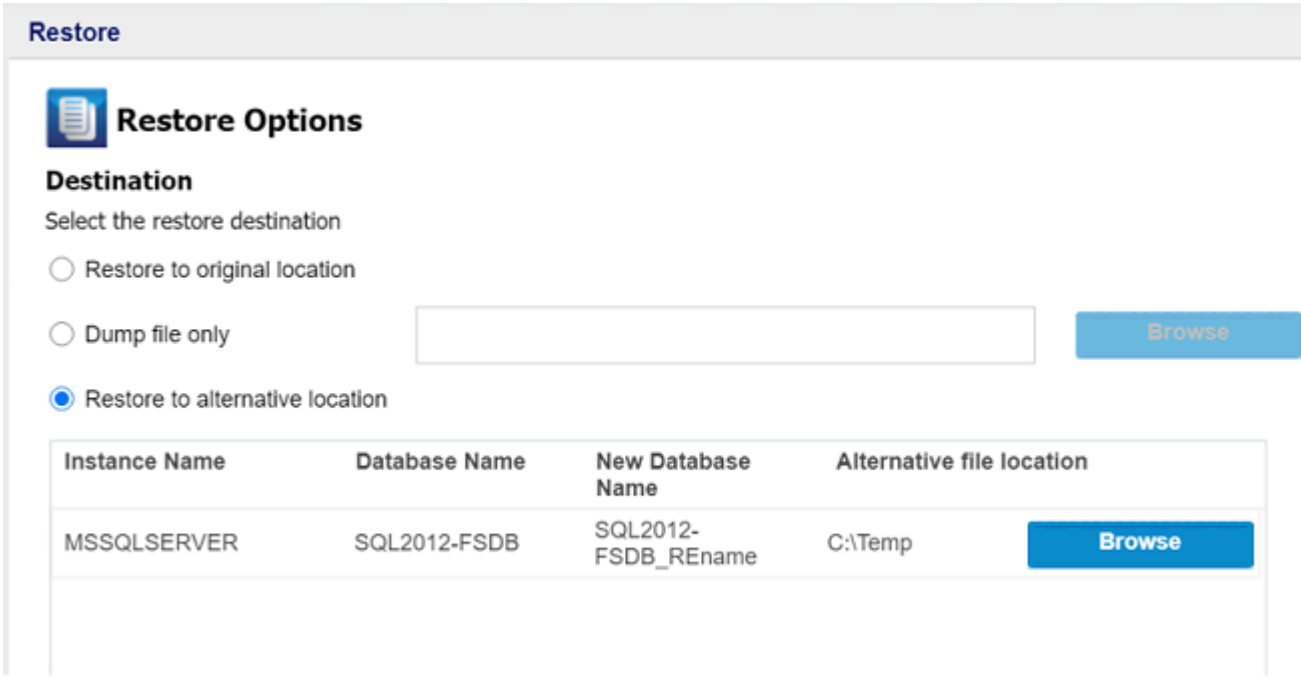
3. Para seleccionar el servidor de puntos de recuperación de origen, haga clic en **Seleccionar servidor de puntos de recuperación**, seleccione el servidor de origen (WIN-MNDGB2V1BJ7) y, a continuación, haga clic en **Aceptar**.



4. Para restaurar a un servidor alternativo, seleccione la base de datos (SQL2012-FSDB) y, a continuación, haga clic en **Siguiente**.



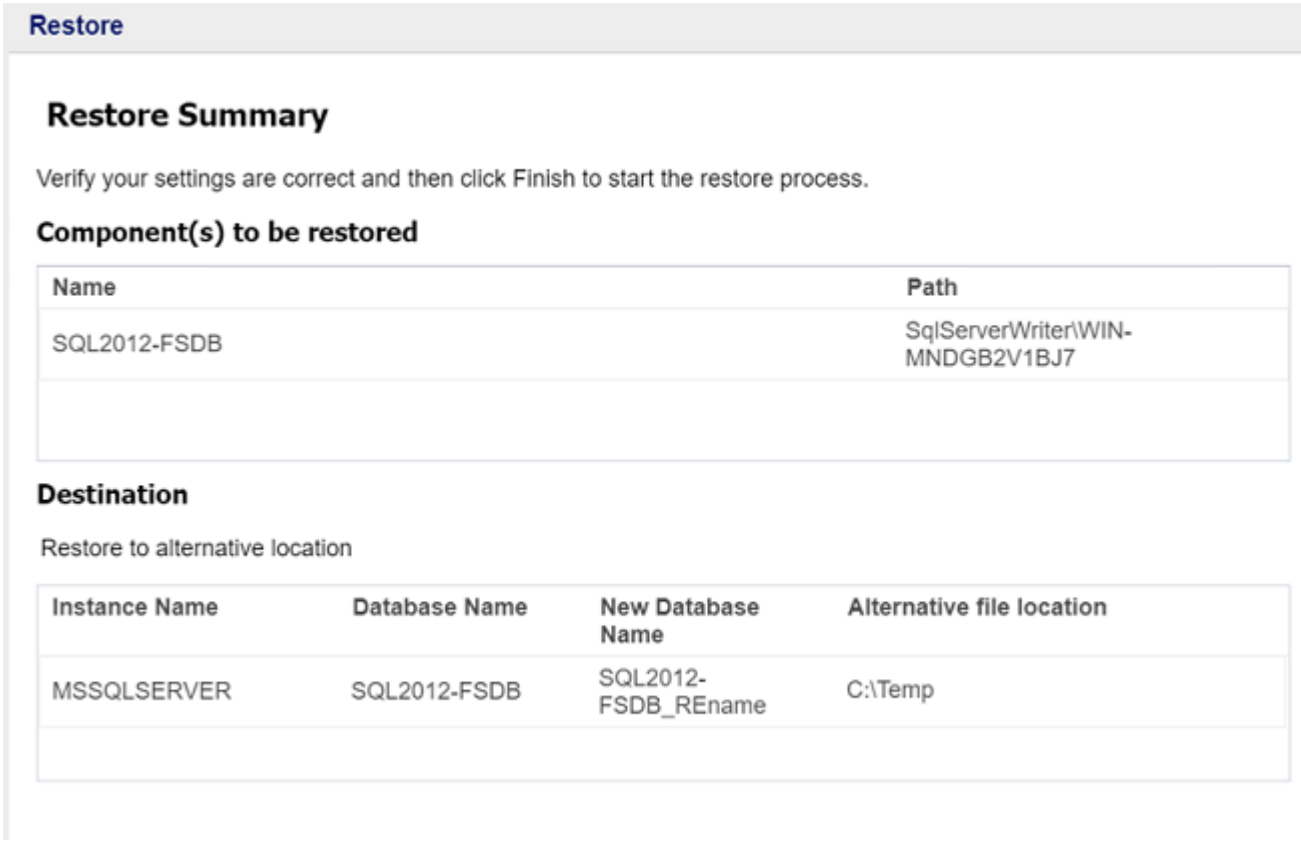
5. En la pantalla Opciones de restauración, seleccione **Restaurar en una ubicación alternativa** y explore la instancia.



Para renombrar el nombre de la base de datos, haga clic en el área de texto **Nuevo nombre de la base de datos** y especifique el nuevo nombre. Por ejemplo, SQL2012-FSDB se renombra como SQL2012-FSDB-REname.

Nota: En Ubicación alternativa del archivo, se selecciona una carpeta temporal. Esta ubicación procesa la restauración de archivos a la ubicación definida en el archivo SqlRestore.ini.

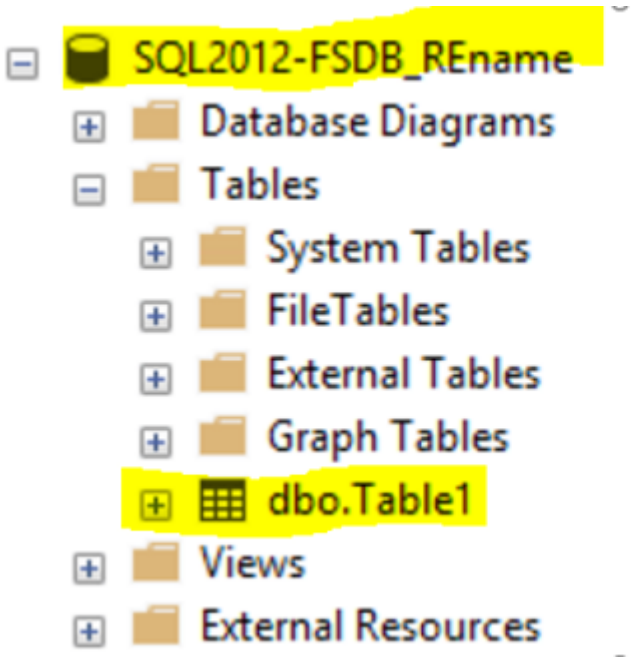
6. Compruebe si la configuración es correcta y, a continuación, haga clic en **Finalizar** para iniciar el proceso de restauración.



El registro de actividad muestra el estado de la restauración junto con el cambio de nombre de la base de datos.

Type	Job ID	Time	Message
	99	4/24/2021 1:12:48 AM	The restore job completed successfully.
	99	4/24/2021 1:12:48 AM	12 directories 38 files(10.250 MB) restore to disk, elapsed time 3 Sec, restore job throughput 154.348 MB/Min.
	99	4/24/2021 1:12:48 AM	Application successfully restored!
	99	4/24/2021 1:12:47 AM	Post-Restore stage...
	99	4/24/2021 1:12:47 AM	Restoring selected files succeeds!
	99	4/24/2021 1:12:39 AM	The file system catalog was not created for this recovery point. As a result, this reco point will be mounted as a volume for recovery.
	99	4/24/2021 1:12:38 AM	Pre-Restore stage...
	99	4/24/2021 1:12:38 AM	The FileStream of the database[SQL2012-FSDB_REname] changing from [F:\MSSQL15.MSSQLSERVER\MSSQL\DATA\fs3\] to [C:\Rest\fs\SQL2012-FSDB_REname_3] .
	99	4/24/2021 1:12:38 AM	The FileStream of the database[SQL2012-FSDB_REname] changing from [F:\MSSQL15.MSSQLSERVER\MSSQL\DATA\fs2\] to [C:\Rest\fs\SQL2012-FSDB_REname_2] .
	99	4/24/2021 1:12:38 AM	The FileStream of the database[SQL2012-FSDB_REname] changing from [F:\MSSQL15.MSSQLSERVER\MSSQL\DATA\fs1\] to [C:\Rest\fs\SQL2012-FSDB_REname_1] .
	99	4/24/2021 12:16:46 AM	Restore SQL database WIN-MNDGB2V1BJ7\SQL2012-FSDB, New Database Name=SQL2012-FSDB_REname, Destination=C:\Temp\MSSQLSERVER\0000\MSSQLSERVER\SQL2012-FSDB_REname.
	99	4/24/2021 12:16:46 AM	Restore option: Restore to alternate location.

El cambio en el nombre de la base de datos se refleja en SQL Management Studio.



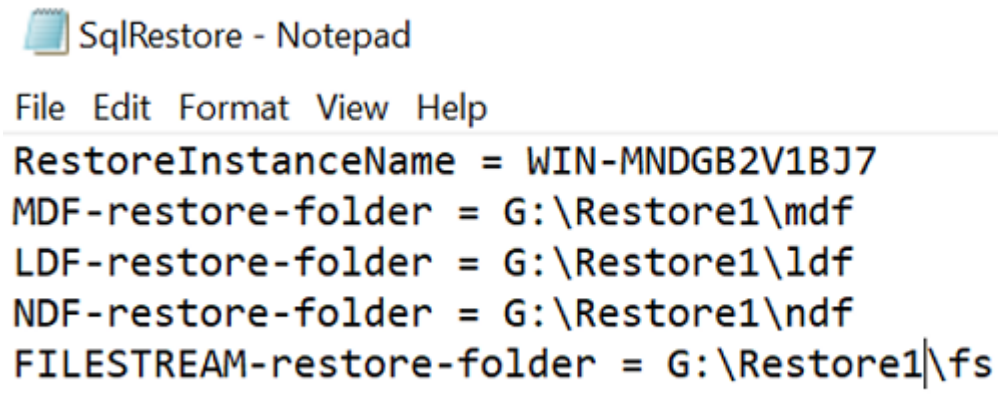
Restauración de la base de datos SQL a una ubicación alternativa en la misma instancia

Esta sección proporciona información sobre cómo restaurar la base de datos SQL con FileStream activado en una ubicación alternativa pero en la misma instancia mientras se cambia el nombre de la base de datos.

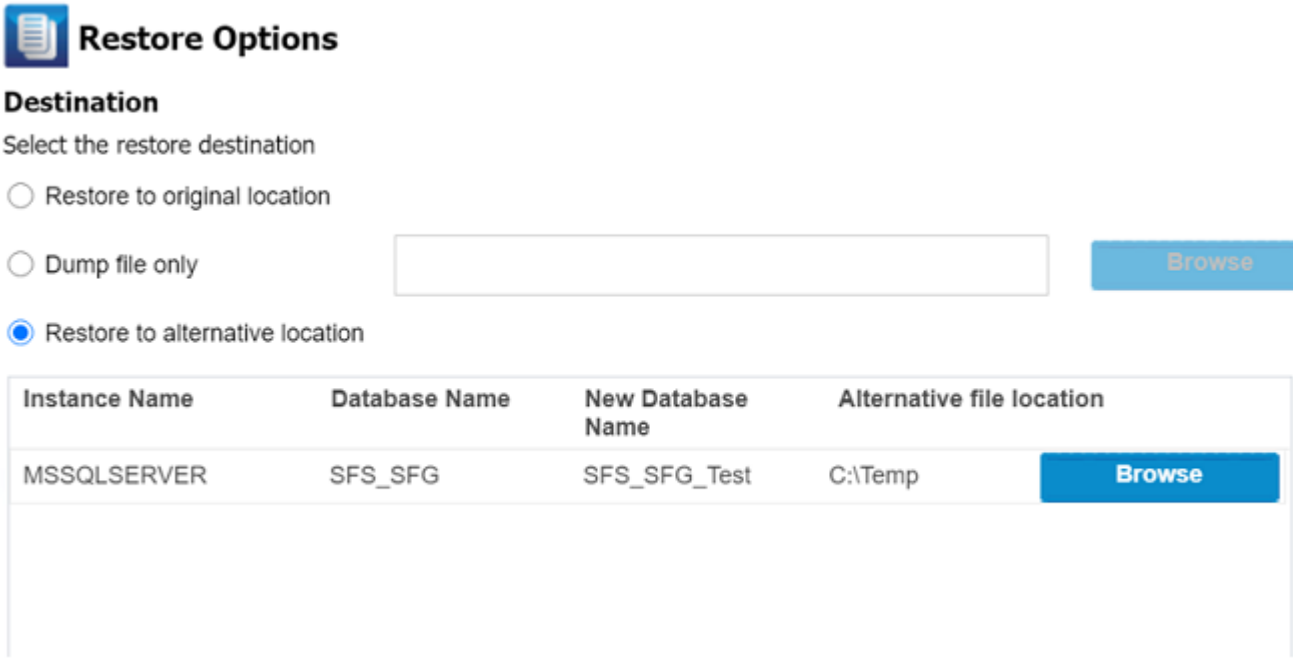
Siga estos pasos:

1. Para modificar la base de datos de restauración a una ubicación alternativa, abra el archivo SqlRestore.ini y, a continuación, cambie las ubicaciones de la carpeta según sea necesario.

   Por ejemplo, cambie las ubicaciones de la carpeta de *C:\singlefs_singlefsgrp\SFS_SFG1* a *G:\Restore1\fs1*.



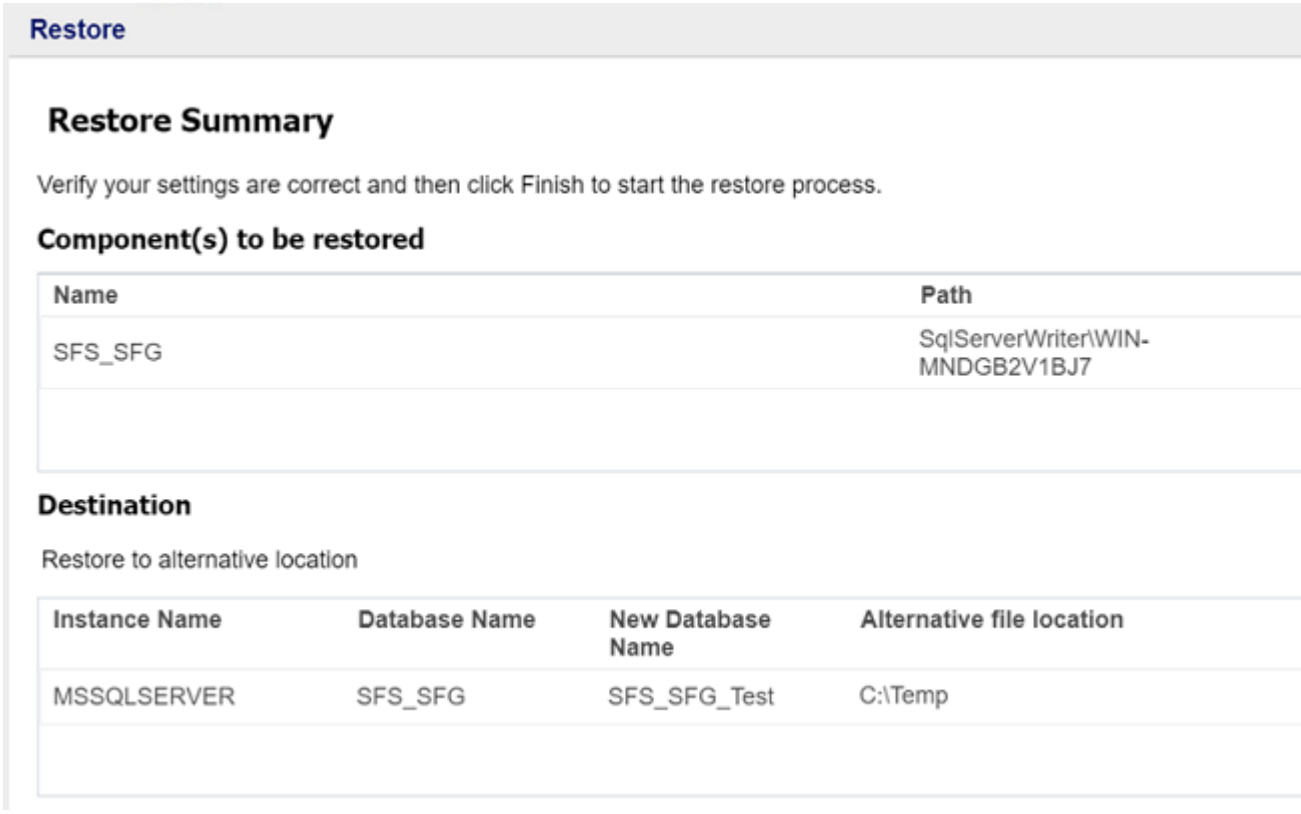
2. En el Agente, en la página Restaurar, seleccione la base de datos que desea restaurar y, a continuación, haga clic en **Siguiente**.
3. En la pantalla Opciones de restauración, seleccione **Restaurar en una ubicación alternativa** y explore la instancia.



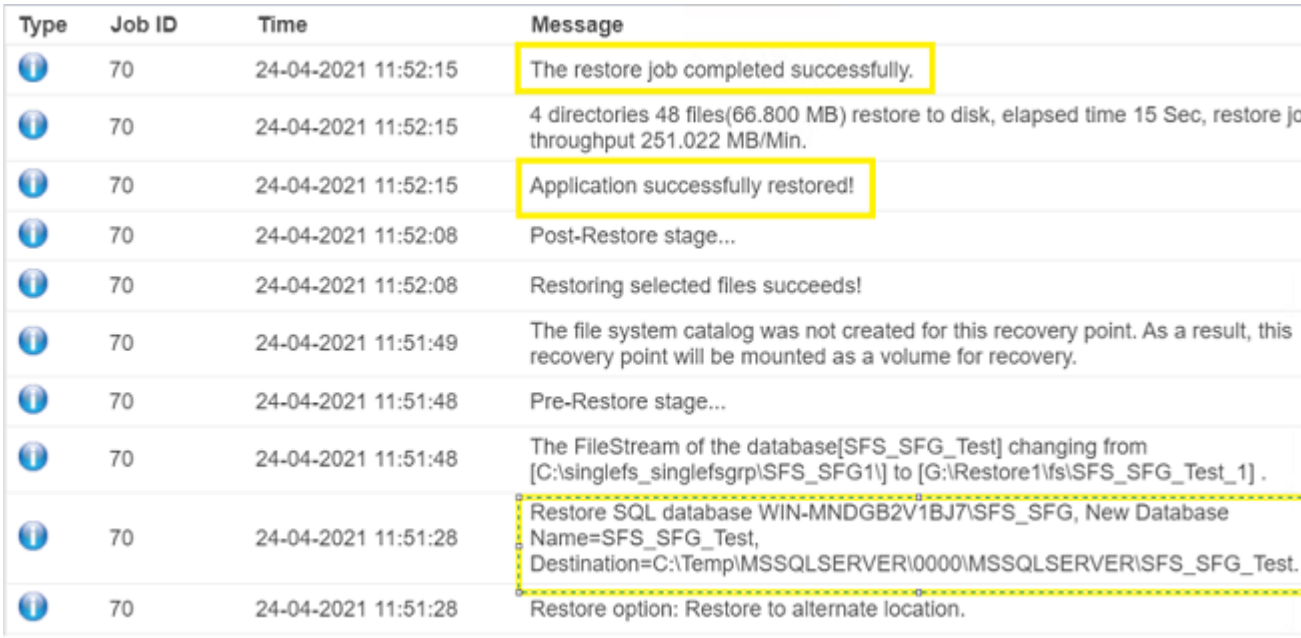
Para renombrar el nombre de la base de datos, haga clic en el área de texto **Nuevo nombre de la base de datos** y especifique el nuevo nombre. Por ejemplo, *SFS_SFG* se renombra como *SFS_SFG_Test*.

Nota: En Ubicación alternativa del archivo, se selecciona una carpeta temporal. Esta ubicación procesa la restauración de archivos a la ubicación definida en el archivo SqlRestore.ini.

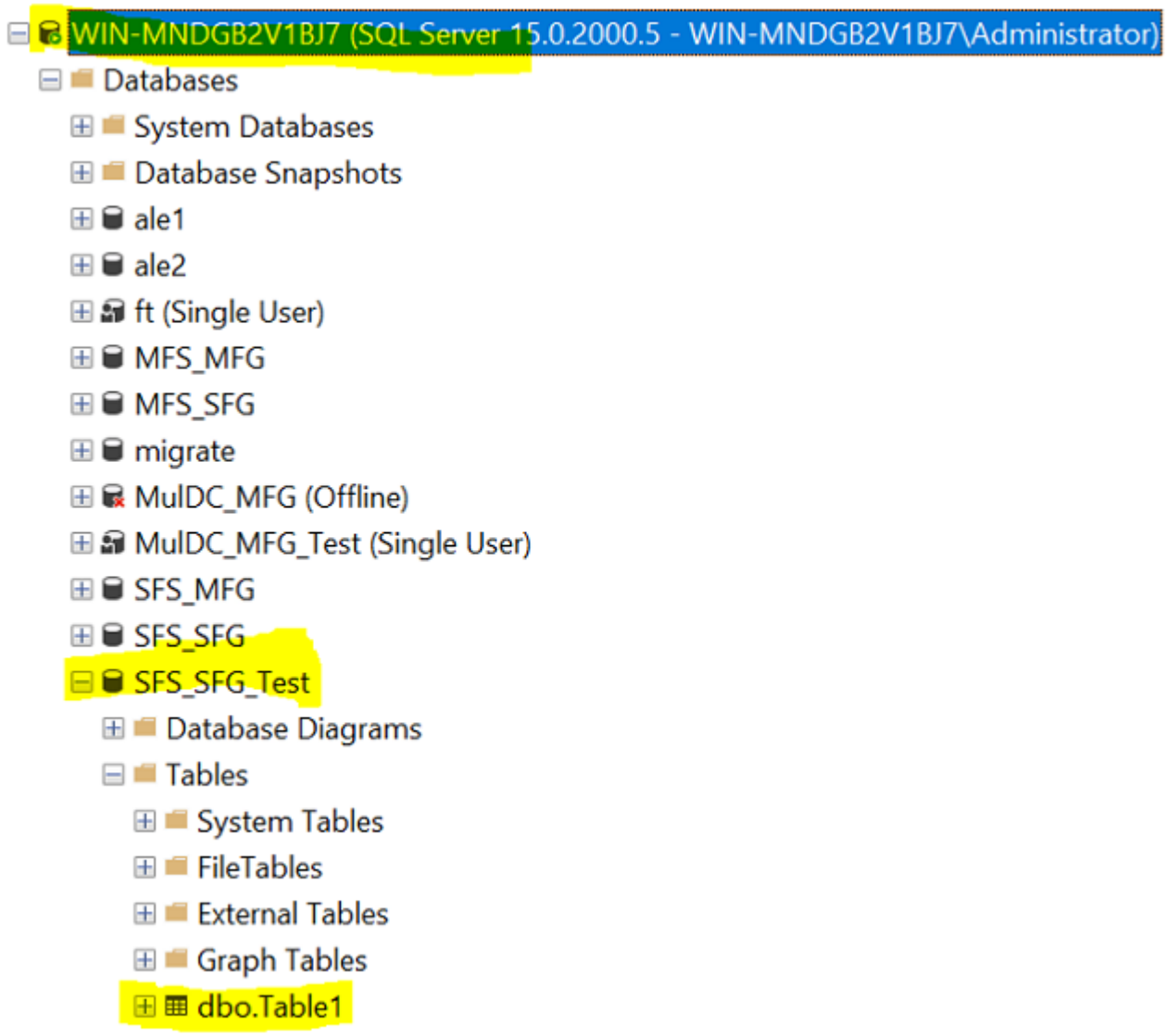
4. Compruebe si la configuración es correcta y, a continuación, haga clic en **Finalizar** para iniciar el proceso de restauración.



El registro de actividad muestra el estado de la restauración junto con el cambio de nombre de la base de datos.



El cambio en el nombre de la base de datos se refleja en SQL Management Studio.

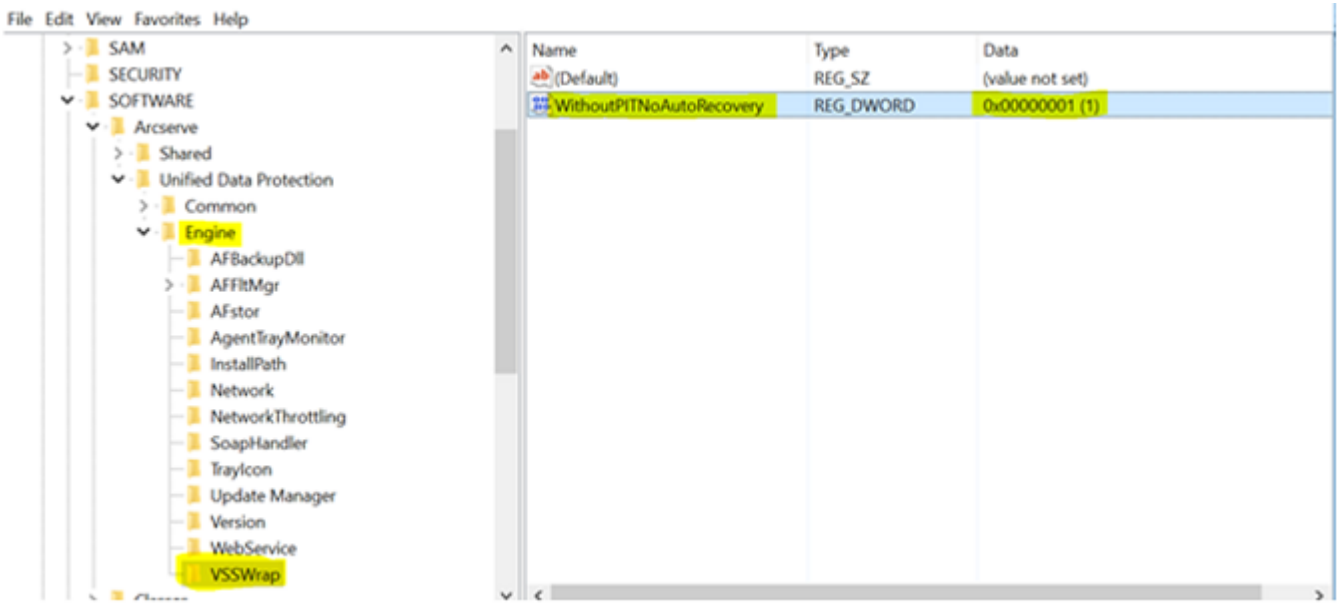


Modo de restauración a través de la clave de registro

Esta sección proporciona información sobre cómo utilizar el modo de restauración utilizando la clave de registro. Este método restaura la base de datos con Files-tream activado a la instancia alternativa (INS1_FSE).

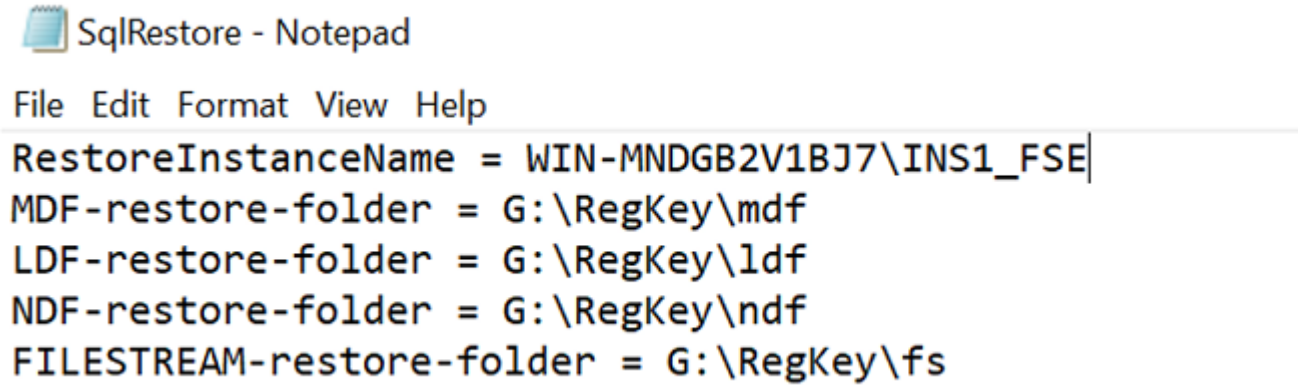
Después de que la copia de seguridad se realice correctamente, agregue la clave de registro en la carpeta VSSWrap con el valor DWORD de 32 bits: *Withou-tPITNoAutoRecovery* y establezca el valor en 1.

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Pro-tection\Engine\VSSWrap\

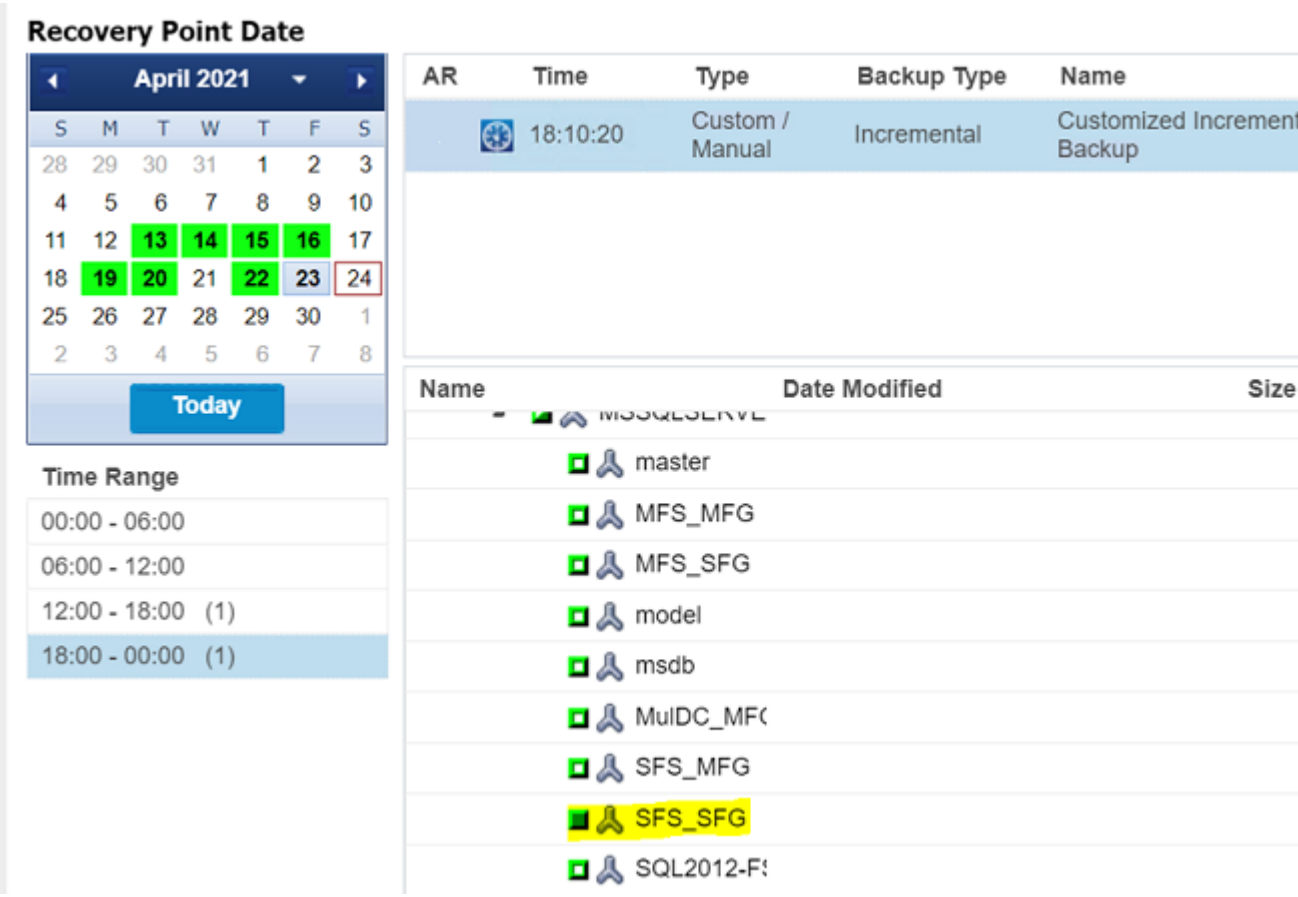


Siga estos pasos:

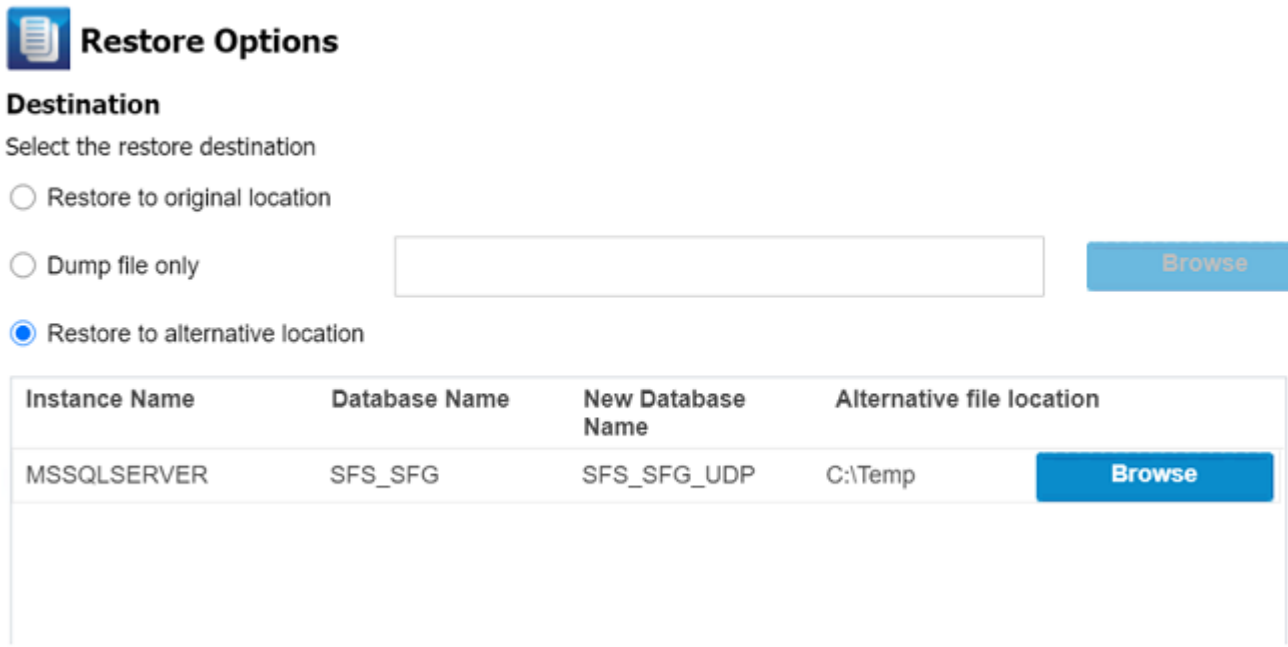
1. Para restaurar la base de datos a una instancia alternativa, abra el archivo SqlRestore.ini y, a continuación, cambie las ubicaciones de la carpeta según sea necesario.



2. En el Agente, en la página Restaurar, seleccione la base de datos que desea restaurar y, a continuación, haga clic en **Siguiente**.



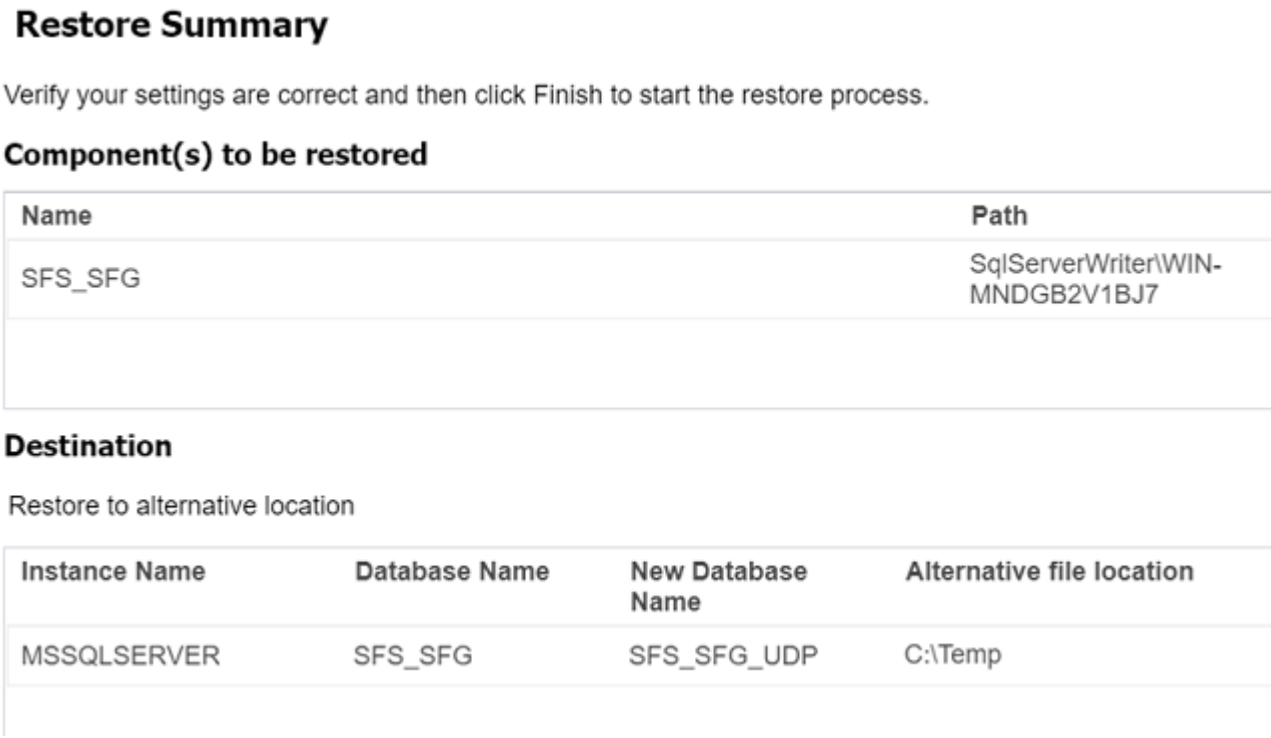
3. En la pantalla Opciones de restauración, seleccione **Restaurar en una ubicación alternativa** y explore la instancia.



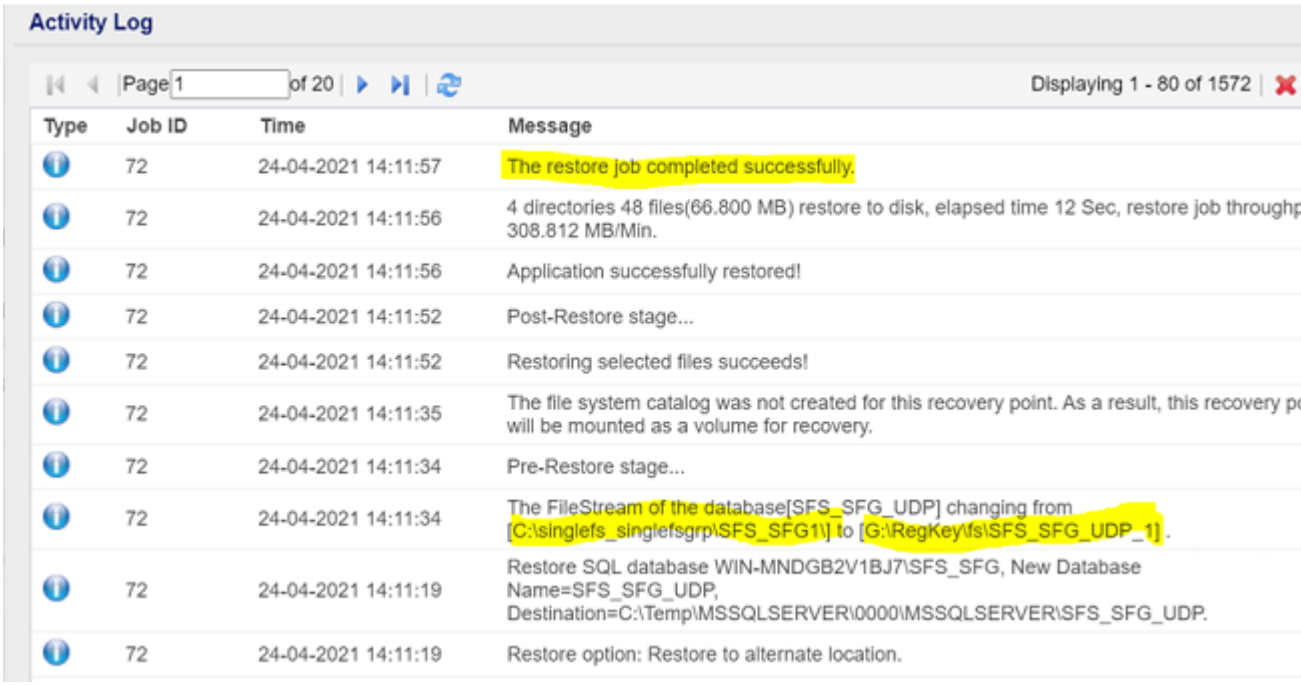
Para renombrar el nombre de la base de datos, haga clic en el área de texto **Nuevo nombre de la base de datos** y especifique el nuevo nombre. Por ejemplo, *SFS_SFG* se renombra como *SFS_SFG_UDP*.

Nota: En Ubicación alternativa del archivo, se selecciona una carpeta temporal. Esta ubicación procesa la restauración de archivos a la ubicación definida en el archivo SqlRestore.ini.

4. Compruebe si la configuración es correcta y, a continuación, haga clic en **Finalizar** para iniciar el proceso de restauración.



El registro de actividad muestra el estado de la restauración junto con el cambio de nombre de la base de datos.



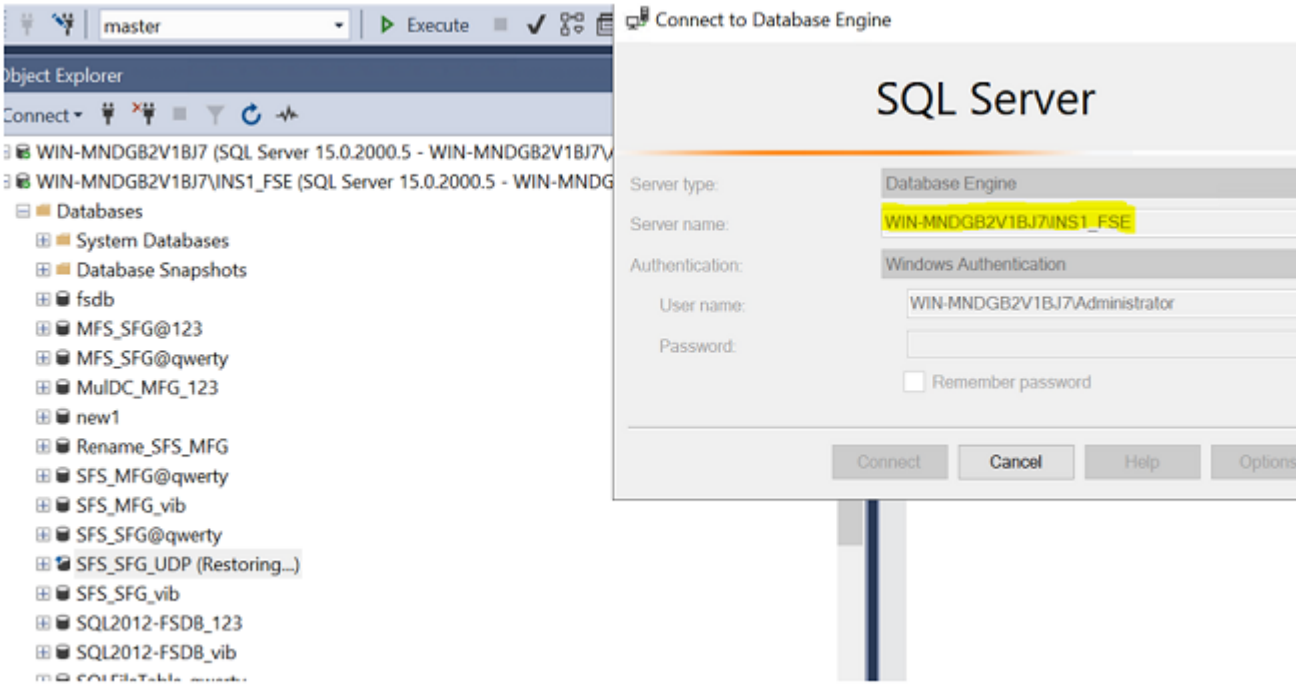
En ciertos casos, la base de datos todavía se muestra como en restauración incluso después de que la tarea se complete correctamente.



Para eliminar la base de datos del modo de restauración, haga lo siguiente:

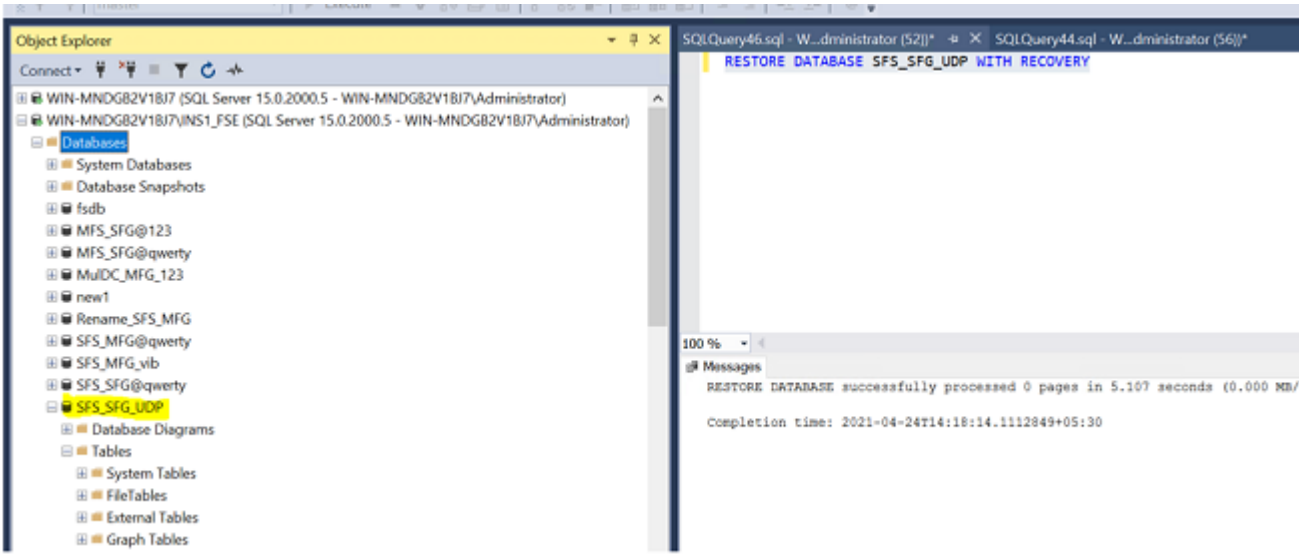
1. Haga clic con el botón secundario del ratón en la base de datos y, a continuación, seleccione **Nueva consulta**.

   La ventana aparece y se conecta a la instancia restaurada.



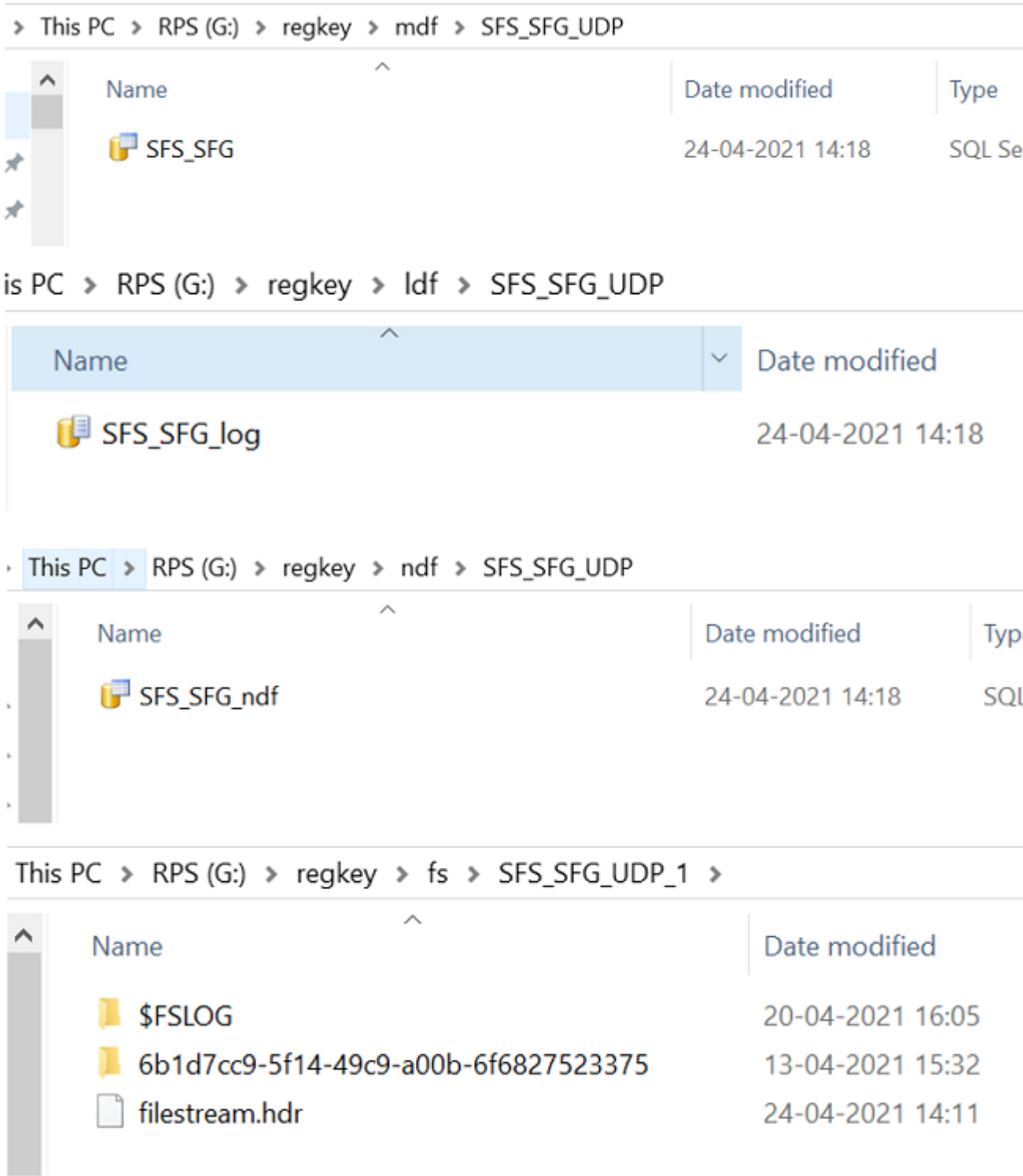
2. En la ventana de consulta, ejecute la consulta siguiente.

   RESTORE DATABASE [DATABASE NAME] WITH RECOVERY



   El modo de restauración se elimina de la base de datos.

   Nota: Cuando el cambio de nombre de un archivo de la base de datos no se realiza correctamente mientras se utiliza el registro, la carpeta principal muestra el nuevo nombre. Sin embargo, los archivos de la base de datos como MDF, NDF y LDF muestran el nombre de la base de datos original.


This PC › RPS (G:) › regkey › mdf › SFS_SFG_UDP
Name
Date modified
Type
SFS_SFG
24-04-2021 14:18
SQL Se
is PC › RPS (G:) › regkey › ldf › SFS_SFG_UDP
Name
Date modified
SFS_SFG_log
24-04-2021 14:18
This PC › RPS (G:) › regkey › ndf › SFS_SFG_UDP
Name
Date modified
Typ
SFS_SFG_ndf
24-04-2021 14:18
SQL
This PC › RPS (G:) › regkey › fs › SFS_SFG_UDP_1 ›
Name
Date modified
$FSLOG
20-04-2021 16:05
6b1d7cc9-5f14-49c9-a00b-6f6827523375
13-04-2021 15:32
filestream.hdr
24-04-2021 14:11

Cómo usar la utilidad Exchange Granular Restore (GRT)

En esta sección se incluye la siguiente información sobre la utilidad Exchange Granular Restore (GRT):

Introducción

Revisión de las consideraciones y requisitos previos

Cómo restaurar datos de Microsoft Exchange Data con la utilidad Exchange Granular Restore (GRT)

Introducción

La utilidad de restauración granular de Exchange se utiliza para restaurar el correo electrónico de Microsoft Exchange y los objetos que no son de correo electrónico. La utilidad incluye la capacidad de inserción de elementos, como los correos electrónicos, de bases de datos sin conexión (*.EDB) y archivos de registro a bases de datos originales en vivo de Exchange, así como la extracción de datos granulares a archivos de almacenamiento individual (.pst).

Esta utilidad incluye las siguientes ventajas esenciales:

- Es compatible con los elementos que no son de correo electrónico (por ejemplo, el calendario, los contactos y las tareas) y con las carpetas públicas.
- Puede trabajar con tan solo un archivo de base de datos. Los registros no son obligatorios, pero tenerlos garantizará que los datos más recientes estén disponibles para la restauración.
- No necesita generar un catálogo y restaura el correo directamente desde el punto de recuperación montado.
- Tarda un tiempo mínimo en restaurar un elemento de nivel de buzón de correo desde una base de datos o un buzón de usuario de cualquier tamaño.
- Es compatible con las opciones de línea de comando para procesar varias bases de datos.

Nota: Para obtener más detalles sobre las especificaciones compatibles, las funcionalidades y otras funciones, consulte la Guía del usuario de Exchange Granular Restore (esr.pdf).

Revisión de las consideraciones y requisitos previos

Verifique que los requisitos previos siguientes existen antes de realizar una restauración:

- La utilidad Exchange Granular Restore se encuentra disponible en la siguiente ubicación:

  La herramienta se instala con el Agente de Arcserve UDP en el siguiente directorio:

  ```
  X:\Archivos de programa\Arcserve\Unified Data Protection\Engine\Exchange GRT
  ```

  Nota: La herramienta se instala con el Agente de Arcserve UDP.

- La tarea de restauración se ha establecido para ejecutarse desde el equipo de Exchange o el equipo de proxy HBBU.

  Nota: Si desea ejecutar la tarea de restauración en cualquier otro equipo, busque el punto de recuperación desde el destino de la copia de seguridad.

- El nombre de la base de datos, el nombre del servidor, la ruta de acceso a la base de datos (.edb) y los archivos de registro del usuario se identifican para llevar a cabo la tarea de restauración.

  Para realizar la identificación, utilice Exchange Management Console (EMC), Exchange Control Panel (ECP) o Exchange Management Shell.

  Por ejemplo:

  ```
  Get-Mailbox -identity "nombreusuario" | fl Database
  ```

  ```
  Get-MailboxDatabase -identity "nombrebasedatos" |
  fl Name, Server, EdbFilePath,LogFolderPath
  ```

Cómo restaurar datos de Microsoft Exchange Data con la utilidad Exchange Granular Restore (GRT)

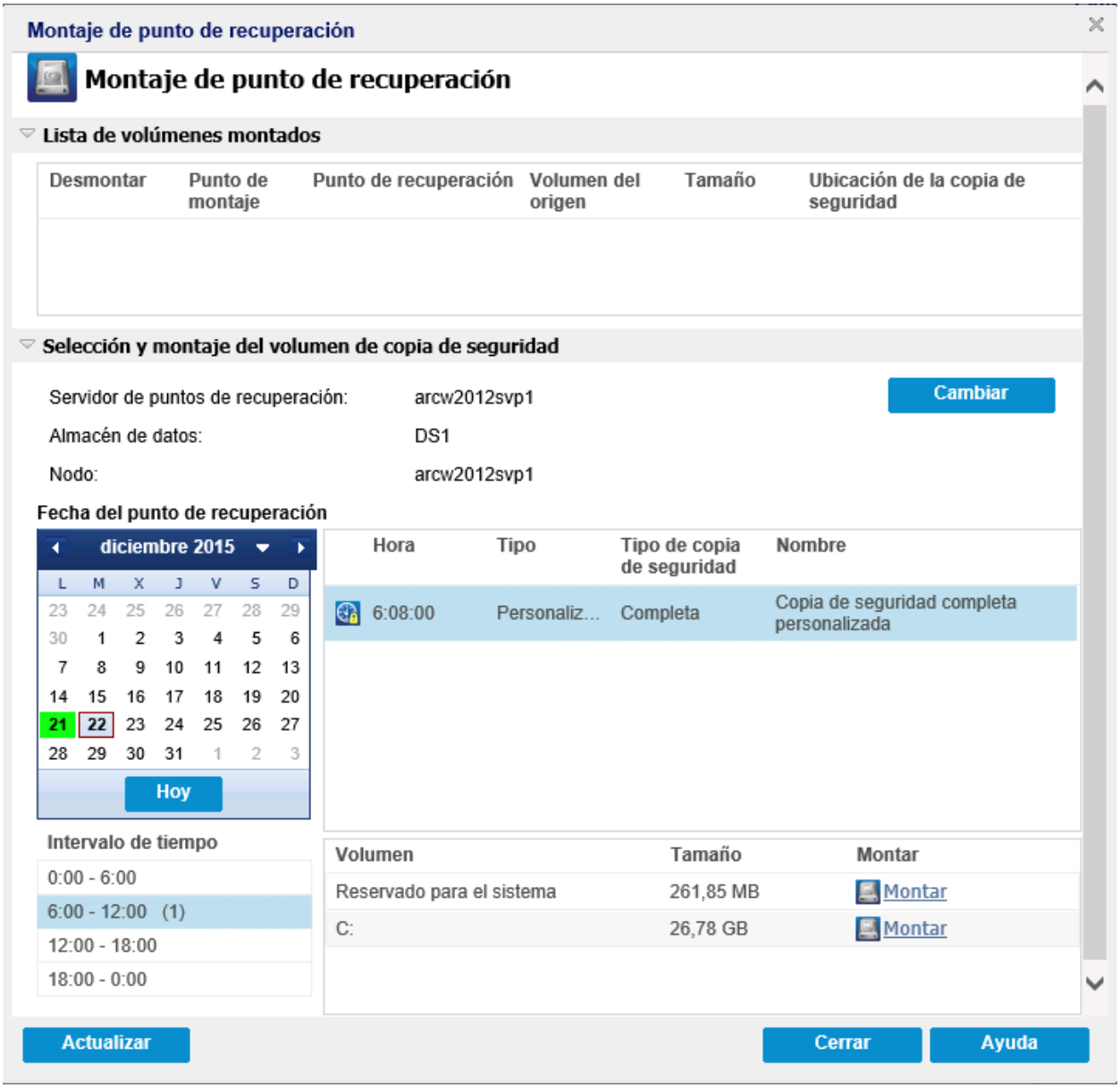
Antes de comenzar, consulte los requisitos previos y las consideraciones.

Realice las tareas siguientes para restaurar los elementos del buzón de correo de Microsoft Exchange mediante la utilidad Exchange Granular Restore:

1. En la Consola del Agente de Arcserve UPD, seleccione la tarea Montar punto de recuperación (recomendado) o restaure la base de datos de Exchange en la unidad local. Aparecerá el cuadro de diálogo Montar punto de recuperación.

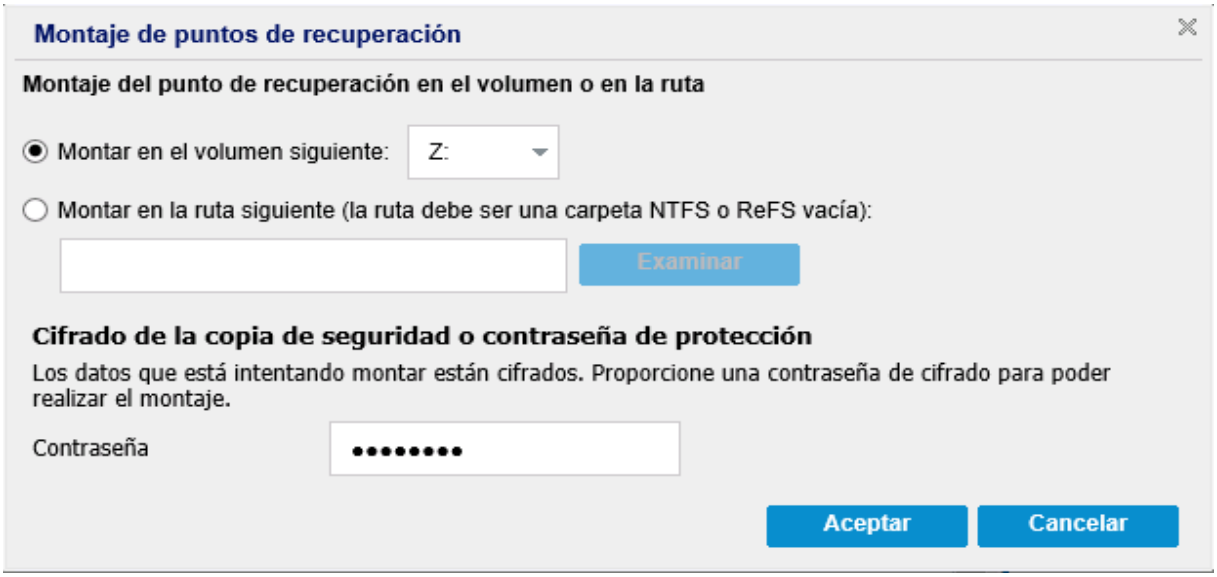


2. Seleccione la fecha del punto de recuperación y haga clic en **Montar** para los volúmenes que contienen la base de datos y los registros de Exchange.



Nota: Si el servidor que está ejecutando la tarea de restauración no es el proxy HBBU o Exchange, haga clic en **Cambiar** para seleccionar el servidor de puntos de recuperación, el almacén de datos y el servidor de Exchange apropiados.

3. Seleccione la letra de unidad de disco para montar el volumen y haga clic en **Aceptar**.



4. Inicie la utilidad Exchange Granular Restore desde una de las siguientes ubicaciones:

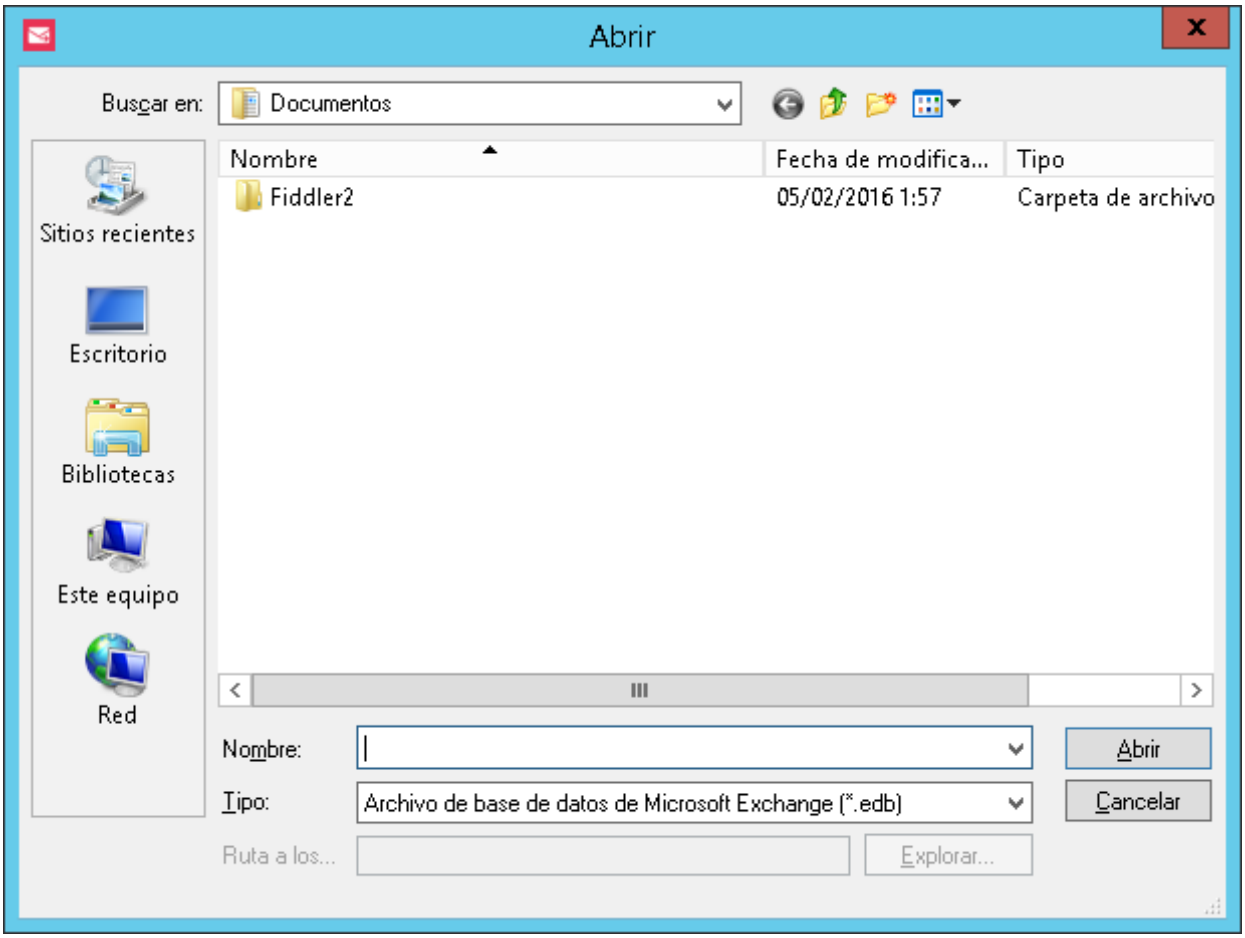
   Inicio > Todos los programas > Arcserve > Unified Data Protection > Arcserve UDP Exchange Granular Restore

   O

   X:\Archivos de programa\Arcserve\Unified Data Protection\Engine\Exchange GRT\esr.exe

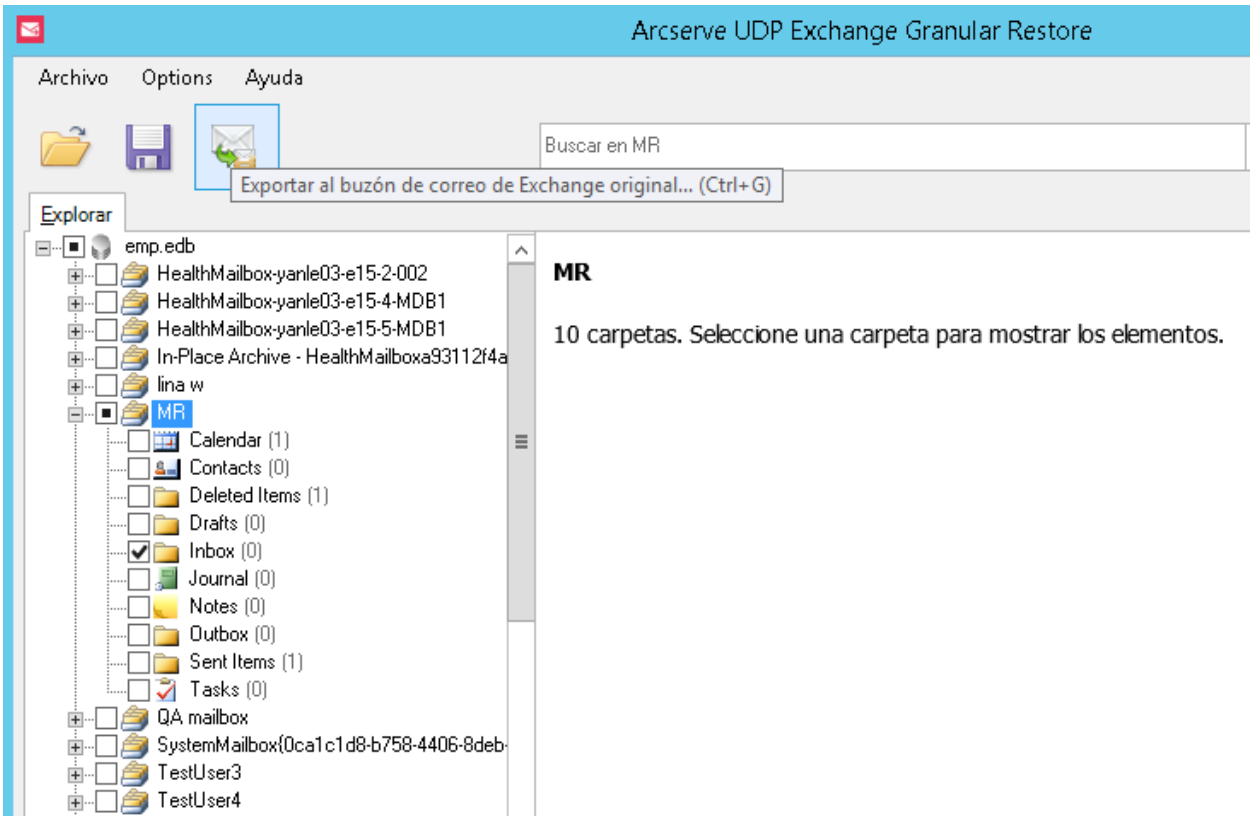
   Aparecerá un cuadro de diálogo en el que podrá especificar la ruta para la base de datos y los archivos de registro.

5. Especifique la ruta al volumen montado y haga clic en **Abrir**.



Se abrirá la utilidad Exchange Granular Restore de Arcserve UPD.

6. Seleccione los datos de usuario que desee restaurar y haga clic en **Export into original mailbox (Exportar en el buzón de correo original)** o **Export into .PST (Exportar en .PST)**.



Notas:

- Para obtener más detalles sobre las limitaciones, las opciones de usuario, las funciones y las especificaciones compatibles, consulte la Guía del usuario de Exchange Granular Restore (esr.pdf), ubicada en:

  %Archivos de programa%\Arcserve\Unified Data Protection\Engine\Exchange GRT o en la Biblioteca.

- De forma predeterminada, la utilidad emplea el usuario actual que ha iniciado sesión en Windows para establecer la conexión. Si dicho usuario no tiene permisos para suplantar al usuario seleccionado, aparecerá un mensaje de error en el panel **Detalles**.

  Si se ha producido un error, la acción recomendada consiste en iniciar sesión en el equipo con una cuenta que disponga de derechos de suplantación para el usuario seleccionado o la cuenta de este.

7. Cuando se complete la tarea de restauración, desmonte el volumen que se ha utilizado para la recuperación.

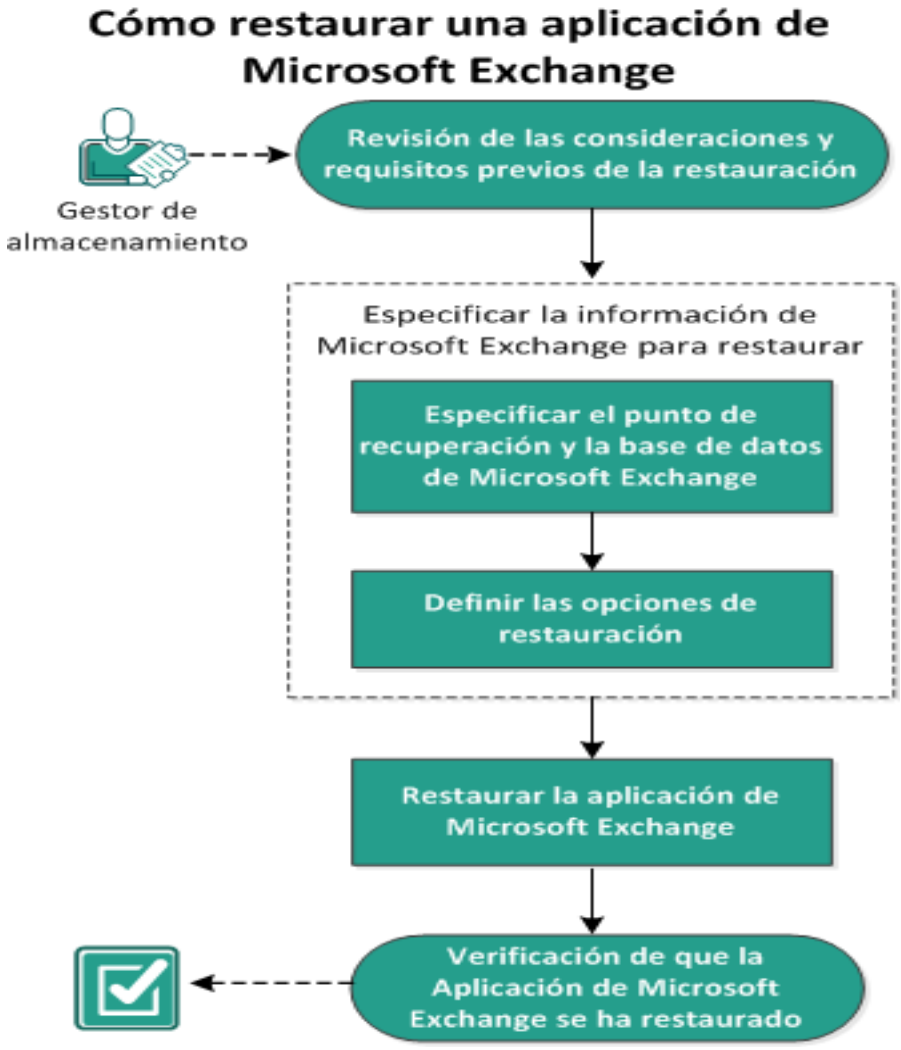
   Para desmontar el volumen, en la Consola del Agente de Arcserve UDP, haga clic en **Montar punto de recuperación** y, a continuación, haga clic en **Desmontar**.


Montaje de punto de recuperación
Montaje de punto de recuperación
Lista de volúmenes montados
Desmontar
Punto de montaje
Punto de recuperación
Volumen del origen
Tamaño
Ubicación de la copia de seguridad
Desmontar
Z:
22/12/2015 6:08:00
C:
26,78 GB
\\arcw2012svp1\CA_UDP_D...

Cómo restaurar una aplicación de Microsoft Exchange

El Agente de Arcserve UDP (Windows) no solo permite proteger y recuperar los datos, sino que también ayuda a obtener las aplicaciones que utilizarán los datos y que los ejecutarán. El método Restauración por punto de recuperación es la única manera de recuperar las aplicaciones. Durante la recuperación de las aplicaciones, el Agente de Arcserve UDP (Windows) aprovecha el Servicio de instantáneas de volumen (VSS) de Windows para garantizar la coherencia de los datos de cualquier aplicación con VSS. Mediante el Agente de Arcserve UDP (Windows), se puede recuperar la aplicación de Microsoft Exchange Server sin necesidad de realizar una recuperación completa de desastres.

El diagrama siguiente ilustra el proceso para restaurar una aplicación de Microsoft Exchange:



Realice las tareas siguientes para restaurar una aplicación de Microsoft Exchange:

1. Revisión de las consideraciones y requisitos previos de la restauración
2. Especificación de la información de Microsoft Exchange para restaurar
    a. Especificación del punto de recuperación y de la base de datos de Microsoft Exchange
    b. Definición de las opciones de restauración
3. Restauración de la aplicación de Microsoft Exchange
4. Verificación de que la aplicación de Microsoft Exchange se ha restaurado

Revisión de las consideraciones y requisitos previos de la restauración

El Agente de Arcserve UDP (Windows) admite las siguientes versiones de Microsoft Exchange Server:

- Microsoft Exchange 2010: entorno de servidor único y entorno del grupo de disponibilidad de la base de datos (DAG).
- Microsoft Exchange 2013 y 2016: entorno de servidor único y entorno del grupo de disponibilidad de la base de datos (DAG).

  Para el entorno de Microsoft Exchange Server 2010, 2013 y 2016 DAG, se deberá instalar el Agente de Arcserve UDP (Windows) en todos los servidores miembros del grupo de DAG. La copia de seguridad también puede realizarse desde cualquier servidor miembro para las copias de base de datos activas y pasivas, pero la restauración sólo puede realizarse en una copia de la base de datos activa.
- Aunque todos los miembros de DAG pueden formar parte del mismo o de otro plan de copia de seguridad, se recomienda utilizar el mismo almacén de datos de deduplicación para eliminar datos duplicados.

Se puede restaurar Microsoft Exchange Server en los niveles siguientes:

Nivel del editor de Microsoft Exchange

Si desea restaurar todos los datos de Microsoft Exchange Server, se puede realizar una restauración en el nivel de editor de Microsoft Exchange.

Nivel de grupo de almacenamiento

Si desea restaurar un grupo de almacenamiento específico, se puede realizar una restauración en este nivel.

Nota: El nivel del grupo de almacenamiento no se aplica para Microsoft Exchange Server 2010, 2013 ni 2016.

Nivel de la base de datos del buzón de correo (Microsoft Exchange 2010, 2013 y 2016)

Si desea restaurar una base de datos del buzón de correo específico, se podrá realizar una restauración en este nivel.

Nivel del buzón de correo (Microsoft Exchange 2010, 2013, y 2016)

Define si se desea restaurar un buzón de correo específico o un objeto de correo.

Verifique que los requisitos previos siguientes existen antes de realizar una restauración de Microsoft Exchange:

Restauración a nivel de base de datos

- El equipo de destino tiene el mismo nombre y la misma versión instalada que la de Microsoft Exchange.
- La base de datos de destino tiene el mismo nombre de base de datos y el mismo nombre de grupo de almacenamiento (Microsoft Exchange 200X) y forma parte de la misma organización de Microsoft Exchange.

Restauración a nivel granular

- Para restaurar datos de Microsoft Exchange, se recomienda utilizar la utilidad Exchange Granular Restore.

Especificación de la información de Microsoft Exchange para restaurar

El Agente de Arcserve UDP (Windows) no solo permite proteger y recuperar los datos, sino que también ayuda a obtener la aplicación de Microsoft Exchange Server que utilizará los datos y que los ejecutará. La recuperación del servidor de Microsoft Exchange sólo puede realizarse mediante el método Restaurar por punto de recuperación.

El proceso implicado en la restauración de la aplicación de Microsoft Exchange es el siguiente:

1. Especificación del punto de recuperación y de la base de datos de Microsoft Exchange
2. Definición de las opciones de restauración

Especificación del punto de recuperación y de la base de datos de Microsoft Exchange

Utilice la opción **Explorar puntos de recuperación** para restaurar desde un punto de recuperación. Al seleccionar una fecha de recuperación, aparecerán todos los puntos de recuperación asociados para la fecha. Tiene la opción de explorar y seleccionar la base de datos de Microsoft Exchange que desee restaurar.

Siga estos pasos:

1. Acceda al cuadro de diálogo Selección del método de recuperación de una de las formas siguientes:

   Desde Arcserve UDP:

   a. Inicie sesión en Arcserve UDP.

   b. Haga clic en la ficha **recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos agregados en el panel central.

   d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   e. Haga clic en **Restaurar** de la opción desplegable **Acción**.

      El cuadro de diálogo Selección del método de restauración se abre.

      Nota: Se inicia sesión automáticamente en el nodo del Agente y el cuadro de diálogo Selección del método de restauración se abre desde el nodo del Agente.

   Desde el Agente de Arcserve UDP (Windows):

   a. Inicie sesión en el Agente de Arcserve UDP (Windows).

   b. En la página principal, seleccione **Restaurar**.

   El cuadro de diálogo Selección del método de restauración se abre.

2. Haga clic en la opción **Explorar puntos de recuperación**.

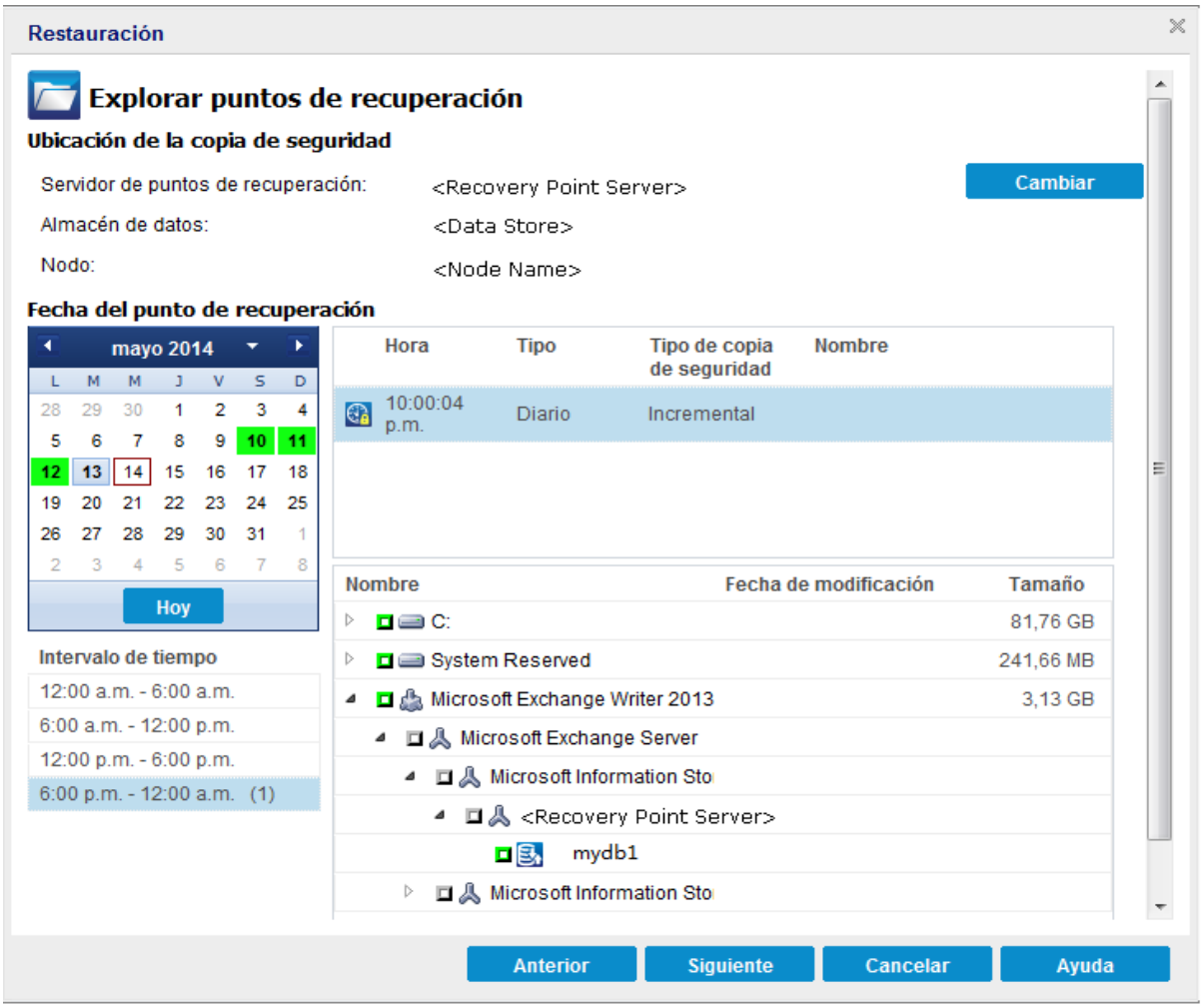
   Aparecerá el cuadro de diálogo **Explorar puntos de recuperación.**

3. Seleccione el punto de recuperación (fecha y hora) y, a continuación, seleccione la base de datos de Microsoft Exchange para restaurar.

   La casilla de marcador correspondiente aparecerá rellenada (verde) para indicar que se ha seleccionado la base de datos para restaurar.

   Nota: Si no desea que los archivos de registro de transacciones se apliquen después de la restauración, debe suprimirlos manualmente antes de que se realice la

restauración. Para más información acerca de cómo suprimir archivos de registro de transacciones manualmente, consulte la documentación de Microsoft Exchange Server.



4. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Opciones de restauración**.

Definición de las opciones de restauración

Después de especificar un punto de recuperación y el contenido que se deben restaurar, defina las opciones de copia para el punto de recuperación seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, seleccione el destino de la restauración.



2. Seleccione el destino de la restauración.

Las opciones disponibles son la restauración en la ubicación original de la copia de seguridad, la restauración en el archivo de vaciado o la restauración en un grupo de almacenamiento de recuperación/ base de datos de buzón de correo de recuperación.

Restauración en la ubicación original

Restaura en la ubicación original desde la que se ha capturado la imagen de copia de seguridad.

Solo archivo de vaciado

Restaura sólo los archivos de vaciado.

Para esta opción, el Agente de Arcserve UDP para Windows restaura el archivo de la base de datos de Microsoft Exchange en una carpeta específica y no lo conectará hasta después de la recuperación. Se puede utilizar para realizar un montaje manual en Microsoft Exchange Server.

Nota: Si existe una base de datos de buzón de correo de recuperación, se producirá un error en la restauración de la opción **Solamente archivos de vaciado**.

Reproducir el registro en la base de datos

Indica que al vaciar los archivos de la base de datos en la carpeta de destino, es posible reproducir los archivos de registro de transacciones de Microsoft Exchange y confirmarlos en la base de datos.

Desmontar la base de datos antes de restaurar y montar la base de datos antes de la restauración

Normalmente antes de una restauración, Microsoft Exchange realizará algunas comprobaciones para garantizar los siguientes puntos:

- La base de datos para restaurar está en el estado *Desmontado*.
- La base de datos no se restaura de manera inesperada.

Para evitar que una base de datos de producción de Microsoft Exchange se restaure de manera inesperada, se agrega un conmutador para poder sobrescribir la base de datos durante el proceso de restauración. Microsoft Exchange no puede restaurar una base de datos si no se establece este conmutador.

En el Agente de Arcserve UDP para Windows, estas dos opciones se controlan mediante la opción Desmonte la base de datos antes de realizar una restauración y móntela de nuevo al terminar. Mediante esta opción, Agente de Arcserve UDP para Windows permite iniciar el proceso de restauración automáticamente sin necesidad de ejecutar ninguna operación manual. (Se puede especificar también desmontar/montar la base de datos de manera manual).

- Si se selecciona, especifica que el proceso de recuperación desmontará automáticamente la base de datos de Microsoft Exchange antes del proceso de restauración y después la montará una vez finalizado el proceso de restauración. Además, si se selecciona, esta opción permitirá que la base de datos de Microsoft Exchange se sobrescriba durante la restauración.
- Si está desactivada, especifica que el proceso de recuperación no desmontará la base de datos de Microsoft Exchange de forma automática antes de la recuperación, sino que la montará después.

El administrador de Microsoft Exchange debería realizar algunas operaciones manuales como desmontar la base de datos de Microsoft Exchange, establecer el indicador Permite la sobrescritura en la base de datos y montar la base de datos de Microsoft Exchange. (Exchange realiza el procedimiento de recuperación durante el montaje de la base de datos).

Además, si esta opción no está activada, no se podrá sobrescribir la base de datos de Microsoft Exchange durante la restauración.

Restauración en la base de datos de recuperación (Microsoft Exchange 2010 y 2013)

Restaura la base de datos en una base de datos de recuperación. Una base de datos de recuperación es una base de datos que puede utilizarse con finalidades de recuperación. Es posible restaurar una base de datos del buzón de correo de Microsoft Exchange desde una base de datos de recuperación y, a continuación, recuperar y extraer los datos desde él sin que afecte a la base de datos de producción a la cual acceden los usuarios finales.

Antes de restaurar la base de datos de Microsoft Exchange 2010 o Exchange 2013 a una base de datos de recuperación, se debe crear una base de datos de recuperación.

3. Haga clic en **Siguiente**.

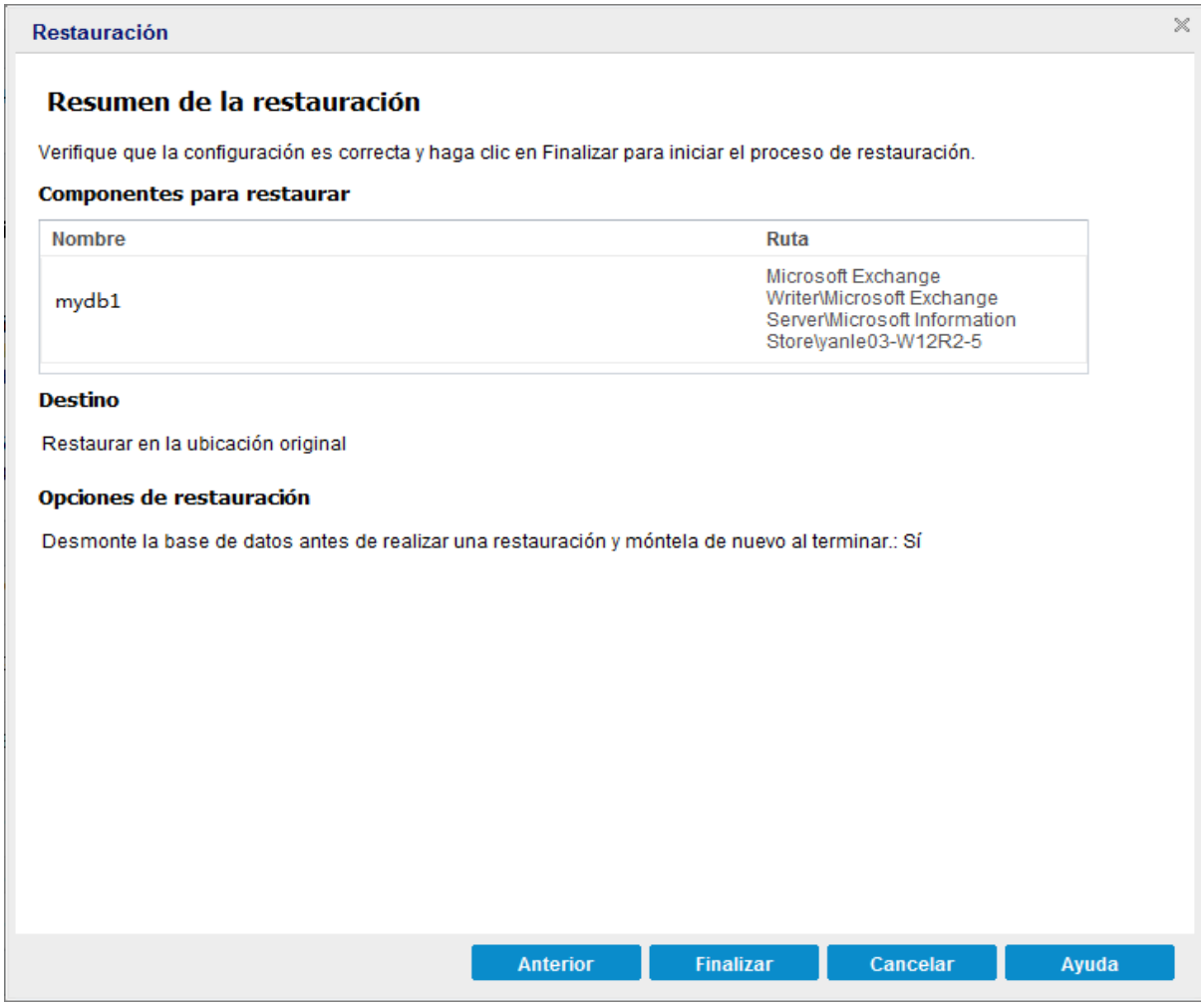
   Se abrirá el cuadro de diálogo **Resumen de la restauración**.

Restauración de la aplicación de Microsoft Exchange

Después de definir las opciones de restauración, verifique que los valores de configuración sean correctos y confirme el proceso de restauración. El **Resumen de la restauración** le ayuda a revisar todas las opciones de la restauración definidas y a modificarlas si es necesario.

Siga estos pasos:

1. En el cuadro de diálogo **Resumen de la restauración**, revise la información que aparece en pantalla para verificar que todos los valores de configuración y las opciones de restauración sean correctos.



- Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo anterior correspondiente para cambiar la configuración incorrecta.
- Si la información de resumen es correcta, haga clic en **Siguiente** y, a continuación, en **Finalizar** para iniciar el proceso de restauración.

La aplicación de Microsoft Exchange se restaura.

Verificación de que la aplicación de Microsoft Exchange se ha restaurado

Siga estos pasos:

1. Vaya al destino de la restauración especificado para el Agente de Arcserve UDP (Windows).

   Por ejemplo, si decide restaurar la base de datos de Microsoft Exchange en la ubicación original, después de finalizar la restauración, busque la ubicación física para comprobar si se restauran la base de datos de Microsoft Exchange y los registros.

   Si se selecciona realizar una restauración de la base de datos de Microsoft Exchange en un archivo de volcado como única ubicación, el Agente de Arcserve UDP (Windows) solamente restaurará la base de datos de Microsoft Exchange y los registros en una ubicación específica.

2. Compruebe que la aplicación de Microsoft Exchange se esté restaurando y asegúrese de que la base de datos se monta y es accesible.

   La aplicación de Microsoft Exchange se ha restaurado correctamente.

Cómo restaurar datos de Exchange en una máquina virtual de VMware

Importante: Para restaurar datos de Microsoft Exchange en una máquina virtual de VMware, se recomienda utilizar la utilidad Exchange Granular Restore.

Cómo descargar archivos o carpetas sin restaurar

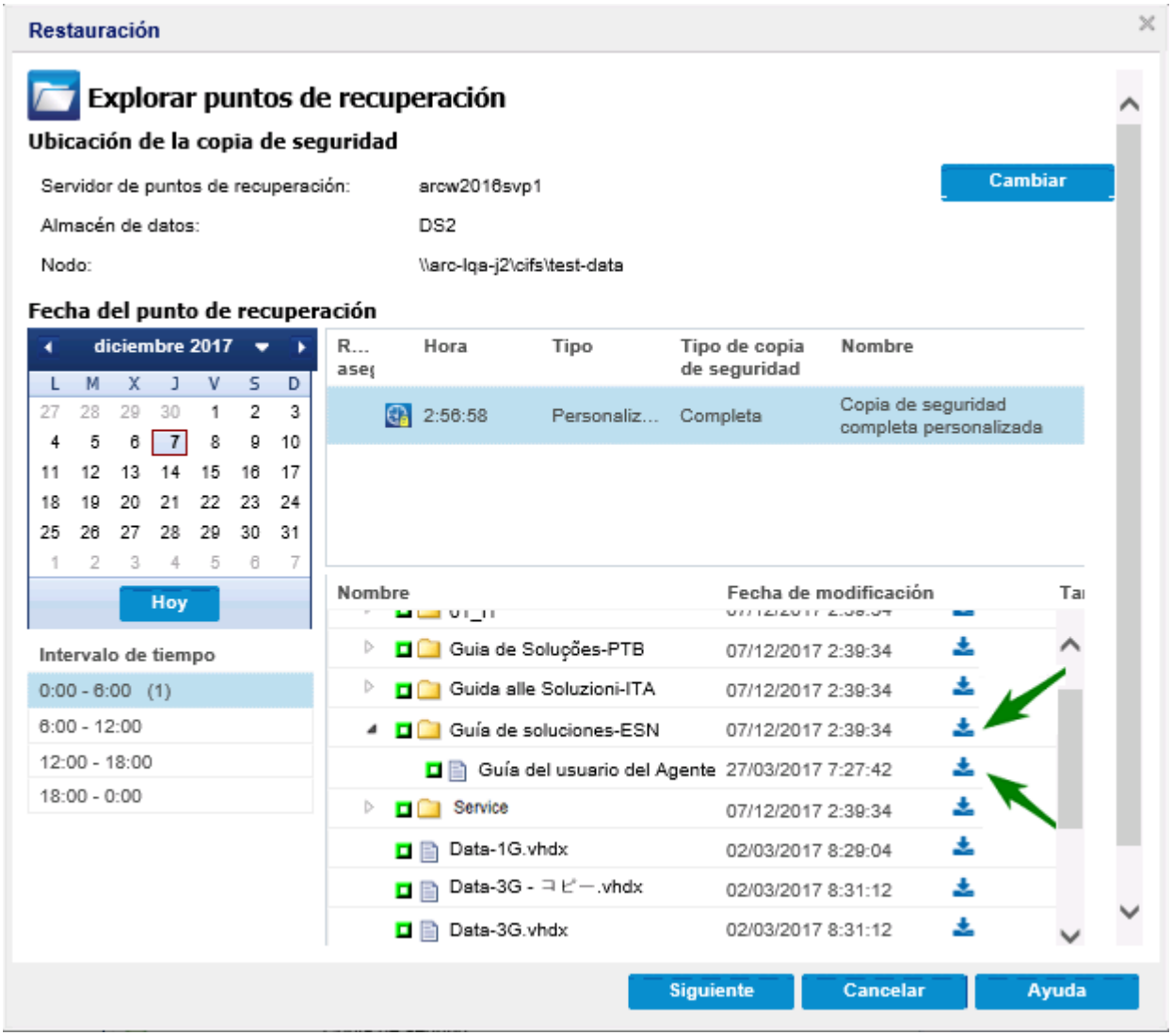
Arcserve UDP permite descargar un archivo o una carpeta completa sin tener que enviarlos a la restauración. En el Asistente de restauración, la pantalla Examen de puntos de recuperación permite descargar directamente cualquier archivo o carpeta completa con todos los archivos. El descargar antes de restaurar puede ayudar a realizar una comprobación rápida de los archivos para evitar que se restauren los archivos no deseados.

Nota: La descarga de los archivos no mantiene los permisos del archivo o carpeta.

Un solo archivo se descarga directamente en el mismo formato, mientras que una carpeta se descarga como un archivo ZIP. El archivo ZIP tiene el siguiente formato de nombre:

[nombredenodo]_[IDsesión]_[marcatiempo].zip

Para descargar, basta con que llegue a la pantalla Examen de puntos de recuperación en el Asistente de restauración. La captura de pantalla que se muestra a continuación muestra cómo se debe realizar la descarga de un archivo o carpeta:



Consideraciones sobre la descarga:

- La descarga o el empaquetado como archivo ZIP no es posible para algunos archivos del sistema. El servicio Agente de Tomcat no tiene suficientes privilegios para tener acceso a los archivos del sistema o a los archivos del usuario de otro nodo protegido.
- Para evitar un consumo excesivo de la memoria de Tomcat y del uso de la CPU, recomendamos enviar una tarea de restauración a la ruta alternativa mientras se descarga un archivo o carpeta grandes.
- Es posible que se produzca un error al utilizar las herramientas de carpeta comprimida de Windows para examinar los archivos ZIP descargados porque la herramienta encuentra que algunos de los nombres de entrada de los archivos ZIP son demasiado largos para buscarlos. Se recomienda utilizar otras herramientas ZIP para abrir el archivo. Por ejemplo, WinZip, WinRAR, 7-Zip.

- Es posible que el usuario de IE9 que utiliza HTTPS en IE9 y el servicio web del agente para proporcionar el servicio no pueda descargar los archivos. Un problema conocido de IE9 en la descarga de recursos desde una página dinámica a través de HTTPS evita esta descarga. Para obtener más información y soluciones, haga clic en vínculo para acceder al artículo de Microsoft.

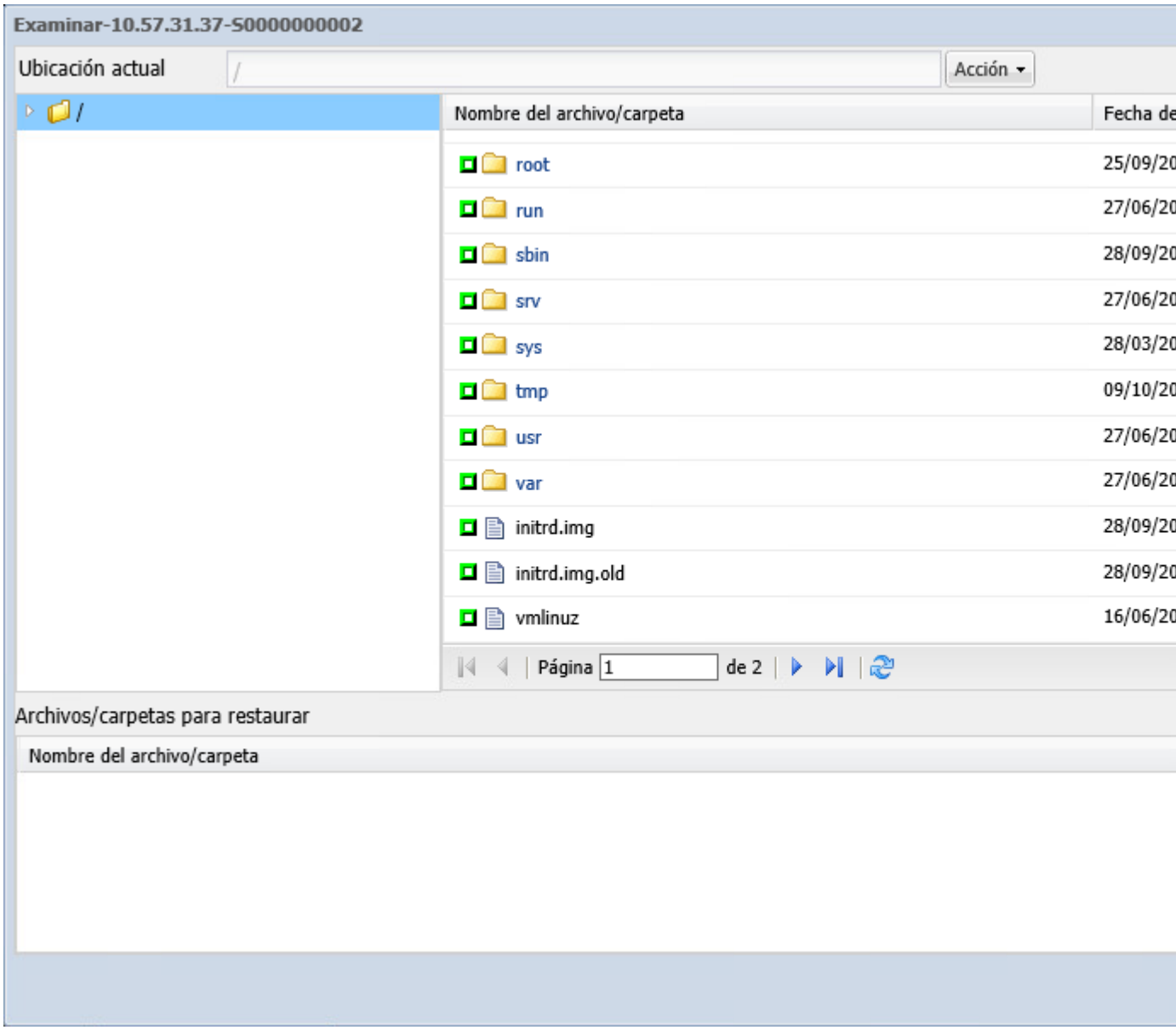
Cómo descargar archivos o carpetas sin restaurar para nodos de Linux

Arcserve UDP permite descargar un archivo o una carpeta completa sin tener que enviarlos a la restauración. En el Asistente de restauración, la pantalla Examen de puntos de recuperación permite descargar directamente cualquier archivo o carpeta completa con todos los archivos. El descargar antes de restaurar puede ayudar a realizar una comprobación rápida de los archivos para evitar que se restauren los archivos no deseados.

Un solo archivo se descarga directamente en el mismo formato, mientras que una carpeta se descarga como un archivo ZIP. El archivo ZIP tiene el siguiente formato de nombre:

[nombredenodo]_[IDsesión]_[marcatiempo].zip

Para descargar, basta con que llegue a la pantalla Examen de puntos de recuperación en el Asistente de restauración. La captura de pantalla que se muestra a continuación muestra cómo se debe realizar la descarga de un archivo o carpeta para los nodos de Linux:

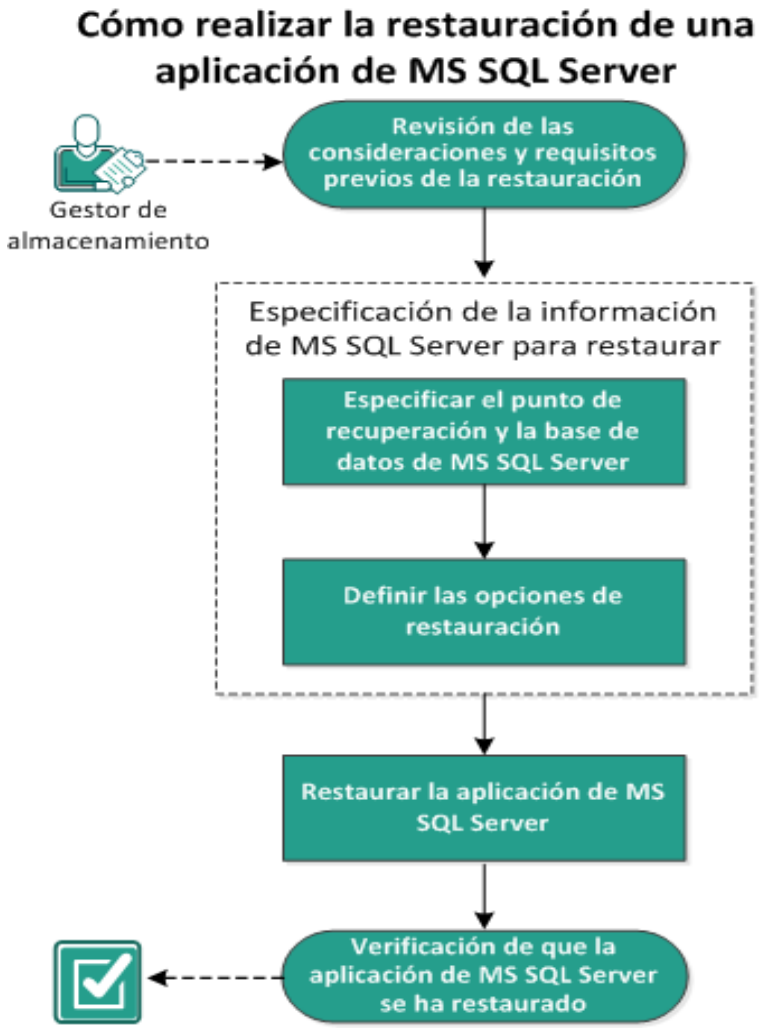


Para abrir los archivos descargados, utilice herramientas como WinZip, WinRAR, 7-Zip, etc.

Cómo restaurar una aplicación de Microsoft SQL Server

El Agente de Arcserve UDP (Windows) no solo permite proteger y recuperar los datos, sino que también ayuda a obtener las aplicaciones que utilizarán los datos y que los ejecutarán. El método Restauración por punto de recuperación es la única manera de recuperar las aplicaciones. Durante la recuperación de las aplicaciones, el Agente de Arcserve UDP (Windows) aprovecha el Servicio de instantáneas de volumen (VSS) de Windows para garantizar la coherencia de los datos de cualquier aplicación con VSS. Mediante el Agente de Arcserve UDP (Windows), se puede recuperar la aplicación de Microsoft SQL Server sin necesidad de realizar una recuperación completa de desastres.

El diagrama siguiente ilustra el proceso para restaurar una aplicación de Microsoft SQL Server:



Realice las tareas siguientes para restaurar una aplicación de Microsoft SQL Server:

1. Revisión de las consideraciones y requisitos previos de la restauración
2. Especificación de la información de Microsoft SQL Server para restaurar
    a. Especificación del punto de recuperación y de la base de datos de Microsoft SQL Server
    b. Definición de las opciones de restauración
3. Restauración de la aplicación de Microsoft SQL Server
4. Verificación de que la aplicación de Microsoft SQL Server se ha restaurado

Revisión de las consideraciones y requisitos previos de la restauración

Verifique que los requisitos previos siguientes existen antes de realizar una restauración:

- La instancia de Microsoft SQL Server es necesaria antes de realizar una restauración de la aplicación de SQL.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones sobre la restauración:

- No se puede restaurar la base de datos a través de una instancia. La realización de una restauración en una ubicación alternativa en el Agente de Arcserve UDP para Windows significa que se puede restaurar la base de datos y cambiar su nombre y la ubicación del archivo. Para obtener más información, consulte Consideraciones de la restauración de Microsoft SQL Server en una ubicación alternativa.
- Si las tareas no son para la misma máquina virtual, Arcserve UDP permite que se ejecuten varias tareas de restauración al mismo tiempo. Si se intenta iniciar una tarea de restauración mientras hay otra tarea de restauración en ejecución para la misma máquina virtual, aparece un mensaje de alerta informando de que se está ejecutando otra tarea y solicitando al usuario que lo vuelva a intentar más tarde.
- Arcserve UDP solamente permite la ejecución de una tarea de restauración al mismo tiempo. Si se intenta iniciar una tarea de restauración manualmente mientras otra tarea de restauración está en ejecución, aparecerá un mensaje de alerta informando de que se está ejecutándose otra tarea y solicitando al usuario que lo vuelva a intentar más tarde.

Consideraciones de restauración de Microsoft SQL Server a una ubicación alternativa

Cuando se especifica la restauración de una aplicación Microsoft SQL Server a una ubicación alternativa, se puede restaurar en una ubicación alternativa en el mismo equipo o en un equipo diferente.

Antes de realizar una restauración del Agente de Arcserve UDP para Windows de una instancia de la aplicación Microsoft SQL Server en una ubicación alternativa, se debe tener en cuenta la información siguiente:

Si la ubicación alternativa se encuentra en el mismo equipo

Para esta opción, se puede restaurar una base de datos en una ubicación nueva (con el mismo nombre) o restaurar con un nuevo nombre (a la misma ubicación):

- **Mismo nombre - Ubicación nueva**

  Por ejemplo, si Base de Datos A se instala en SQL Server actual en "C:\DB_A" y si se ha realizado una copia de seguridad. Se puede utilizar esta opción y especificar "Ubicación de archivo alternativa" para restaurar Base de Datos A a una ubicación alternativa como "D:\Alternate_A.

  Después de restaurar la base de datos, el archivo de base de datos que se encuentra en la nueva ubicación "D:\Alternate_A" se volverá a utilizar.

  Importante: Durante la restauración, si se cambia la ubicación de la base de datos pero se conserva el nombre de la base de datos, la base de datos anterior se suprimirá después de finalizar la restauración. El archivo de la base de datos restaurada hará referencia a la nueva ubicación.

  Cuando se restaura a una ubicación alternativa, la sección Nombre de la instancia no está disponible debido a que el nombre de instancia debe ser siempre el mismo y no se pueden cambiar. Como resultado, no se puede restaurar una base de datos a una instancia alternativa que se encuentre actualmente en el mismo MS SQL Server.

- **Misma ubicación - Nuevo nombre**

  Por ejemplo, en el caso que tenga dos bases de datos (Base de datos A y Base de datos B) instaladas en SQL Server actual y se realice copia de seguridad de las dos. Se puede utilizar esta opción y especificar "Nuevo nombre para la base de datos" para restaurar Base de Datos A a una misma ubicación como Base de datos A_Nueva.

  Después de restaurar la base de datos, esta ubicación ahora dispondrá de tres bases de datos (Base de datos A, Base de datos B y Base de datos A_Nueva).

Si la ubicación alternativa se encuentra en un equipo distinto

- La ruta de instalación de SQL Server debe ser la misma que la ruta que existía al realizar la copia de seguridad.

  Por ejemplo, si la copia de seguridad de SQL Server está instalada en C:\SQLServer, la instancia de SQL Server que se encuentra en el nuevo servidor del Agente de Arcserve UDP para Windows se deberá instalar también en C:\SQLServer.

- Se debe instalar el mismo nombre de instancia para la base de datos que existía al realizar la copia de seguridad en el servidor del Agente de Arcserve UDP para Windows; de lo contrario, se omitirá de la restauración la base de datos

asociada a ese nombre de instancia.

Por ejemplo, se puede dar el caso de que la copia de seguridad de SQL Server contuviera "Instancia_1" con la base de datos A y la base de datos B e "Instancia_2" con la base de datos C, pero el servidor del Agente de Arcserve UDP para Windows solamente contenga "Instancia_1". Cuando la restauración sea total, Base de Datos A y Base de Datos B se restaurarán, pero Base de Datos C no se restaurará.

- La versión de SQL Server en el servidor del Agente de Arcserve UDP para Windows debe ser compatible con las versiones anteriores de SQL Server que se han utilizado durante la sesión de copia de seguridad.

  Por ejemplo, se puede restaurar un equipo SQL Server 2008 a otro SQL Server 2010. Sin embargo, el proceso contrario no es posible.

- No se puede restaurar una base de datos de una instancia de 64 bits a una instancia de 32 bits.

Consideraciones de restauración para Microsoft SQL Server 2012/2014 AAG

Cuando se restaura una base de datos de Microsoft SQL Server 2012/2014 que forma parte de un grupo de AlwaysOn Availability Group (AAG), hay que tener en cuenta algunas consideraciones.

Si la base de datos de MS SQL forma parte de MS SQL 2012/2014 AlwaysOn Availability Group (AAG) y se produce un error al restaurar en la ubicación original, realice las tareas siguientes:

1. Elimine la base de datos que se tiene que restaurar del grupo de disponibilidad. Para obtener más información, consulte el enlace.
2. Comparta la sesión de copia de seguridad del Agente de Arcserve UDP para Windows en todos los nodos de grupo de disponibilidad y después restaure la sesión del Agente de Arcserve UDP para Windows en todos los nodos de grupo de disponibilidad.
3. Vuelva a agregar la base de datos al grupo de disponibilidad. Para obtener más información, consulte el enlace.

Especificación de la información de Microsoft SQL Server para restaurar

El Agente de Arcserve UDP (Windows) no solo permite proteger y recuperar los datos, sino que también ayuda a obtener la aplicación de Microsoft SQL Server que utilizará los datos y que los ejecutará. La recuperación del servidor de Microsoft SQL sólo puede realizarse mediante el método Restaurar por punto de recuperación.

El proceso implicado en la restauración de la aplicación de Microsoft SQL Server es el siguiente:

1. Especificación del punto de recuperación y de la base de datos de Microsoft SQL Server
2. Definición de las opciones de restauración

Especificación del punto de recuperación y de la base de datos de Microsoft SQL Server

Utilice la opción **Explorar puntos de recuperación** para restaurar desde un punto de recuperación. Al seleccionar una fecha de recuperación, aparecerán todos los puntos de recuperación asociados para la fecha. Tiene la opción de explorar y seleccionar la base de datos de Microsoft SQL Server que desee restaurar.

Siga estos pasos:

1. Acceda al cuadro de diálogo Selección del método de recuperación de una de las formas siguientes:

   - Desde Arcserve UDP:

     a. Inicie sesión en Arcserve UDP.

     b. Haga clic en la ficha **recursos**.

     c. Seleccione **Todos los nodos** en el panel izquierdo.

     Se muestran todos los nodos agregados en el panel central.

     d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

     e. Haga clic en **Restaurar** en la opción desplegable del nombre del servidor.

     El cuadro de diálogo Selección del método de restauración se abre.

     Nota: Se inicia sesión automáticamente en el nodo del Agente y el cuadro de diálogo Selección del método de restauración se abre desde el nodo del Agente.

   - Desde el Agente de Arcserve UDP (Windows):

     a. Inicie sesión en el Agente de Arcserve UDP (Windows).

     b. En la página principal, seleccione **Restaurar**.

     El cuadro de diálogo Selección del método de restauración se abre.

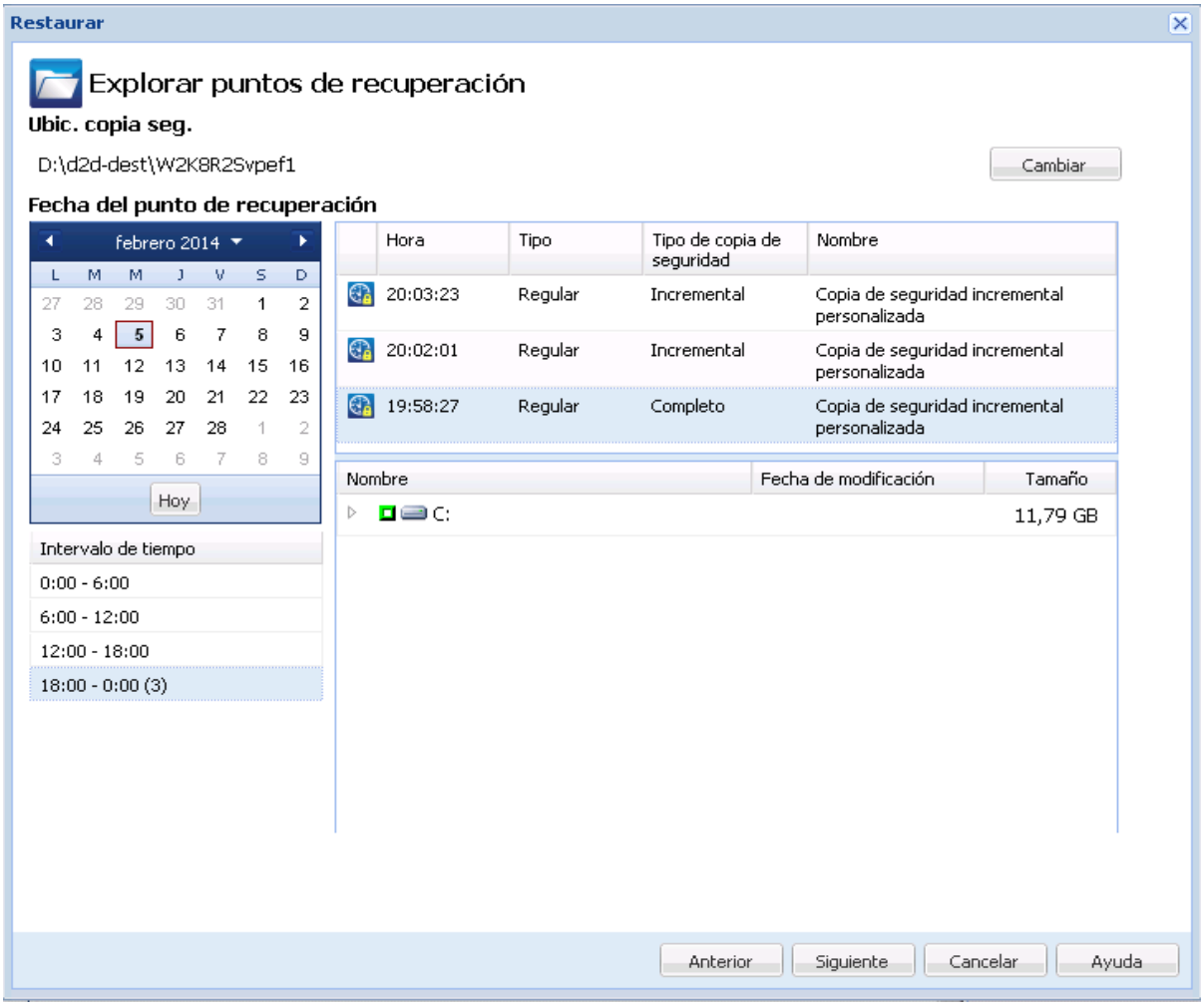
   6. Haga clic en la opción **Explorar puntos de recuperación**.

      Aparecerá el cuadro de diálogo **Explorar puntos de recuperación.**

   7. Seleccione el punto de recuperación (fecha y hora) y, a continuación, seleccione la base de datos de Microsoft SQL Server para restaurar.

   8. La casilla de marcador correspondiente aparecerá rellenada (verde) para indicar que se ha seleccionado la base de datos para restaurar.

Nota: Si no desea que los archivos de registro de transacciones se apliquen después de la restauración, debe suprimirlos manualmente antes de que se realice la restauración. Para obtener más información acerca de cómo suprimir archivos de registro de transacciones manualmente, consulte la documentación de Microsoft SQL Server.



9. Haga clic en **Siguiente**.

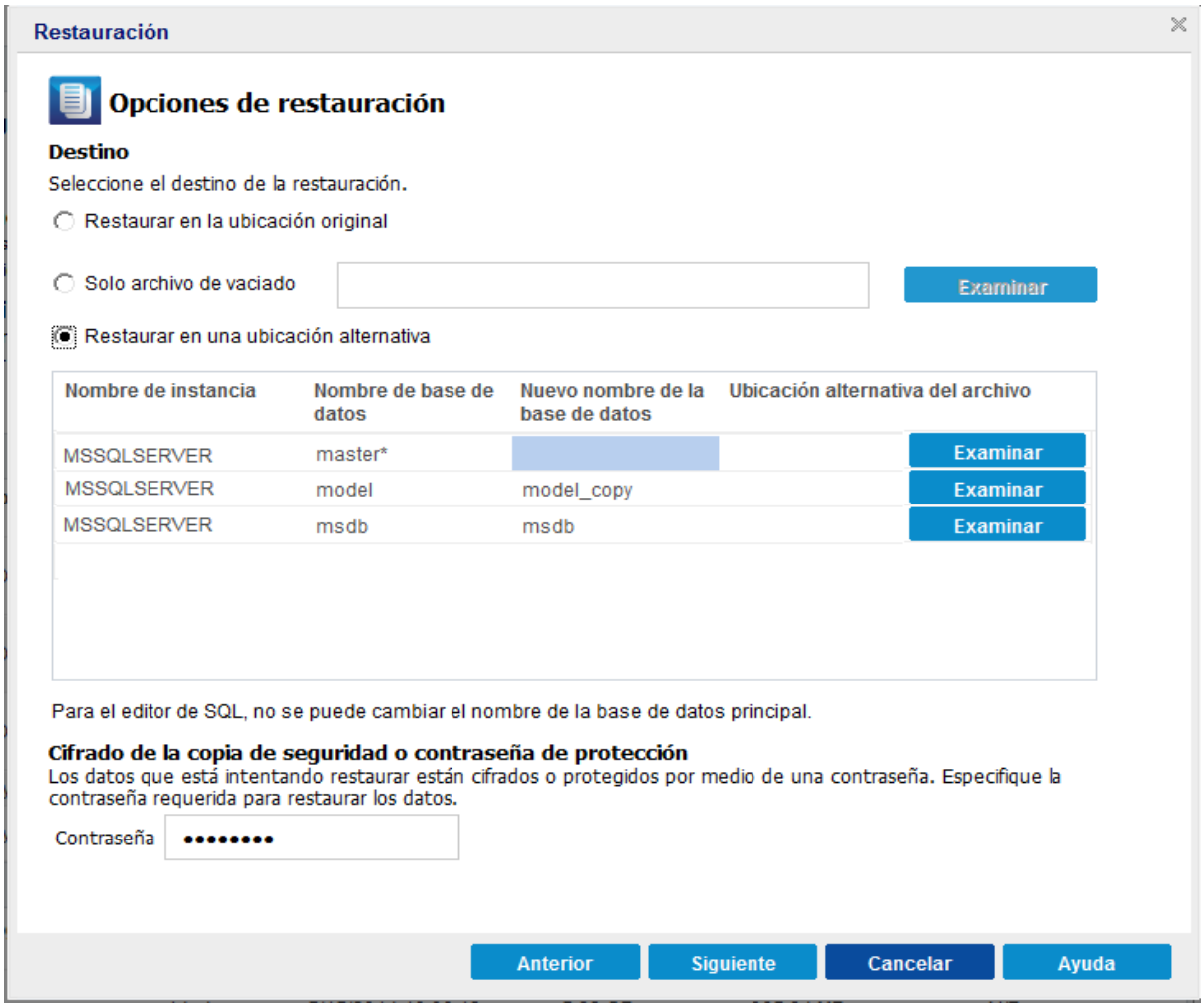
   Se abrirá el cuadro de diálogo **Opciones de restauración**.

Definición de las opciones de restauración

Después de especificar un punto de recuperación y el contenido que se deben restaurar, defina las opciones de copia para el punto de recuperación seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, seleccione el destino de la restauración.



2. Seleccione el destino de la restauración.

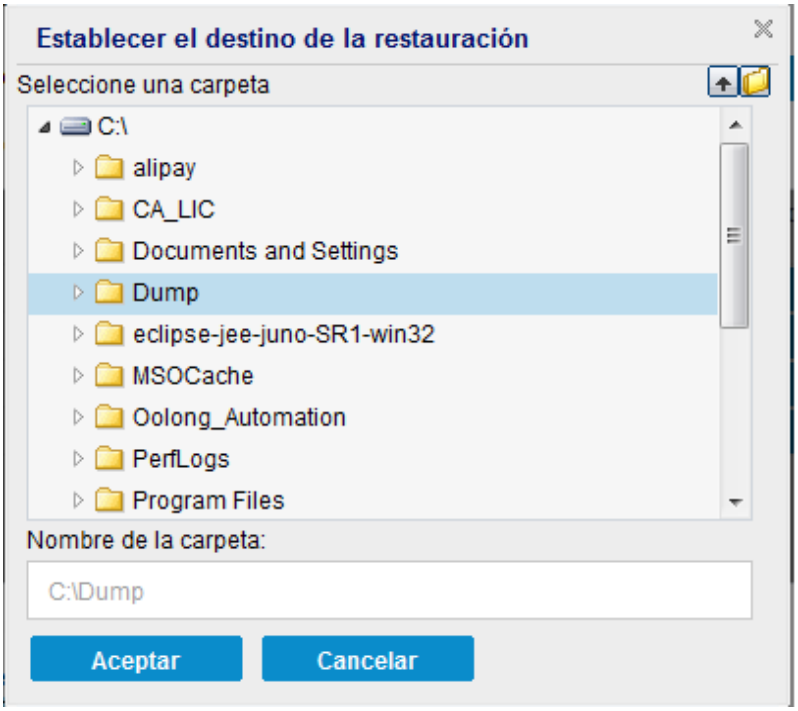
   Las opciones disponibles son la restauración en la ubicación original de la copia de seguridad, la restauración solo del archivo de vaciado o la restauración en una ubicación alternativa.

   Restauración en la ubicación original

   Restaura en la ubicación original desde la que se ha capturado la imagen de copia de seguridad.

   Solo archivo de vaciado

   Para esta opción, el Agente de Arcserve UDP (Windows) vuelca los archivos de base de datos de Microsoft SQL seleccionados a la carpeta especificada. Al seleccionar esta opción, especifique o explore la ubicación de la carpeta en la que se desea restaurar el archivo de vaciado.



   Restauración en una ubicación alternativa

   Restaura en una ubicación alternativa (no en la ubicación original).



Dado que es posible copiar las copias de seguridad en ubicaciones de red, varias instancias de SQL Server las pueden utilizar. Se puede realizar una restauración de varias bases de datos (simultáneamente) desde el nivel de instancia. Desde este listado se puede seleccionar la instancia de base de datos y especificar un nuevo nombre para la base de datos y una ubicación alternativa donde restaurar la base de datos. Además, también es posible explorar la ubicación alternativa donde restaurar la base de datos.

La restauración de una aplicación de Microsoft SQL Server a una ubicación alternativa tiene algunas limitaciones que hay que tener en cuenta. Para obtener más información, consulte la sección **Consideraciones de restauración de Microsoft SQL Server a una ubicación alternativa** en el tema Revisión de las consideraciones y requisitos previos de la restauración.

3. Haga clic en **Siguiente**.

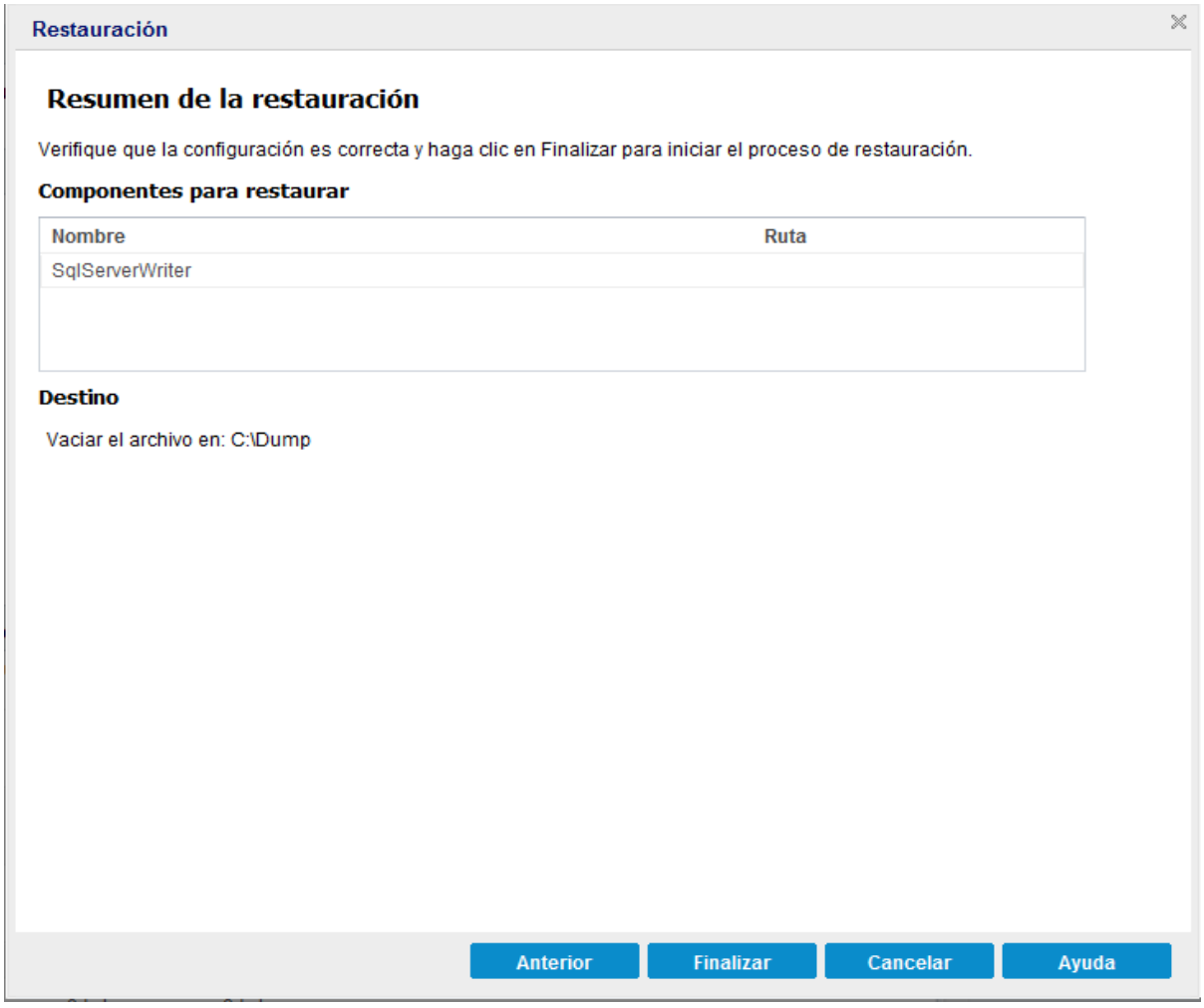
   Se abrirá el cuadro de diálogo **Resumen de la restauración**.

Restauración de la aplicación de Microsoft SQL Server

Después de definir las opciones de restauración, verifique que los valores de configuración sean correctos y confirme el proceso de restauración. El **Resumen de la restauración** le ayuda a revisar todas las opciones de la restauración definidas y a modificarlas si es necesario.

Siga estos pasos:

1. En el cuadro de diálogo **Resumen de la restauración**, revise la información que aparece en pantalla para verificar que todos los valores de configuración y las opciones de restauración sean correctos.



- Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo anterior correspondiente para cambiar la configuración incorrecta.
- Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar el proceso de restauración.

Se restaura la aplicación de Microsoft SQL Server.

Verificación de que la aplicación de Microsoft SQL Server se ha restaurado

Siga estos pasos:

1. Vaya al destino de la restauración especificado para el Agente de Arcserve UDP (Windows).

   Por ejemplo, si decide restaurar la base de datos de Microsoft SQL Server en la ubicación original, después de finalizar la restauración, busque la ubicación física para comprobar si se restauran la base de datos de Microsoft Exchange y los registros.

   Si se selecciona realizar una restauración de la base de datos de Microsoft SQL Server en un archivo de volcado como única ubicación, el Agente de Arcserve UDP (Windows) solamente restaurará la base de datos de Microsoft SQL Server y los registros en una ubicación específica.

2. Compruebe que la aplicación de Microsoft SQL Server se ha restaurado y asegúrese de que la base de datos se monta y es accesible.

   La aplicación de Microsoft SQL Server se ha restaurado correctamente.

Cómo restaurar desde una ruta UNC/NFS

Cada vez que Arcserve UDP realiza una copia de seguridad correcta de la ruta UNC/NFS, restaura todos los archivos y carpetas que han cambiado desde la última tarea de copia de seguridad correcta. Este método de restauración permite explorar los archivos y carpetas archivados y especificar exactamente qué archivo se desea restaurar.

Realice las tareas siguientes para restaurar desde un punto de recuperación:

1. Revisión de las consideraciones y requisitos previos de la restauración
2. Especificación de los archivos y directorios de una ruta UNC/NFS que se deben restaurar
    a. Especificación de los archivos y contenido que se deben restaurar
    b. Definición de las opciones de restauración
3. Restauración de los archivos y contenido
4. Verificación de que se ha restaurado el contenido

Revisión de las consideraciones y requisitos previos de la restauración

Verifique que los requisitos previos siguientes existen antes de realizar una restauración:

- Como mínimo, existe un punto de recuperación disponible para restaurar.
- Tiene un destino del punto de recuperación válido y accesible desde el que poder restaurar el contenido del punto de recuperación.
- Tiene una ubicación de destino válida y accesible a la que poder restaurar el contenido del punto de recuperación.

Especificación de la información de la ruta UNC/NFS que se debe restaurar

Arcserve UDP proporciona una opción para restaurar datos desde una ruta UNC/NFS. El objetivo de ejecutar una tarea de restauración correcta es de identificar los datos necesarios de forma rápida y de recuperarlos desde la ubicación de copia de seguridad correspondiente. Cada tarea de restauración necesita un origen y un destino.

El proceso de restauración desde una ruta UNC/NFS se muestra a continuación:

1. Especificación del contenido y de los archivos y carpetas de una ruta que se deben restaurar
2. Definición de las opciones de restauración

Especificación del contenido y de los archivos y carpetas de una ruta UNC/NFS que se deben restaurar

Esta sección proporciona información sobre cómo especificar los archivos y carpetas UNC/NFS y el contenido para restaurar.

Siga estos pasos:

1. Acceda al cuadro de diálogo Selección del método de recuperación de una de las formas siguientes:

   En la Consola de Arcserve UDP:

   a. Inicie sesión en la Consola de Arcserve UDP.

   b. Vaya a **recursos** > **Nodo** > **Todos los nodos**.

      Se muestran todos los nodos de agregados en el panel central.

   c. Haga clic con el botón secundario del ratón en el nodo y, a continuación, haga clic en **Restaurar**.

      Se inicia sesión automáticamente en la consola del nodo del agente y se abre el cuadro de diálogo Restaurar.

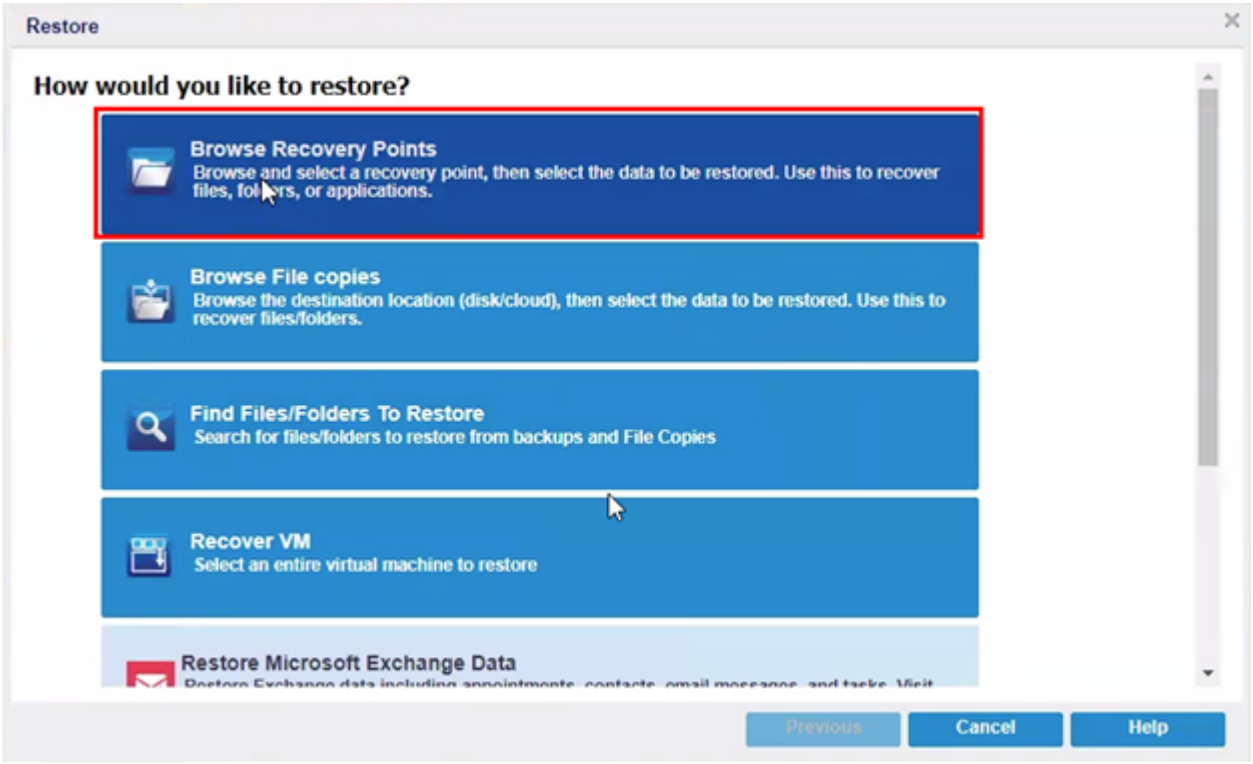
   Desde el Agente de Arcserve UDP (Windows):

   a. Inicie sesión en el Agente de Arcserve UDP (Windows).

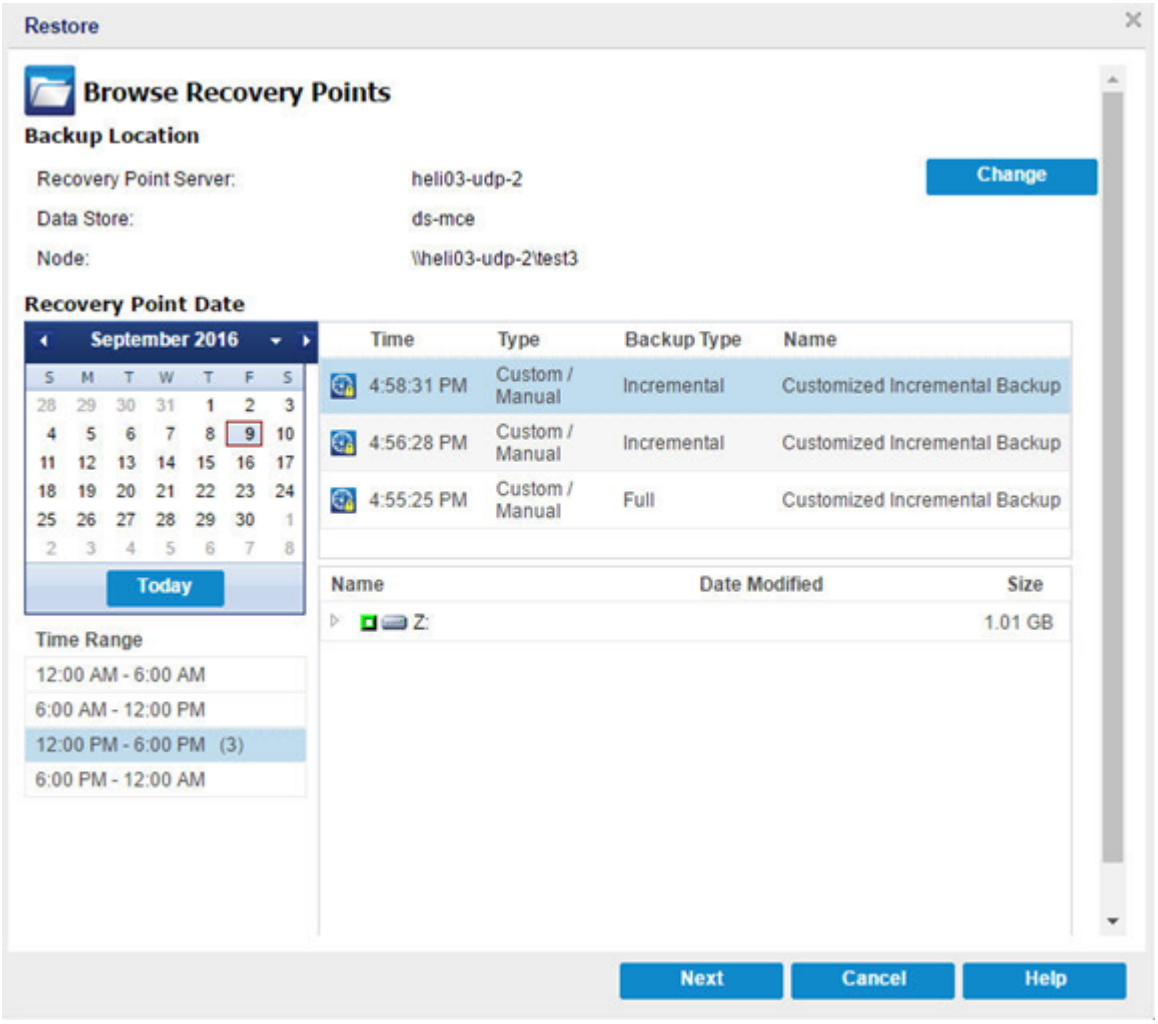
   b. En la página principal, seleccione **Restaurar**.

      Se abrirá el cuadro de diálogo Restauración.

2. En el cuadro de diálogo Restaurar haga clic en la opción **Explorar puntos de recuperación**.



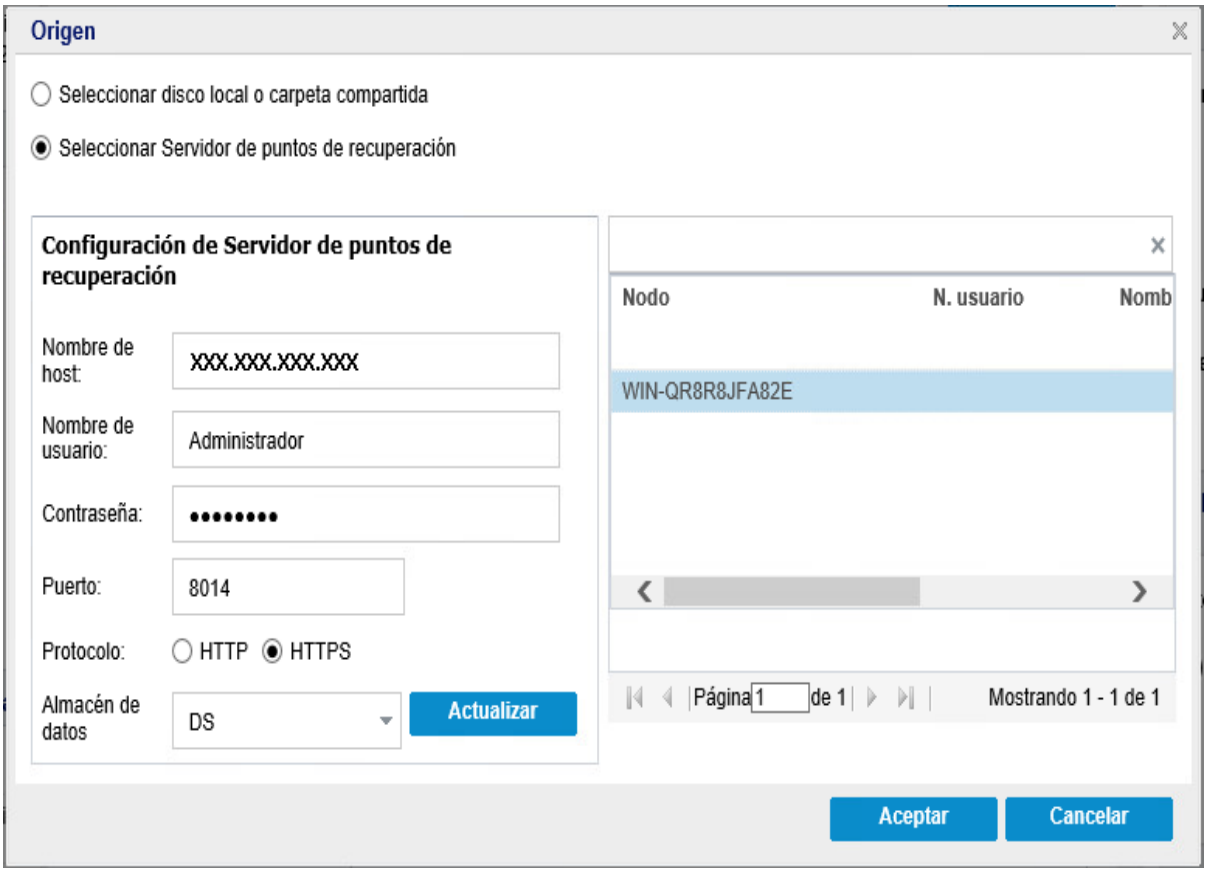
3. En la página Explorar puntos de recuperación, haga lo siguiente:



a. Para actualizar la ubicación de la copia de seguridad, haga clic en **Cambiar**.

   Se abrirá el cuadro de diálogo Origen.

b. En el cuadro de diálogo Origen, seleccione una de las siguientes ubicaciones de copia de seguridad y, a continuación, haga clic en **Aceptar**:



Seleccionar disco local o carpeta compartida

1. Especifique o vaya a la ubicación donde se almacenan las imágenes de copia de seguridad y seleccione el origen de la copia de seguridad adecuado.
2. Para verificar la conexión a la ubicación especificada, haga clic en el botón de flecha verde. Si es necesario, especifique el Nombre de usuario y la Contraseña para acceder a dicha ubicación de origen.

   El cuadro de diálogo Selección de la ubicación de la copia de seguridad se abre.
3. Seleccione la carpeta en la cual se almacenan los puntos de recuperación y, a continuación, haga clic en **Aceptar**.

   El cuadro de diálogo Selección de la ubicación de la copia de seguridad se cierra y se muestra la ubicación de la copia de seguridad en el cuadro de diálogo Origen.

   Los puntos de recuperación se clasifican en el cuadro de diálogo Examinar puntos de recuperación.

Seleccionar servidor de puntos de recuperación

1. Especifique los detalles del valor de configuración del servidor de puntos de recuperación y, a continuación, haga clic en **Actualizar**.

   Todos los agentes se muestran en la columna Agente de protección de datos en el cuadro de diálogo Origen.

2. Seleccione el agente de la lista que se muestra.

   Los puntos de recuperación se clasifican en el cuadro de diálogo Examinar puntos de recuperación.

c. Seleccione la fecha de calendario para la imagen de copia de seguridad que se desea restaurar.

   Todas las fechas que contienen puntos de recuperación para el origen de la copia de seguridad especificado se resaltan en verde.

   Aparecerán los puntos de recuperación correspondientes para la fecha, junto con la hora de la copia de seguridad, el tipo de copia de seguridad que se realiza (completa, incremental o de verificación) y el nombre de la copia de seguridad.

d. Seleccione un punto de recuperación para restaurar.

   Se muestra el contenido de la copia de seguridad (incluyendo cualquier aplicación) del punto de recuperación seleccionado.

   Nota: Si un icono de reloj aparece con el símbolo de candado, significa que el punto de recuperación contiene información cifrada y que puede requerir una contraseña para realizar la restauración.

e. Seleccione el contenido que desee restaurar.

   - Para la restauración de nivel de volumen, es posible especificar la restauración del volumen entero o de los archivos o carpetas seleccionados integrados en el volumen.
   - Para la restauración de nivel de aplicaciones, tiene la opción de especificar la restauración de la aplicación entera o de los componentes seleccionados, las bases de datos, las instancias, etcétera, integrados en la aplicación.

4. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo Opciones de restauración.

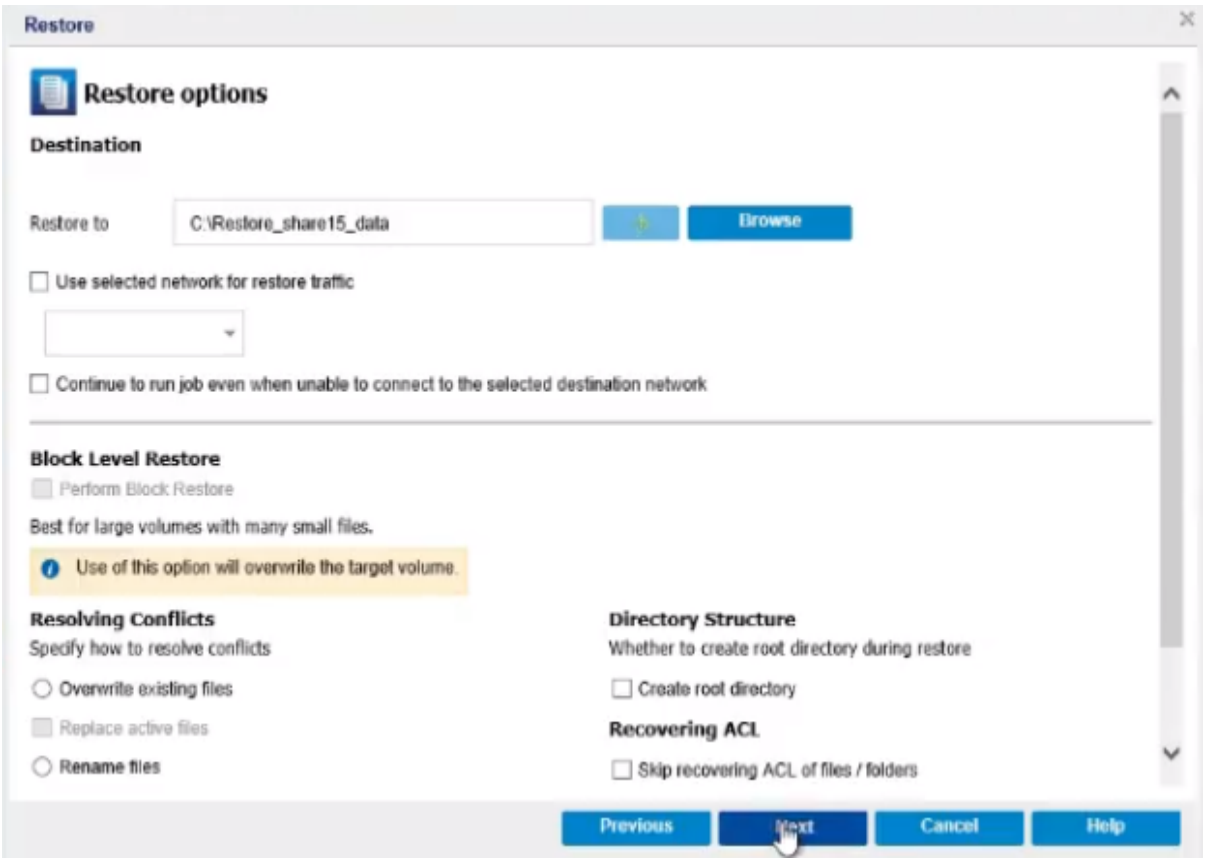
   Se especifica el punto de recuperación y el contenido que se debe restaurar.

Definición de las opciones de restauración

Después de especificar un punto de recuperación y el contenido que se deben restaurar, defina las opciones de copia para el punto de recuperación seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo Opciones de restauración, seleccione el destino para la restauración.



La opción de destino disponible es:

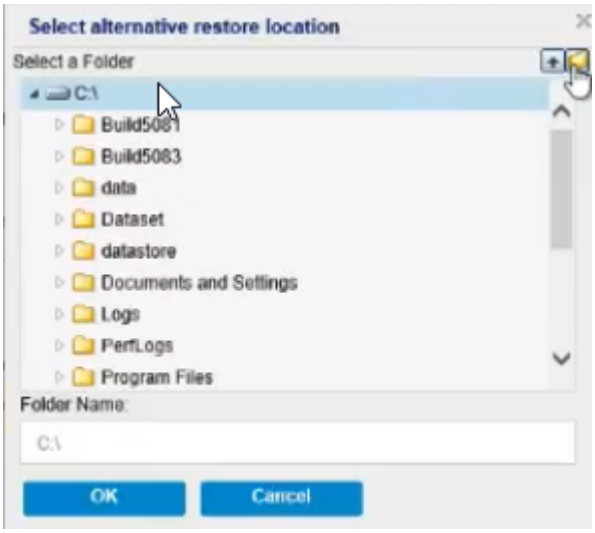
Restaurar en

Restaura en la ubicación especificada. Para restaurar datos en la ubicación especificada, realice lo siguiente:

a. Para proporcionar el destino, haga clic en **Examinar**.

   Aparecerá el cuadro de diálogo Seleccionar ubicación de restauración alternativa.

b. Seleccione la carpeta existente o cree una nueva según sea necesario y, a continuación, haga clic en **Aceptar**.



c. Para verificar la conexión a la ubicación especificada, haga clic en el botón de flecha verde. Si es necesario, especifique el Nombre de usuario y la Contraseña para obtener acceso a dicha ubicación.

Nota: No se permite la restauración en el recurso compartido de NFS desde un plan de protección de NFS.

2. Para activar la comunicación entre la red seleccionada y el servidor de puntos de recuperación, seleccione la casilla de verificación **Utilizar la red seleccionada para el tráfico de la restauración** y, a continuación, seleccione la red en la lista desplegable.

   Nota: Si no se puede acceder a la red de copia de seguridad seleccionada y para continuar la tarea de copia de seguridad con la red disponible o con la red predeterminada, haga clic en la casilla de verificación **Continuar ejecutando la tarea incluso cuando no se pueda conectar con la red de copia de seguridad seleccionada**.

3. En **Resolución de conflictos**, especifique la opción correspondiente a la acción que deberá realizar si se encuentran conflictos durante el proceso de restauración.Arcserve UDP

   A continuación se especifican las opciones disponibles:

   Sobrescribir archivos existentes

   Sobrescribe (reemplaza) todos los archivos existentes que se encuentran en el destino de restauración. Todos los objetos se restaurarán desde los archivos de copia de seguridad, independientemente de si actualmente se encuentran en el equipo.

   Reemplazar los archivos activos

Reemplaza todos los archivos activos después del reinicio. Si durante el intento de restauración, el Agente de Arcserve UDP para Windows detecta que el archivo existente está actualmente en uso o que algún usuario está accediendo al archivo, no sustituye ese archivo de forma inmediata, sino que retrasa la sustitución de los archivos activos hasta que se reinicie de nuevo el equipo con el fin de evitar problemas. (La restauración ocurrirá de forma inmediata pero los archivos activos se sustituirán a partir del reinicio siguiente).

Esta opción solamente está disponible si selecciona la opción **Sobrescribir archivos existentes**.

Nota: Si no se selecciona esta opción, se omite de la restauración cualquier archivo activo.

Cambiar el nombre de los archivos

Si el nombre de archivo ya existe, crea un archivo nuevo. Al seleccionar esta opción se copiará el archivo de origen en el destino con el mismo nombre de archivo pero con una extensión diferente. A continuación, los datos se restaurarán en un archivo nuevo.

Omitir archivos existentes

Omite y no sobrescribe (reemplaza) ningún archivo existente que se encuentre en el destino de restauración. Solo se restaurarán desde los archivos de copia de seguridad los objetos que no estén en el equipo actualmente.

Valor por omisión: Omitir archivos existentes

4. Para crear un directorio raíz durante la restauración, especifique la **Estructura de directorios**.

Crear directorio raíz

Especifica que si una estructura de directorio raíz existe en la imagen de copia de seguridad capturada, Arcserve UDP recreará la misma estructura de directorio raíz en la ruta de destino de la restauración.

Si no se selecciona esta opción, el archivo o carpeta se restaurará directamente en la carpeta de destino.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt" y "C:\Folder1\SubFolder2\B.txt" y durante la restauración ha especificado como destino de la restauración "D:\Restore".

- Si ha seleccionado la restauración de los archivos "A.txt" y "B.txt" de manera individual, el destino de los archivos restaurados será "D:\Restore\A.txt" y "D:\Restore\B.txt" (no se recreará el directorio raíz anterior en el nivel de archivo especificado).

- Si se selecciona la restauración desde el nivel "Subcarpeta2", el destino para los archivos restaurados será "D:\Restore\SubFolder2\A.txt" y "D:\Restore\SubFolder2\B.txt" (el directorio raíz superior al nivel de carpeta especificada no se recreará).

Con esta opción seleccionada, la ruta completa de directorio raíz para los archivos/carpetas (incluyendo el nombre de volumen) se recrea en la carpeta de destino. Si los archivos o carpetas que deben restaurarse provienen del mismo nombre de volumen, la ruta del directorio raíz de destino no incluirá el nombre del volumen. Sin embargo, si los archivos o carpetas que deben restaurarse provienen de diferentes nombres de volúmenes, la ruta del directorio raíz de destino incluirá el nombre de volumen.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", y también E:\Folder3\SubFolder4\C.txt", y durante la restauración ha especificado el destino de restauración como "D:\Restore".

- Si ha seleccionado la restauración únicamente del archivo "A.txt", el destino para el archivo restaurado será "D:\Restore\Folder1\SubFolder2\A.txt" (se recreará todo el directorio raíz sin el nombre de volumen).
- Si ha seleccionado la restauración tanto del archivo "A.txt" como del archivo "C.txt", el destino para los archivos restaurados será "D:\Restore\C\ Folder1\SubFolder2\A.txt" y "D:\Restore\ E\Folder3\SubFolder4\C.txt" (se recreará todo el directorio raíz con el nombre de volumen).

5. Especifique si se desea que la recuperación de la lista de control de acceso omita la recuperación de la lista de control de acceso de los archivos y carpetas.

   Si la opción **Omitir recuperación de la lista de control de acceso de archivos y carpetas** está seleccionada, solo se restaurarán los archivos y carpetas de origen. El atributo de los archivos y carpetas no se restaura, por lo que todos los usuarios pueden tener acceso.

   Valor predeterminado: Se restauran los archivos y carpetas de origen con el atributo - Lista de control de acceso.

6. Si es necesario, especifique la **Contraseña de cifrado de la copia de seguridad**, cuando los datos que se están intentando restaurar están cifrados.

   Si se intenta realizar una restauración desde el mismo equipo del Agente de Arcserve UDP para Windows desde el que se ha realizado la copia de seguridad cifrada, no es necesario proporcionar ninguna contraseña. Sin embargo, sí será necesaria una contraseña si se intenta realizar la restauración desde otro equipo del Agente de Arcserve UDP para Windows.

Nota: Si un icono de reloj aparece con el símbolo de candado, significa que el punto de recuperación contiene información cifrada y que puede requerir una contraseña para realizar la restauración.

7. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo Resumen de la restauración.

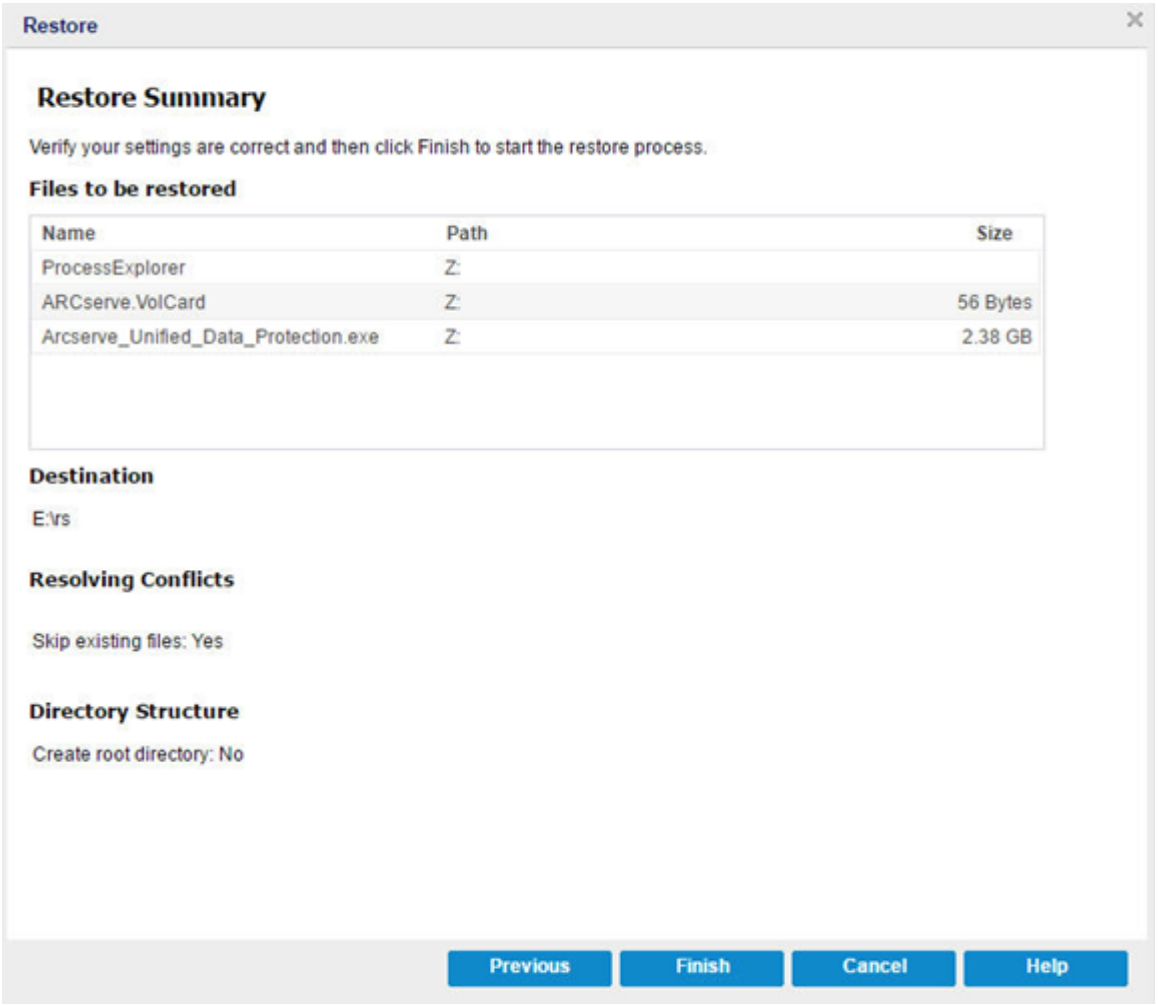
   Las opciones de restauración se han definido para restaurar desde un punto de recuperación.

Restauración de los archivos o carpetas y el contenido que se encuentra en la ruta UNC/NFS

Después de definir las opciones de restauración, verifique que los valores de configuración sean correctos y confirme el proceso de restauración. La página Resumen de la restauración le ayuda a revisar todas las opciones de la restauración definidas y a modificarlas si es necesario.

Siga estos pasos:

1. En el cuadro de diálogo Resumen de la restauración, revise la información que aparece en pantalla para verificar que todas las opciones de restauración y los valores de configuración sean correctos.



2. Realice uno de los procedimientos siguientes:

   - Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para cambiar el valor de configuración

incorrecto.

- Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar el proceso de restauración.

El contenido del punto de recuperación se restaura.

Verificación de que se ha restaurado el contenido

Después de la finalización de la tarea de restauración, verifique que todos los archivos se restauren en el nodo de destino. Compruebe el **Historial de tareas** y las fichas **Registro de actividad** en el panel Estado para controlar el progreso del proceso de restauración.

Siga estos pasos:

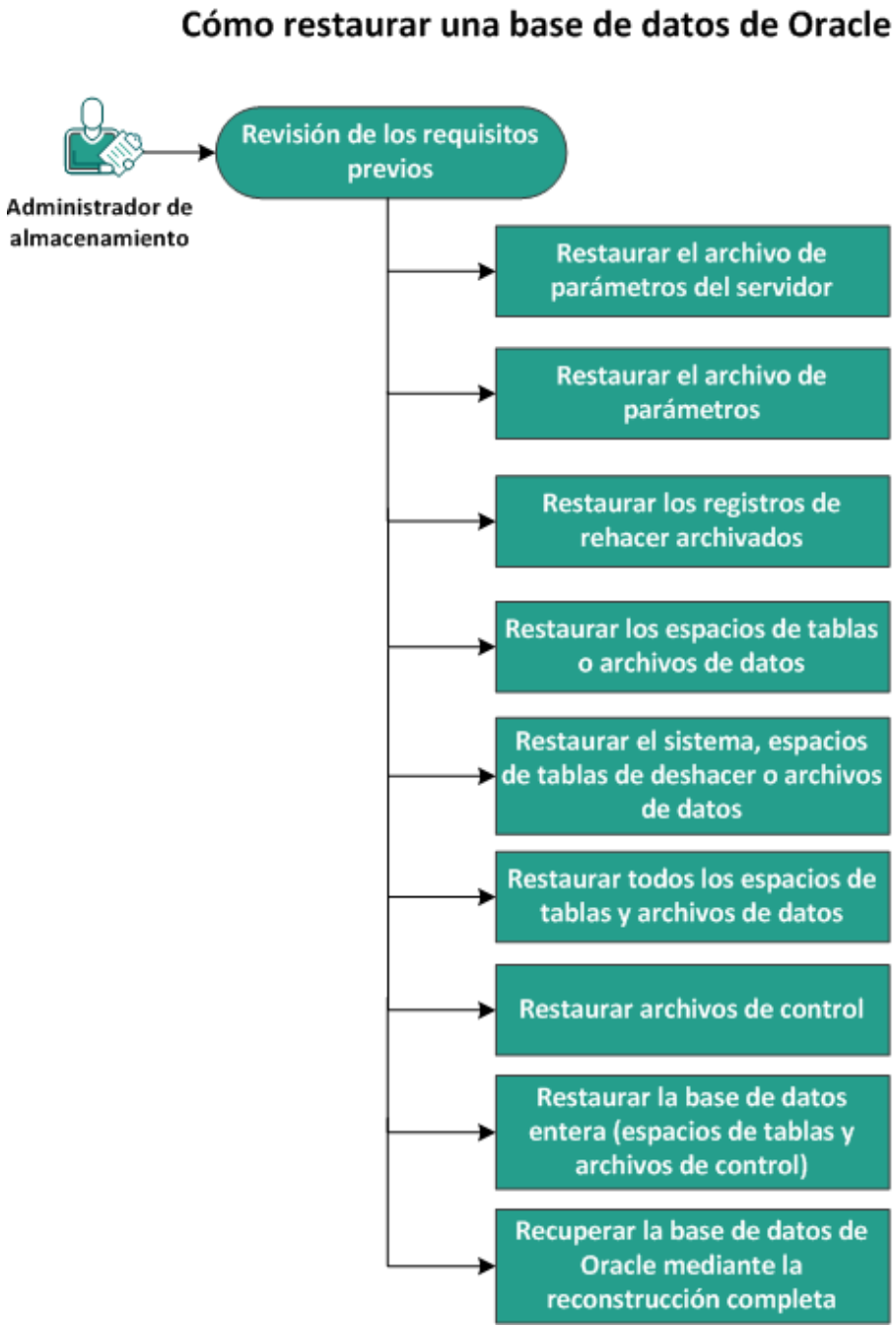
1. Vaya al equipo de destino en el que se han restaurado los datos.
2. Compruebe que los datos obligatorios del punto de recuperación se hayan restaurado.

   El contenido restaurado se ha verificado correctamente.

Cómo restaurar una base de datos de Oracle

Mediante el asistente de restauración se pueden restaurar bien algunos archivos y espacios de tablas o la base de datos Oracle entera. Para restaurar una base de datos de Oracle, busque los archivos o espacios de tablas en el nodo de destino. A continuación, restaure los archivos o espacios de tablas mediante el asistente de restauración.

El diagrama siguiente ilustra el proceso de restauración de la base de datos de Oracle:



Realice las tareas siguientes para restaurar una base de datos de Oracle:

- Revisión de los requisitos previos
- Restauración del archivo de parámetros del servidor
- Restauración del archivo de parámetros
- Restauración de los registros de rehacer archivados
- Restauración de los espacios de tablas o archivos de datos
- Restauración del sistema, espacios de tablas de deshacer o archivos de datos
- Restauración de todos los espacios de tablas y archivos de datos
- Restauración de archivos de control
- Restauración de la base de datos entera (espacios de tablas y archivos de control)
- Recuperación de la base de datos de Oracle mediante la reconstrucción completa

Revisión de las consideraciones y requisitos previos

Revise los requisitos previos siguientes antes de restaurar la base de datos de Oracle:

- El editor de Oracle VSS en el nodo de copia de seguridad funciona correctamente. Si el editor de Oracle VSS no funciona correctamente, aparecerá un mensaje de advertencia en el registro de actividades asociado con la tarea de copia de seguridad.
- Tiene un punto de recuperación válido.
- Para evitar cualquier error en la restauración, se ha guardado una copia duplicada de los archivos del sistema antes de sobrescribir los archivos originales.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Restauración del archivo de parámetros del servidor

El archivo de parámetros del servidor es un repositorio para los parámetros de inicialización. Antes de la restauración, se debe encontrar el archivo. Cuando se han localizado los archivos, asegúrese de que la base de datos está en el estado Abierto.

Siga estos pasos:

1. Inicie sesión en el equipo donde desee restaurar los archivos.
2. Abra el archivo de parámetros del servidor mediante el siguiente comando:

   SQL> SHOW PARAMETER SPFILE;
3. Cierre la base de datos o la instancia de Oracle antes de iniciar el proceso de restauración:

   SQL> SHUTDOWN IMMEDIATE;
4. Inicie sesión en la Consola de Arcserve UDP.
5. Restaure el archivo de parámetros del servidor mediante el Asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo restaurar desde un punto de recuperación.
6. Inicie sesión en el equipo de destino.
7. Vaya a las carpetas específicas y compruebe que los archivos se han restaurado.
8. Conéctese a SQL*Plus para reiniciar la instancia de Oracle con el archivo de parámetros del servidor restaurado.

   El archivo de parámetros del servidor se ha restaurado.

Restauración del archivo de parámetros

El archivo de parámetros incluye una lista de los parámetros de inicialización y los valores para cada uno de los parámetros. Antes de la restauración, se debe encontrar el archivo. Cuando se han localizado los archivos, asegúrese de que la base de datos está en el estado Abierto.

Siga estos pasos:

1. Inicie sesión en el equipo donde desee restaurar los archivos.
2. Busque el archivo de parámetros (pfile).

   Normalmente, pfile (INIT<SID>.ORA) se encuentra en el directorio %ORACLE_HOME/database. Se puede escribir "INIT<SID>.ORA" para localizar el archivo pfile.
3. Cierre la base de datos o la instancia de Oracle antes de iniciar el proceso de restauración:

   SQL> SHUTDOWN IMMEDIATE;
4. Inicie sesión en la Consola de Arcserve UDP.
5. Restaure el archivo de parámetros mediante el Asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo restaurar desde un punto de recuperación.
6. Inicie sesión en el equipo de destino.
7. Vaya a las carpetas específicas y compruebe que los archivos se han restaurado.
8. Conéctese a SQL*Plus para reiniciar la instancia de Oracle con el archivo de parámetros restaurado.

   El archivo de parámetros se ha restaurado.

Restauración de los registros de rehacer archivados

Los registros de rehacer archivados se utilizan para recuperar una base de datos o actualizar una base de datos en espera. Antes de la restauración, se debe encontrar el archivo. Cuando se han localizado los archivos, asegúrese de que la base de datos está en el estado Abierto.

Siga estos pasos:

1. Inicie sesión en el equipo donde desee restaurar los archivos.
2. Localice los registros de rehacer archivados mediante el comando siguiente.

   SQL> ARCHIVE LOG LIST;

   SQL> SHOW PARAMETER DB_RECOVERY_FILE_DEST;
3. Inicie sesión en la Consola de Arcserve UDP.
4. Restaure los registros de rehacer archivados mediante el Asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo restaurar desde un punto de recuperación.
5. Inicie sesión en el equipo de destino.
6. Vaya a las carpetas específicas y compruebe que los registros de rehacer archivados se han restaurado.

   Los registros de rehacer archivados se han restaurado.

Restauración de los espacios de tablas o archivos de datos

Se puede restaurar el espacio de tablas o los archivos de datos. Antes de la restauración, se debe encontrar el archivo. Cuando se han localizado los archivos, asegúrese de que la base de datos está en el estado Abierto. Si la base de datos está abierta, utilice ALTER TABLESPACE. El comando OFFLINE establece los espacios de tablas o los archivos de datos fuera de conexión antes de iniciar el proceso de restauración.

Siga estos pasos:

1. Inicie sesión en el equipo en que desee restaurar los espacios de tablas o los archivos de datos.
2. Localice los espacios de tablas o los archivos de datos del usuario mediante el comando siguiente:

   SQL> SELECT FILE_NAME, TABLESPACE_NAME FROM DBA_DATA_FILES;
3. Cambie el estado de la base de datos a mount o nomount, o apáguela antes de restaurar los espacios de tablas o los archivos de datos.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Inicie sesión en la Consola de Arcserve UDP.
5. Restaure los espacios de tablas o los archivos de datos mediante el Asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo restaurar desde un punto de recuperación.
6. Inicie sesión en el equipo de destino.
7. Vaya a las carpetas específicas y compruebe que se han restaurado los espacios de tablas o los archivos de datos.
8. Recupere el espacio de tablas o los archivos de datos.
   - Para recuperar un espacio de tablas, introduzca el comando siguiente en el símbolo del sistema SQL*Plus:

     SQL> RECOVER TABLESPACE "tablespace_name";
   - Para recuperar un archivo de datos, introduzca el comando siguiente en el símbolo del sistema SQL*Plus:

     SQL> RECOVER DATAFILE 'path';

Oracle busca los archivos de registro de rehacer de archivado que debe aplicar y muestra los nombres de los archivos en una secuencia.

9. Introduzca AUTO en el símbolo del sistema SQL*Plus para aplicar los archivos.

   Oracle aplicará los archivos de registro para restaurar los archivos de datos. Una vez que Oracle termine de aplicar el archivo de registro de rehacer, aparecerán los siguientes mensajes:

   Applying suggested logfile

   Log applied

   Una vez aplicado cada registro, Oracle continuará aplicando el siguiente archivo de registro de rehacer hasta que se complete la recuperación.

10. Introduzca el comando siguiente para establecer el espacio de tablas en línea:

    SQL> ALTER TABLESPACE "tablespace_name" ONLINE;

    El espacio de tabla se recuperará ahora en el archivo de registro más reciente disponible.

Restauración del sistema o acción de deshacer espacios de tablas o archivos de datos

Se puede restaurar un sistema o deshacer espacios de tablas o archivos de datos. Antes de la restauración, se debe encontrar el archivo. Cuando se han localizado los archivos, asegúrese de que la base de datos está en el estado Abierto.

Siga estos pasos:

1. Inicie sesión en el equipo en el que desee restaurar el sistema o deshacer espacios de tablas o archivos de datos.
2. Localice los espacios de tablas o los archivos de datos del usuario mediante el comando siguiente:

   SQL> SELECT TABLESPACE_NAME, FILE_NAME FROM DBA_DATA_FILES;
3. Cambie el estado de la base de datos a mount o nomount, o apáguela antes de restaurar los espacios de tablas o los archivos de datos.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Inicie sesión en la Consola de Arcserve UDP.
5. Restaure los espacios de tablas o los archivos de datos mediante el Asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo restaurar desde un punto de recuperación.
6. Inicie sesión en el equipo de destino.
7. Vaya a las carpetas específicas y compruebe que se han restaurado los archivos de datos o los espacios de tablas de rehacer.
8. Recupere el espacio de tablas o los archivos de datos.
   - Para recuperar un espacio de tablas, introduzca el comando siguiente en el símbolo del sistema SQL*Plus:

     SQL> RECOVER TABLESPACE "tablespace_name";
   - Para recuperar un archivo de datos, introduzca el comando siguiente en el símbolo del sistema SQL*Plus:

     SQL> RECOVER DATAFILE 'path';

   Oracle busca los archivos de registro de rehacer de archivado que debe aplicar y muestra los nombres de los archivos en una secuencia.
9. Introduzca AUTO en el símbolo del sistema SQL*Plus para aplicar los archivos.

Oracle aplicará los archivos de registro para restaurar los archivos de datos. Una vez que Oracle termine de aplicar el archivo de registro de rehacer, aparecerán los siguientes mensajes:

Applying suggested logfile

Log applied

Una vez aplicado cada registro, Oracle continuará aplicando el siguiente archivo de registro de rehacer hasta que se complete la recuperación.

10. Introduzca el comando siguiente para establecer el espacio de tablas en línea:

    SQL> ALTER TABLESPACE "tablespace_name" ONLINE;

    El espacio de tabla se recuperará ahora en el archivo de registro más reciente disponible.

Restauración de todos los espacios de tablas y archivos de datos

Se pueden restaurar todos los espacios de tablas y archivos de datos. Antes de la restauración, se debe encontrar el archivo. Cuando se han localizado los archivos, asegúrese de que la base de datos está en el estado Abierto. Si la base de datos está abierta, utilice ALTER TABLESPACE. El comando OFFLINE establece los espacios de tablas o los archivos de datos fuera de conexión antes de iniciar el proceso de restauración.

Siga estos pasos:

1. Inicie sesión en el equipo en que desee restaurar los espacios de tablas o los archivos de datos.
2. Localice los espacios de tablas o los archivos de datos del usuario mediante el comando siguiente:

   SQL> SELECT FILE_NAME, TABLESPACE_NAME FROM DBA_DATA_FILES;
3. Cambie el estado de la base de datos a mount o nomount, o apáguela antes de restaurar los espacios de tablas o los archivos de datos.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Inicie sesión en la Consola de Arcserve UDP.
5. Restaure los espacios de tablas o los archivos de datos mediante el Asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo restaurar desde un punto de recuperación.
6. Inicie sesión en el equipo de destino.
7. Vaya a las carpetas específicas y compruebe que se han restaurado los espacios de tablas o los archivos de datos.
8. Recupere la base de datos.

   SQL> RECOVER DATABASE;

   Oracle busca los archivos de registro de rehacer de archivado que debe aplicar y muestra los nombres de los archivos en una secuencia.
9. Introduzca AUTO en el símbolo del sistema SQL*Plus para aplicar los archivos.

Oracle aplicará los archivos de registro para restaurar los archivos de datos. Una vez que Oracle termine de aplicar el archivo de registro de rehacer, aparecerán los siguientes mensajes:

Applying suggested logfile

Log applied

Una vez aplicado cada registro, Oracle continuará aplicando el siguiente archivo de registro de rehacer hasta que se complete la recuperación.

Nota: Si Oracle muestra un mensaje de error indicando que no se puede abrir el archivo de registro, es posible que el archivo de registro no esté disponible. En tales casos, realice la recuperación de medios incompleta para recuperar la base de datos de nuevo. Cuando se hayan aplicado todos los archivos de registro, la recuperación de la base de datos habrá finalizado. Para obtener más información sobre la recuperación de medios incompleta, consulte la documentación de Oracle.

10. Introduzca el comando siguiente para establecer la base de datos en línea:

    SQL> ALTER DATABASE OPEN;

    El espacio de tabla se recuperará ahora en el archivo de registro más reciente disponible.

    Nota: Si se realiza una recuperación de medios incompleta, introduzca el comando siguiente para cambiar la base de datos al estado Abierto:

    SQL> ALTER DATABASE OPEN RESETLOGS;

Restauración de archivos de control

Se pueden restaurar los archivos de control que almacena la estructura física de la base de datos. Antes de la restauración, se debe encontrar el archivo. Cuando se han localizado los archivos, asegúrese de que la base de datos está en el estado Abierto.

Siga estos pasos:

1. Inicie sesión en el equipo donde desee restaurar los archivos de control.
2. Localice los archivos de control mediante el comando siguiente:

   SQL> SHOW PARAMETER CONTROL FILES;
3. Cambie el estado de la base de datos a nomount o apáguela antes de restaurar los archivos de control.

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Inicie sesión en la Consola de Arcserve UDP.
5. Restaure el archivo de control mediante el Asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo restaurar desde un punto de recuperación.
6. Inicie sesión en el equipo de destino.
7. Vaya a las carpetas específicas y compruebe que los archivos de control se han restaurado.
8. Monte la base de datos para empezar la recuperación de la base de datos:

   SQL> STARTUP MOUNT
9. Introduzca el comando RECOVER con la cláusula USING BACKUP CONTROLFILE.

   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE

   El proceso de recuperación de la base de datos empieza.
10. (Opcional) Especifique la cláusula UNTIL CANCEL para realizar una recuperación incompleta.

    SQL> RECOVER DATABASE USING BACKUP CONTROLFILE UNTIL CANCEL
11. Aplique los registros archivados solicitados.

    Nota: Si falta el registro archivado obligatorio, esto implica que un registro de rehacer necesario se encuentra en los registros de rehacer en línea. Esto ocurre porque se encuentran cambios no archivados en los registros en línea cuando se produce un error en la instancia. Se puede especificar la ruta completa de un archivo de

registro de rehacer en línea. A continuación, pulse Intro (es posible que tenga que intentar realizar este proceso unas cuantas veces hasta localizar el registro correcto).

12. Introduzca el comando siguiente para devolver la información del archivo de control sobre el registro de rehacer de una base de datos:

    SQL>SELECT * FROM V$LOG;

13. (Opcional) Introduzca el comando siguiente para ver los nombres de todos los miembros de un grupo:

    SQL>SELECT * FROM V$LOGFILE;

    Ejemplo: Después de aplicar los registros archivados solicitados, podrá ver los mensajes siguientes:

    ORA-00279: change 55636 generated at 24/06/2014 16:59:47 needed for thread 1

    ORA-00289: suggestion e:\app\Administrator\flash_recovery_area\orcl\ARCHIVELOG\2014_06_24\ O1_MF_1_2_9TKXGGG2_.ARC

    ORA-00280: change 55636 for thread 1 is in sequence #24

    Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

14. Especifique la ruta completa del archivo de registro de rehacer en línea y pulse Intro.

    Ejemplo: E:\app\Administrator\oradata\orcl\redo01.log

    Nota: Se debe especificar la ruta completa varias veces hasta obtener el registro correcto.

    Se muestran los siguientes mensajes:

    Log applied

    Recuperación de medios completa

15. Abra la base de datos con la cláusula RESETLOGS después de finalizar el proceso de recuperación.

    SQL> ALTER DATABASE OPEN RESETLOGS;

    Los archivos de control perdidos se recuperan.

Restauración de la base de datos entera (espacios de tablas y archivos de control)

Se puede restaurar toda la base de datos entera (todos los espacios de tablas y los archivos de control). Antes de la restauración, se debe encontrar el archivo. Cuando se han localizado los archivos, asegúrese de que la base de datos está en el estado Abierto. Si la base de datos está abierta, utilice ALTER TABLESPACE. El comando OFFLINE establece los espacios de tablas o los archivos de datos fuera de conexión antes de iniciar el proceso de restauración.

Siga estos pasos:

1. Inicie sesión en el equipo en que desee restaurar los espacios de tablas o los archivos de datos.
2. Localice los espacios de tablas o los archivos de datos del usuario mediante el comando siguiente:

   SQL> SELECT TABLESPACE_NAME, FILE_NAME from DBA_DATA_FILES;

   SQL> SHOW PARAMETER CONTROL FILES;
3. Cambie el estado de la base de datos a nomount o apáguela antes de restaurar los espacios de tablas o los archivos de datos.

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Inicie sesión en la Consola de Arcserve UDP.
5. Restaure los espacios de tablas o los archivos de datos mediante el Asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo restaurar desde un punto de recuperación.
6. Inicie sesión en el equipo de destino.
7. Vaya a las carpetas específicas y compruebe que se han restaurado los espacios de tablas o los archivos de datos.
8. Recupere la base de datos.

   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE UNTIL CANCEL;
9. Aplique los registros archivados solicitados.

   Nota: Si falta el registro archivado obligatorio, esto implica que un registro de rehacer necesario se encuentra en los registros de rehacer en línea. Esto ocurre porque se encuentran cambios no archivados en los registros en línea cuando se produce un error en la instancia. Se puede especificar la ruta completa de un archivo de registro de rehacer en línea. A continuación, pulse Intro (es posible que tenga que

intentar realizar este proceso unas cuantas veces hasta localizar el registro correcto).

10. Introduzca el comando siguiente para devolver la información del archivo de control sobre el registro de rehacer de una base de datos:

    SQL>SELECT * FROM V$LOG;

11. (Opcional) Introduzca el comando siguiente para ver los nombres de todos los miembros de un grupo:

    SQL>SELECT * FROM V$LOGFILE;

    Ejemplo: Después de aplicar los registros archivados solicitados, podrá ver los mensajes siguientes:

    ORA-00279: change 55636 generated at 24/06/2014 16:59:47 needed for thread 1

    ORA-00289: suggestion e:\app\Administrator\flash_recovery_area\orcl\ARCHIVELOG\2014_06_24\ O1_MF_1_2_9TKXGGG2_.ARC

    ORA-00280: change 55636 for thread 1 is in sequence #24

    Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

12. Especifique la ruta completa del archivo de registro de rehacer en línea y pulse Intro.

    Ejemplo: E:\app\Administrator\oradata\orcl\redo01.log

    Nota: Se debe especificar la ruta completa varias veces hasta obtener el registro correcto.

    Se muestran los siguientes mensajes:

    Log applied

    Recuperación de medios completa

13. Abra la base de datos con la cláusula RESETLOGS después de finalizar el proceso de recuperación.

    SQL> ALTER DATABASE OPEN RESETLOGS;

    Nota: Para las bases de datos multicliente (CDB/PDB), también se deben abrir todas las bases de datos conectables.

    SQL> ALTER PLUGGABLE DATABASE <NOMBRE_PDB> OPEN;

    Se restaura la base de datos entera.

14. Reinicie el servidor de Oracle después de realizar los pasos 1 al 13 para las bases de datos multicliente.

    Nota: Este paso no es necesario para el servidor que solo ejecuta bases de datos independientes.

Recuperación de la base de datos de Oracle mediante la reconstrucción completa

La reconstrucción completa permite recuperar y reconstruir el sistema informático entero durante un desastre. Se puede restaurar el equipo original o se puede restaurar otro equipo.

Siga estos pasos:

1. Restaure el equipo mediante uno de los métodos siguientes:
   - Si los puntos de recuperación proceden de una copia de seguridad del agente, realice una reconstrucción completa para restaurar el equipo.
   - Si los puntos de recuperación proceden de una copia de seguridad sin agente basada en el host, utilice Recuperar máquina virtual para restaurar el equipo.
2. Inicie sesión en el equipo restaurado.
3. Abra el símbolo del sistema y conéctese a la instancia de Oracle (por ejemplo ORCL) como sysdba.
4. Verifique el estado de la instancia de Oracle.

   SQL> SELECT STATUS FROM V$INSTANCE;
5. Realice uno de los pasos siguientes en función del estado de la instancia de Oracle:
   - Si el estado es Cierre, inicie y abra la instancia.

     SQL> STARTUP;

     SQL> ALTER DATABASE OPEN;
   - Si el estado es Nomount, monte y abra la instancia.

     SQL> ALTER DATABASE MOUNT;

     SQL> ALTER DATABASE OPEN;
   - Si el estado es Mount, abra la instancia de Oracle.

     SQL> ALTER DATABASE OPEN;
6. Recuperación mediante la ejecución del comando RECOVER si la base de datos necesita una recuperación de medios

   SQL> RECOVER DATABASE;
7. Abra la instancia de Oracle después de haber completado la recuperación de medios.

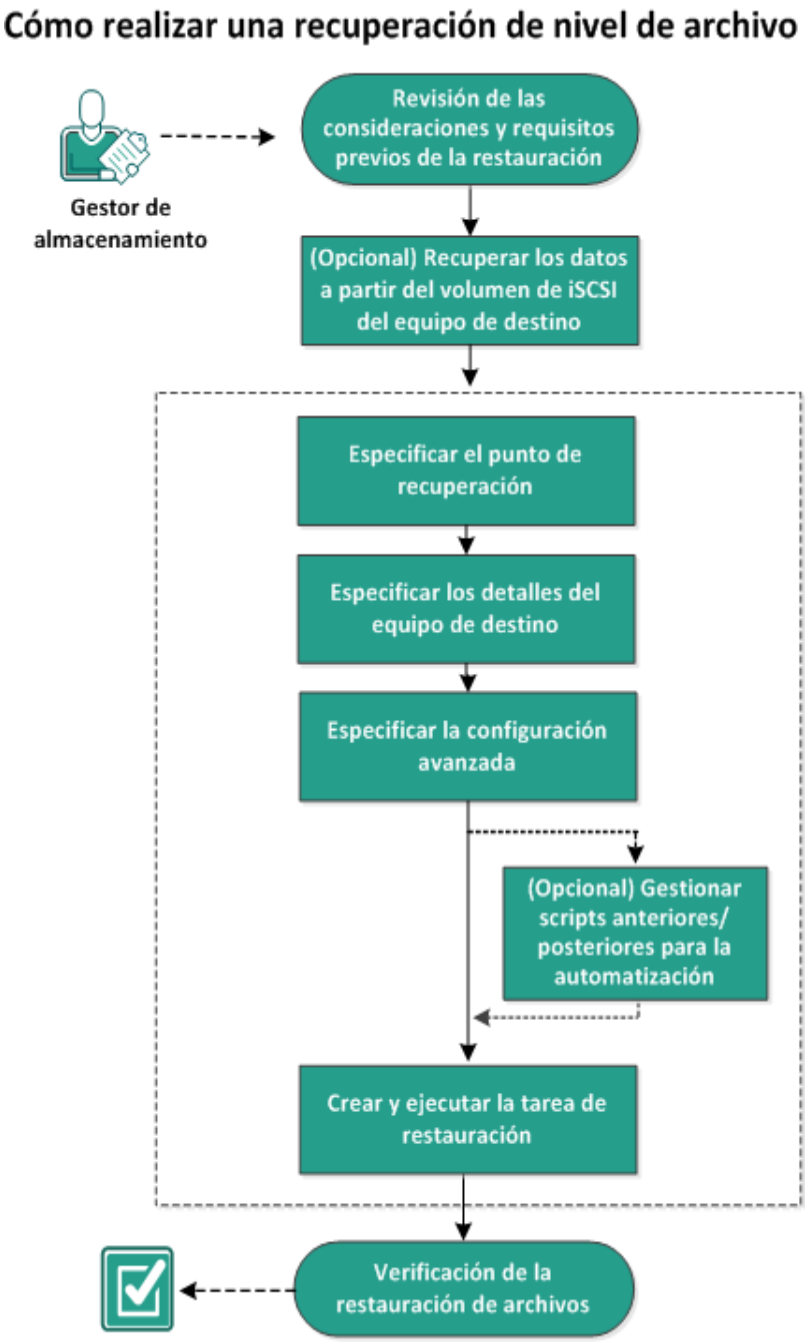
   SQL> ALTER DATABASE OPEN;

   La base de datos de Oracle se recupera mediante la reconstrucción completa.

Cómo realizar una recuperación a nivel de archivo en nodos de Linux

Una recuperación de nivel de archivo restaura archivos y carpetas individuales desde un punto de recuperación. La restauración mínima consiste en restaurar un archivo del punto de recuperación. Esta opción es útil si se desea restaurar solo los archivos seleccionados y no todo el punto de recuperación.

El diagrama siguiente muestra el proceso para realizar una recuperación de nivel de archivo:



Realice estas tareas para realizar una recuperación de nivel de archivo:

- Revisión de los requisitos previos
- (Opcional) Recuperación de los datos a partir del volumen de iSCSI del equipo de destino
- Especificación del punto de recuperación
- Especificación de los detalles del equipo de destino
- Especificación de la configuración avanzada
- (Opcional) Gestión de scripts anteriores/posteriores para la automatización
- Creación y ejecución de la tarea de restauración
- Verificación de la restauración de archivos

Revisión de los requisitos previos

Tenga en cuenta las opciones siguientes antes de realizar una recuperación de nivel de archivo:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado, si hay.
- Tiene un nodo de destino válido para la recuperación de datos.
- Ha verificado que el servidor de copia de seguridad de Linux sea compatible con el sistema de archivos que desee restaurar.

  Por ejemplo, RedHat 7.x no es compatible con el sistema de archivos de *reiserfs.* Si el sistema operativo del servidor de copia de seguridad es RedHat 7.x y desea restaurar el sistema de archivos reiserfs, se deberá instalar el controlador del sistema de archivos para admitir reiserfs. También se puede utilizar el Live CD del Agente de Arcserve Unified Data Protection para Linux para realizar la restauración a nivel del archivo, ya que el Live CD es compatible con todos los tipos de sistemas de archivos.
- Se han instalado los paquetes siguientes en el servidor de copia de seguridad de Linux:
  - mdadm
  - kpartx
  - lvm2
  - Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

(Opcional) Recuperación de los datos a partir del volumen de iSCSI del equipo de destino

Si se han almacenado sus datos en un volumen de destino de iSCSI, se puede conectar al volumen de iSCSI y recuperar datos. El volumen de iSCSI permite gestionar datos y transferirlos a una red.

Verifique que tiene la última versión del software del iniciador de iSCSI instalado en el servidor de copia de seguridad. El software de iniciador en sistemas de RHEL se encuentra dentro del paquete de iscsi-iniciador-utils. El software de iniciador en sistemas de SLES se encuentra dentro del paquete de open-iscsi.

Siga estos pasos:

1. Inicie sesión en el entorno de shell del servidor de copia de seguridad.
2. Ejecute uno de los siguientes comandos para iniciar el daemon del iniciador iSCSI.
   - Para los sistemas de RHEL:

     /etc/init.d/iscsid start

     El servicio en los sistemas de RHEL se denomina iscsid.
   - Para los sistemas de SLES:

     /etc/init.d/open-iscsi start

     El servicio en los sistemas de SLES se denomina open-iscsi.
3. Ejecute un script de detección para detectar el host de destino de iSCSI.

   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>

   El valor del puerto predeterminado del host de destino de iSCSI es 3260.
4. Tome nota del nombre completo de iSCSI (IQN) del host de destino de iSCSI que ha encontrado el script de detección antes de realizar el registro manual en el destino detectado.
5. Enumere el dispositivo de bloqueo disponible del servidor de copia de seguridad.

   #fdisk -l
6. Inicie sesión en el destino detectado.

   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l

   Se puede ver un dispositivo de bloqueo en el directorio /dev del servidor de copia de seguridad.
7. Ejecute el comando siguiente para obtener el nuevo nombre del dispositivo:

#fdisk -l

Se puede ver otro dispositivo denominado /dev/sd<x> en el servidor de copia de seguridad.

Por ejemplo, tenga en cuenta que el nombre del dispositivo es /dev/sdc. Este nombre de dispositivo se utilizará para crear una partición y un sistema de archivos en los pasos siguientes.

8. Monte el volumen de iSCSI mediante los comandos siguientes:

   # mkdir /iscsi

   # mount /dev/sdc1 /iscsi

   Nota: Cuando se especifique la ubicación de la sesión en el asistente de restauración, será necesario seleccionar Local e introducir la ruta /iscsi.

   Ejemplo: <ruta>/iscsi

9. (Opcional) Agregue el registro siguiente al archivo /etc/fstab para que el volumen de iSCSI se conecte automáticamente al servidor de copia de seguridad después de reiniciar el servidor.

   /dev/sdc1 /iscsi ext3 _netdev 0 0

   El servidor de copia de seguridad se puede conectar ahora al volumen de iSCSI y podrá recuperar datos del volumen de iSCSI.

Especificación del punto de recuperación para la copia de seguridad basada en agentes

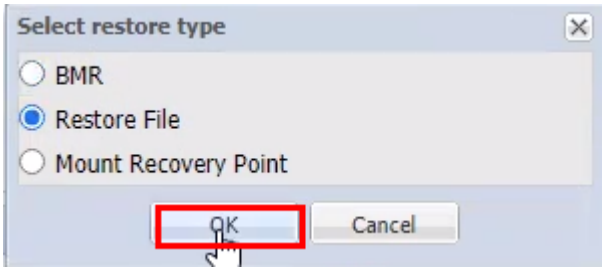
Cada vez que se realiza una copia de seguridad correcta, se creará un punto de recuperación. Especifique la información del punto de recuperación en el Asistente de restauración para que se puedan recuperar los datos exactos que desee. Se pueden restaurar archivos específicos o todos los archivos en función de sus requisitos.

Siga estos pasos:

1. Acceda al asistente de restauración de una de las formas siguientes:
   - **En Arcserve UDP:**
     a. Iniciar sesión en Arcserve UDP.
     b. Vaya a **recursos** > **Nodo** > **Todos los nodos**.

        Se muestran todos los nodos agregados en el panel central.
     c. Haga clic con el botón secundario del ratón en el nodo y, a continuación, haga clic en **Restaurar**.

        Se abre la interfaz web del Agente de Arcserve UDP (Linux) y se muestra el cuadro de diálogo Seleccionar tipo de restauración.
     d. En el cuadro de diálogo Seleccionar tipo de restauración, haga clic en la opción **Restaurar archivo** y, a continuación, haga clic en **Aceptar**.

        Nota: Se inicia sesión automáticamente en el nodo del agente y el Asistente de restauración se abre desde el nodo del agente.
   - **En el Agente de Arcserve Unified Data Protection para Linux:**
     a. Abra la interfaz web del Agente de Arcserve Unified Data Protection para Linux.

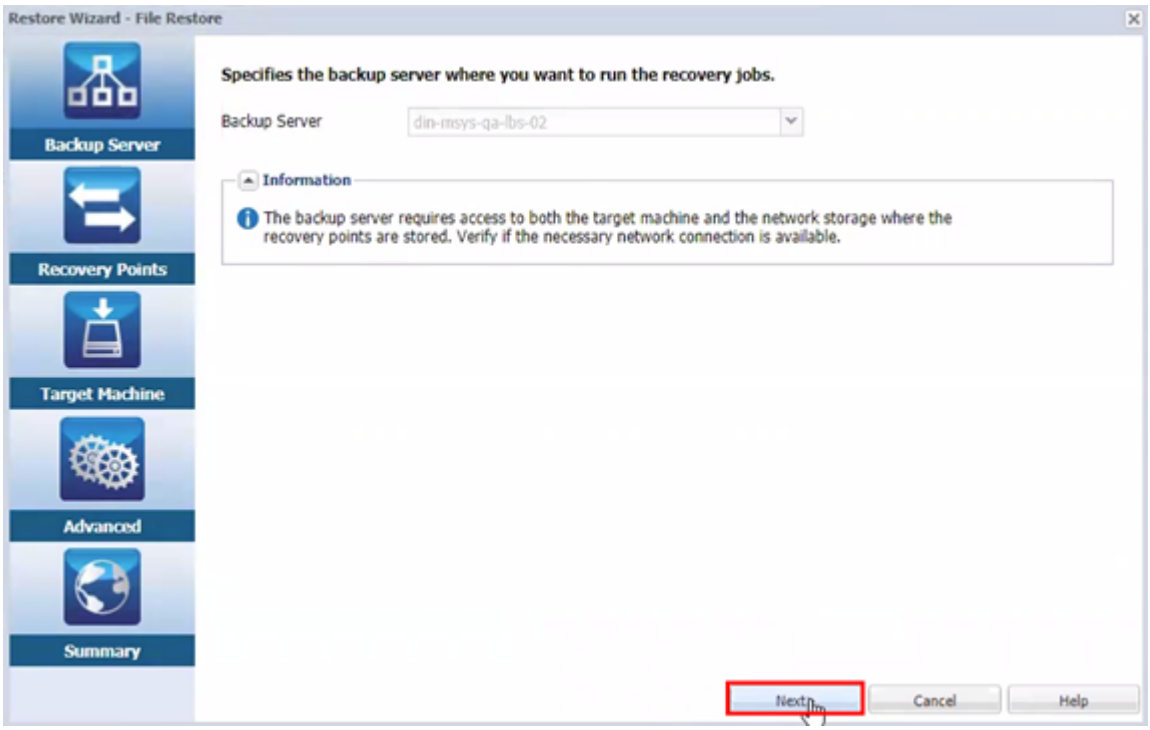
        Nota: Durante la instalación del Agente de Arcserve Unified Data Protection para Linux, recibirá la dirección URL para acceder al

servidor y gestionarlo. Inicie sesión en Agente de Arcserve Unified Data Protection para Linux.

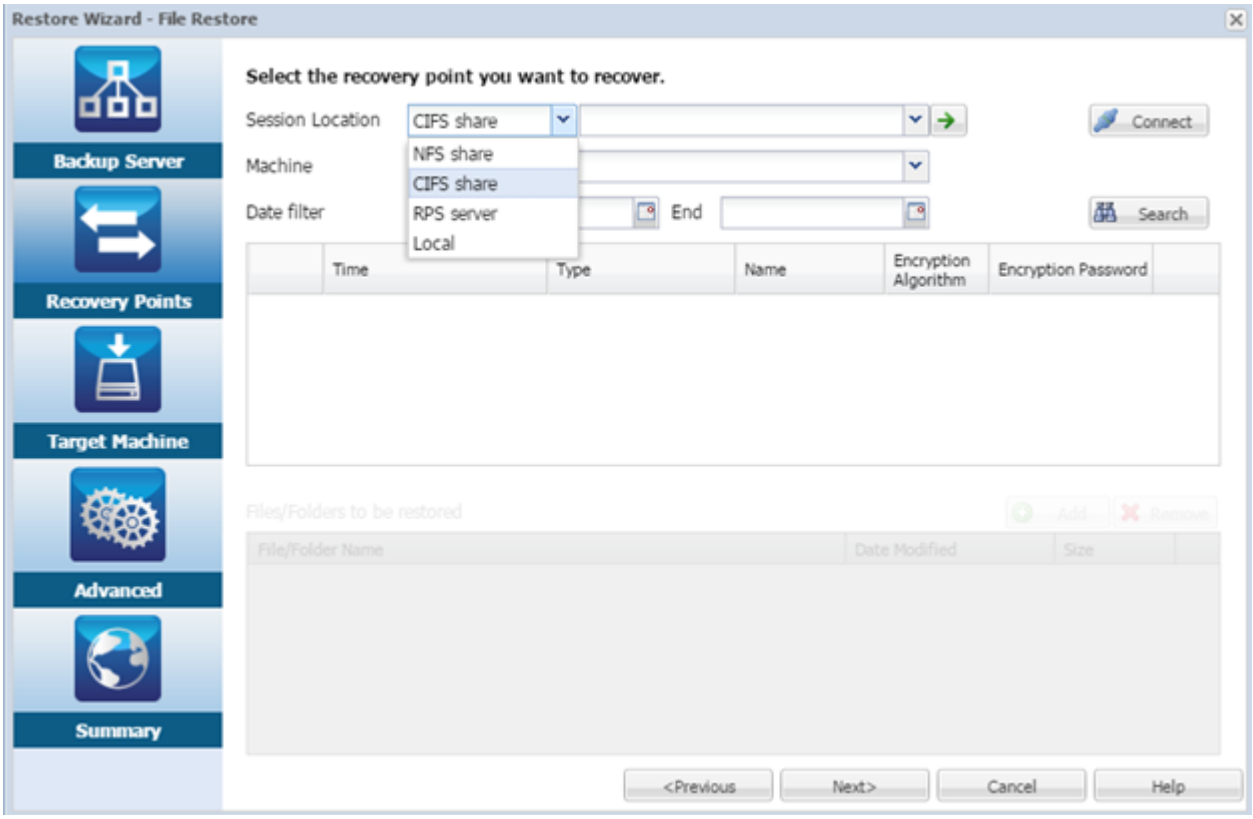
b. En el menú Asistente, haga clic en **Restaurar** y, a continuación, seleccione **Restaurar archivo**.

   Se abre el cuadro de diálogo Asistente de restauración - Restaurar archivo.

2. En la página Servidor de copia de seguridad del Asistente de restauración, se puede ver el servidor de copia de seguridad. No se puede seleccionar ninguna opción en la lista desplegable Servidor de copia de seguridad. Haga clic en **Siguiente**.



3. En la página Puntos de recuperación del Asistente de restauración, haga lo siguiente:



Importante: Si ha abierto el Asistente desde la Consola, los detalles del equipo y de la ubicación de la sesión se muestran automáticamente. Vaya al paso 4.

a. Seleccione **Recurso compartido de CIFS**, **Recurso compartido de NFS**, **Servidor de puntos de recuperación** o **Local** en la lista desplegable Ubicación de la sesión.

b. Realice uno de los pasos siguientes en función de la ubicación de la sesión:

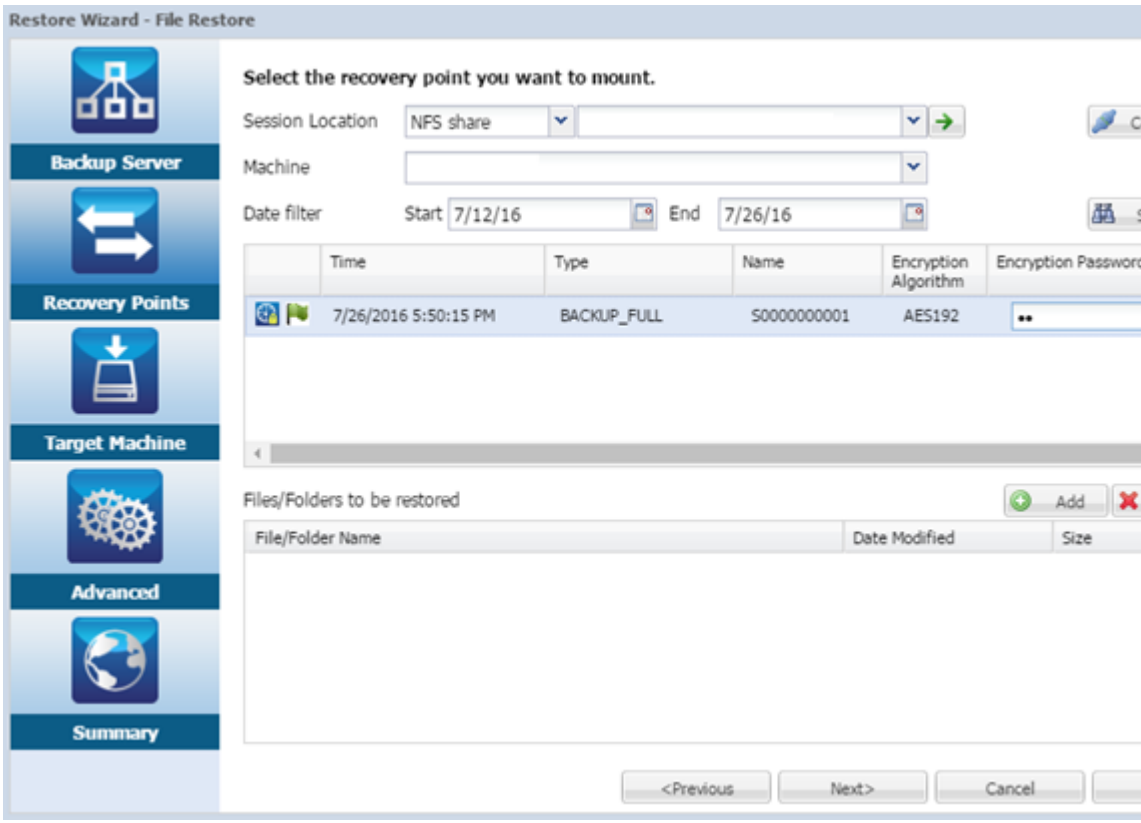
Para Recurso compartido de CIFS, Recurso compartido de NFS o Local

Especifique la ruta completa del recurso compartido de CIFS, el recurso compartido de NFS o el recurso local y, a continuación, haga clic en **Conectar**.

Se muestra la lista desplegable Equipo que incluye todos los equipos.

Nota: Si se selecciona la opción **Recurso compartido de CIFS**, se

deben especificar el nombre de usuario y la contraseña.



Para el servidor de puntos de recuperación:

a. Seleccione el servidor de puntos de recuperación y, a continuación, haga clic en **Agregar**.

   Aparece el cuadro de diálogo Información del servidor de puntos de recuperación.

b. Proporcione los detalles del servidor de puntos de recuperación y, a continuación, haga clic en **Sí**.

c. Seleccione el almacén de datos en la lista desplegable.

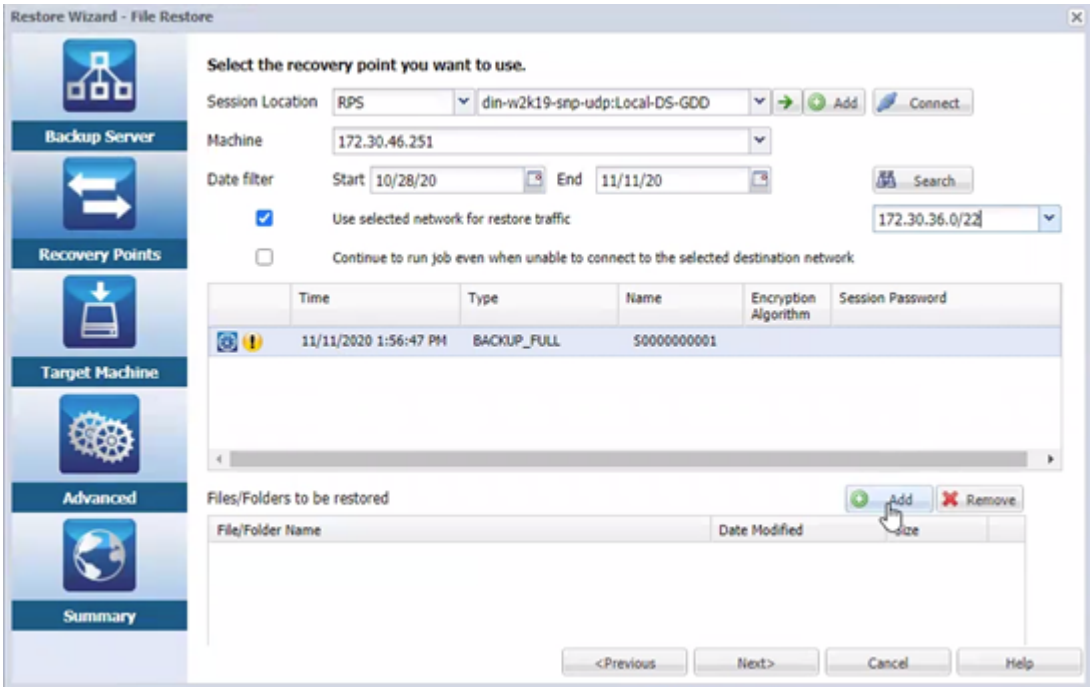
   El cuadro de diálogo Información del servidor de puntos de recuperación se cierra y aparece el Asistente.

d. Haga clic en **Conectar**.

   Todos los nodos de los cuales se ha realizado copia de seguridad en esta ubicación aparecen en la lista desplegable Equipo.

e. En la lista desplegable Equipo, seleccione el nodo que desea restaurar.

Aparecen todos los puntos de recuperación del nodo seleccionado.



4. Aplique el filtro de fecha para que se muestren los puntos de recuperación que se han generado entre la fecha especificada y, a continuación, haga clic en **Buscar**.

   Valor predeterminado: Las dos últimas semanas.

   Se muestran todos los puntos de recuperación disponibles entre las fechas especificadas.

5. Para activar la comunicación entre el Agente de Linux y el servidor de puntos de recuperación, seleccione la casilla de verificación **Utilizar la red seleccionada para el tráfico de restauración** y, a continuación, seleccione la red en la lista desplegable.

   Nota: Si no se puede acceder a la red de copia de seguridad seleccionada y para continuar la tarea de copia de seguridad con la red disponible o con la red predeterminada, haga clic en la casilla de verificación **Continuar ejecutando la tarea incluso cuando no se puede conectar con la red de copia de seguridad seleccionada**.

6. Seleccione el punto de recuperación que desee restaurar. Si se cifra el punto de recuperación, introduzca la contraseña de cifrado para restaurar datos.

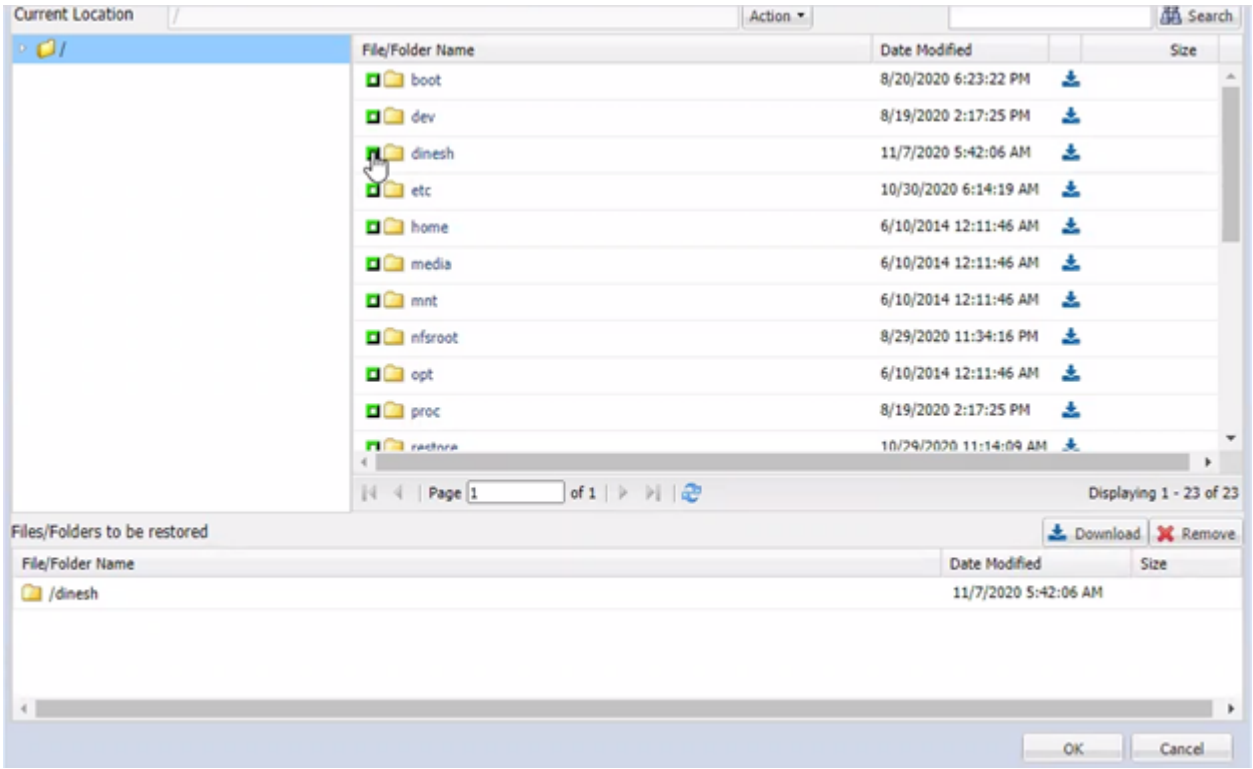
7. Para restaurar los archivos o carpetas, haga clic en **Agregar**.

   Aparece el cuadro de diálogo Examinar <nombre de nodo>.

Importante: Si aparece el mensaje de advertencia "Los archivos y las carpetas se muestran debajo del archivo del dispositivo. Haga clic para obtener más ayuda. En la Consola, consulte la siguiente nota para la resolución.

Nota: En el caso de algunos diseños de disco complejos, el archivo de dispositivo muestra el sistema de archivos. Este cambio en el comportamiento de visualización del sistema de archivos no afecta a la función de restauración a nivel de archivo de la máquina virtual de Linux basada en el host. Se puede explorar el sistema de archivos del archivo de dispositivo. También, se puede utilizar la función de búsqueda para buscar un directorio o archivo específicos.

8. En el cuadro de diálogo Explorar-<nombre de nodo>, seleccione el archivo o carpeta que desea restaurar y, a continuación, haga clic en **Aceptar**.



Nota: Si desea ubicar un archivo o una carpeta mediante el campo **Buscar**, asegúrese de que se selecciona la carpeta superior en la jerarquía. La búsqueda se realiza en todas las carpetas secundarias de la carpeta seleccionada.

El cuadro de diálogo Examinar <nombre de nodo> se cierra y vuelve a la página Puntos de recuperación. Los archivos y carpetas que se han seleccionado aparecen en Archivos/carpetas para restaurar.

9. Haga clic en **Siguiente**.

Aparecerá la página Equipo de destino.

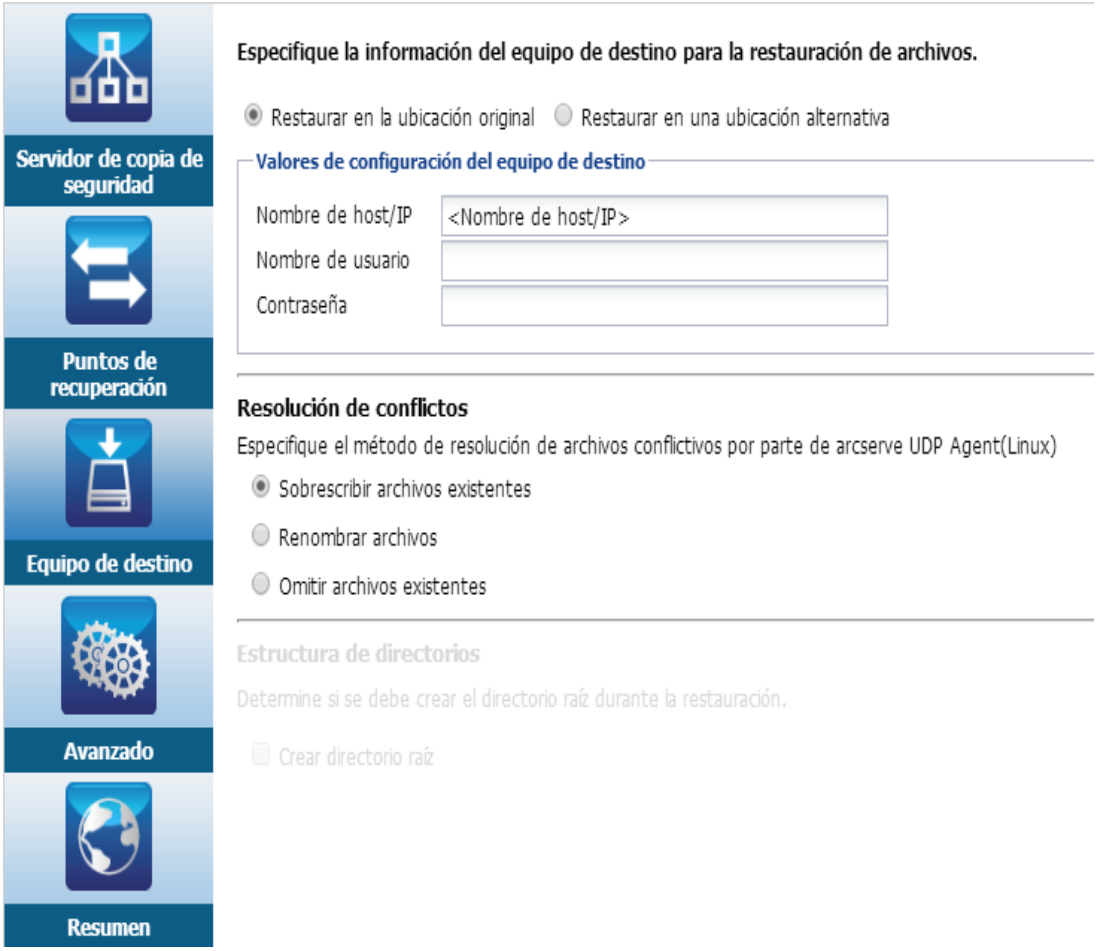
Se especifica el punto de recuperación.

Especificación de los detalles del equipo de destino

Especifique los detalles del nodo de destino para restaurar los datos en el nodo. Se pueden restaurar los archivos o las carpetas que se han seleccionado en el nodo de origen o en un nodo nuevo.

Para realizar una restauración en el nodo del cual se ha realizado la copia de seguridad de los datos, siga los pasos siguientes:

1. En la página Equipo de destino, seleccione **Restaurar en la ubicación original**.



2. Introduzca el nombre de usuario y la contraseña del nodo.
3. Seleccione una de las opciones siguientes para resolver los archivos en conflicto:

   Sobrescribir archivos existentes

Especifica si existe el archivo en el equipo de destino. A continuación, el archivo de copia de seguridad del punto de recuperación reemplazará el archivo existente.

Cambiar el nombre de los archivos

Especifica que, si el archivo existe en el equipo de destino, se creará a continuación un nuevo archivo con el mismo nombre de archivo y con la extensión de archivo *.d2dduplicate<x>.* <x> especifica el número de veces que se ha restaurado el archivo. Todos los datos se restaurarán en el nuevo archivo.

Omitir archivos existentes

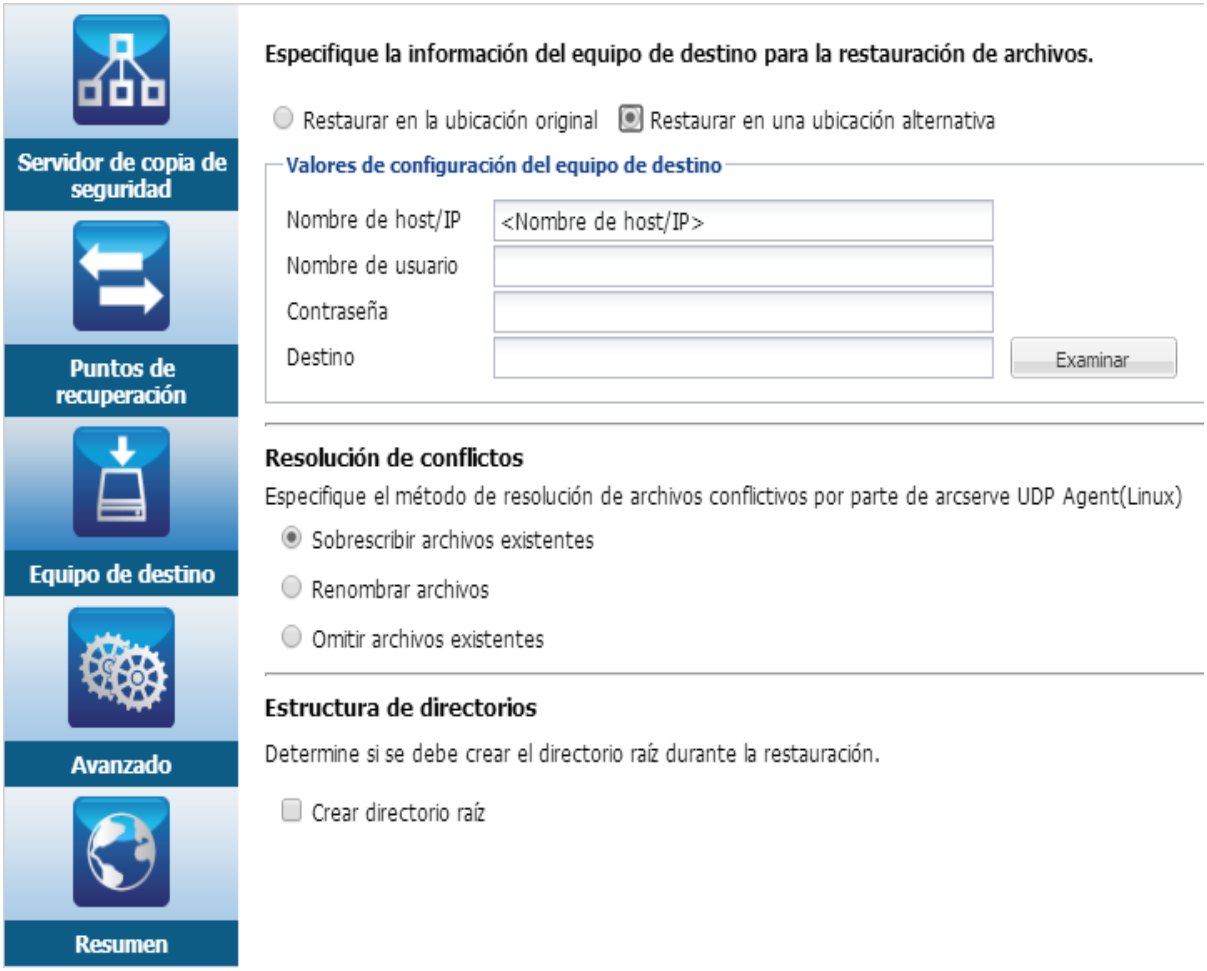
Especifica que existe el mismo archivo en el equipo de destino. A continuación, los archivos no se restauran desde el punto de recuperación.

4. (Opcional) Seleccione **Crear directorio raíz**.
5. Haga clic en **Siguiente**.

   Aparecerá la página Configuración avanzada.

Para restaurar en un nodo nuevo, siga estos pasos:

1. En la página Equipo de destino, seleccione **Restaurar en la ubicación alternativa**.



2. Introduzca el nombre de host o la dirección IP del nodo de destino.
3. Introduzca el nombre de usuario y la contraseña del nodo.
4. Introduzca la ruta donde se restauran los datos o haga clic en **Examinar** para seleccionar la carpeta donde se restauran los datos y, a continuación, haga clic en **Aceptar**.
5. Seleccione una de las opciones siguientes para resolver los archivos en conflicto:

   Sobrescribir archivos existentes

   Especifica si existe el archivo en el equipo de destino. A continuación, el archivo de copia de seguridad del punto de recuperación reemplazará el archivo existente.

   Cambiar el nombre de los archivos

   Especifica que, si el archivo existe en el equipo de destino, se creará a continuación un nuevo archivo con el mismo nombre de archivo y con la extensión de archivo *.d2dduplicate<x>*. <x> especifica el número de veces

que se ha restaurado el archivo. Todos los datos se restaurarán en el nuevo archivo.

Omitir archivos existentes

Especifica que existe el mismo archivo en el equipo de destino. Como consecuencia, los archivos no se restauran desde el punto de recuperación.

6. (Opcional) Seleccione **Crear directorio raíz**.
7. Haga clic en **Siguiente**.

   Aparecerá la página Configuración avanzada.

Se especifican los detalles del equipo de destino.

Especificación de la configuración avanzada

Especifique la configuración avanzada para realizar una recuperación programada de los datos. La recuperación programada asegura que los datos se recuperen en la hora especificada incluso en su ausencia.

Siga estos pasos:

1. Establezca la fecha y la hora de inicio seleccionando una de las opciones siguientes:

   Ejecutar ahora

   Inicia la tarea de restauración de nivel de archivo tan pronto como se envíe la tarea.

   Establecer fecha y hora de inicio

   Inicia la tarea de restauración de nivel de archivo a la hora especificada después de haber enviado la tarea.

2. (Opcional) Seleccione la **Estimación del tamaño del archivo**.
3. (Opcional) Seleccione un script de la opción **Configuración de scripts anteriores/posteriores**.

   Estos scripts ejecutan comandos de script para realizar acciones antes del inicio de la tarea o cuando esta se finalice.

   Nota: Los campos **Configuración de scripts previos y posteriores** se rellenan solamente si ya se ha creado un archivo de script y se ha colocado en la siguiente ubicación:

   /opt/Arcserve/d2dserver/usr/prepost

   Nota: Para obtener más información acerca de cómo crear los scripts anteriores/posteriores, consulte *Gestión de scripts anteriores/posteriores para la automatización*.

4. Haga clic en **Siguiente**.

   Aparecerá la página **Resumen**.

   Se especifica la configuración avanzada.

(Opcional) Gestión de scripts anteriores/posteriores para la automatización

Los scripts previos/posteriores permiten ejecutar su propia lógica empresarial en las etapas específicas de una tarea en ejecución. Se puede especificar cuando se ejecutan los scripts en **Configuración previa/posterior** de los scripts del **Asistente de copia de seguridad** y el **Asistente de restauración** en la interfaz de usuario. Los scripts se pueden ejecutar en el servidor de copia de seguridad en función de la configuración.

La gestión de scripts anteriores/posteriores constituye un proceso de dos partes que consta de la creación del script anterior/posterior y la colocación de dicho script en la carpeta prepost.

Creación de scripts anteriores/posteriores

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un archivo de script mediante el uso de las variables de entorno en el lenguaje de generación de scripts preferido.

   Variables de entorno de scripts anteriores/posteriores

   Para crear un script, utilice las variables de entorno siguientes:

   D2D_JOBNAME

   Indica el nombre de la tarea.

   D2D_JOBID

   Identifica el ID de la tarea. El ID de la tarea es un número que se proporciona a la tarea cuando esta se ejecuta. Si se ejecuta la misma tarea de nuevo, obtendrá un nuevo número de tareas.

   D2D_TARGETNODE

   Identifica el nodo del cual se realiza copia de seguridad o que se restaura.

   D2D_JOBTYPE

   Identifica el tipo de tarea en ejecución. Los valores siguientes identifican la variable D2D_JOBTYPE:

   backup.full

   Identifica la tarea como copia de seguridad completa.

   backup.incremental

Identifica la tarea como copia de seguridad incremental.

backup.verify

Identifica la tarea como copia de seguridad de verificación.

restore.bmr

Identifica la tarea como una reconstrucción completa. Esta tarea es de restauración.

restore.file

Identifica la tarea como una restauración de nivel de archivo. Esta tarea es de restauración.

D2D_SESSIONLOCATION

Identifica la ubicación donde se almacenan los puntos de recuperación.

D2D_PREPOST_OUTPUT

Identifica un archivo temporal. El contenido de la primera línea del archivo temporal aparecerá en el registro de actividades.

D2D_JOBSTAGE

Indica la etapa de la tarea. Los valores siguientes identifican la variable D2D_ JOBSTAGE:

pre-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad antes de que se inicie la tarea.

post-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad después de que se complete la tarea.

pre-job-target

Identifica el script que se ejecuta en el equipo de destino antes de que se inicie la tarea.

post-job-target

Identifica el script que se ejecuta en el equipo de destino después de que se complete la tarea.

pre-snapshot

Identifica el script que se ejecuta en el equipo de destino antes de capturar la instantánea.

post-snapshot

Identifica el script que se ejecuta en el equipo de destino después de capturar la instantánea.

D2D_TARGETVOLUME

Identifica el volumen del cual se realiza copia de seguridad durante una tarea de copia de seguridad. Esta variable es aplicable para los scripts de instantáneas previas y posteriores para una tarea de copia de seguridad.

D2D_JOBRESULT

Identifica el resultado para un script de tarea de publicación. Los valores siguientes identifican la variable D2D_JOBRESULT:

success

Identifica el resultado como correcto.

fail

Identifica el resultado como incorrecto.

D2DSVR_HOME

Identifica la carpeta donde se instala el servidor de copia de seguridad. Esta variable es aplicable para los scripts que se ejecutan en el servidor de copia de seguridad.

El script se crea.

Nota: En todos los scripts, un valor de retorno de cero indica que se ha realizado correctamente, mientras que un valor de retorno distinto a cero indica que se han producido errores.

Colocación del script en la carpeta prepost y verificación

Todos los scripts previos/posteriores para un servidor de copia de seguridad se gestionan centralmente desde la carpeta prepost en la ubicación siguiente:

/opt/Arcserve/d2dserver/usr/prepost

Siga estos pasos:

1. Coloque el archivo en la siguiente ubicación del servidor de copia de seguridad:

   /opt/Arcserve/d2dserver/usr/prepost
2. Proporcione los permisos de ejecución al archivo de script.
3. Inicie sesión en la interfaz web del Agente de Arcserve Unified Data Protection para Linux.
4. Abra el **Asistente de copia de seguridad** o el **Asistente de restauración** y vaya a la ficha **Configuración avanzada**.

5. Seleccione el archivo de script en la lista desplegable **Configuración de scripts anteriores/posteriores** y, a continuación, envíe la tarea.
6. Haga clic en **Registro de actividad** y verifique que el script se ejecute en la tarea de copia de seguridad especificada.

   El script se ejecuta.

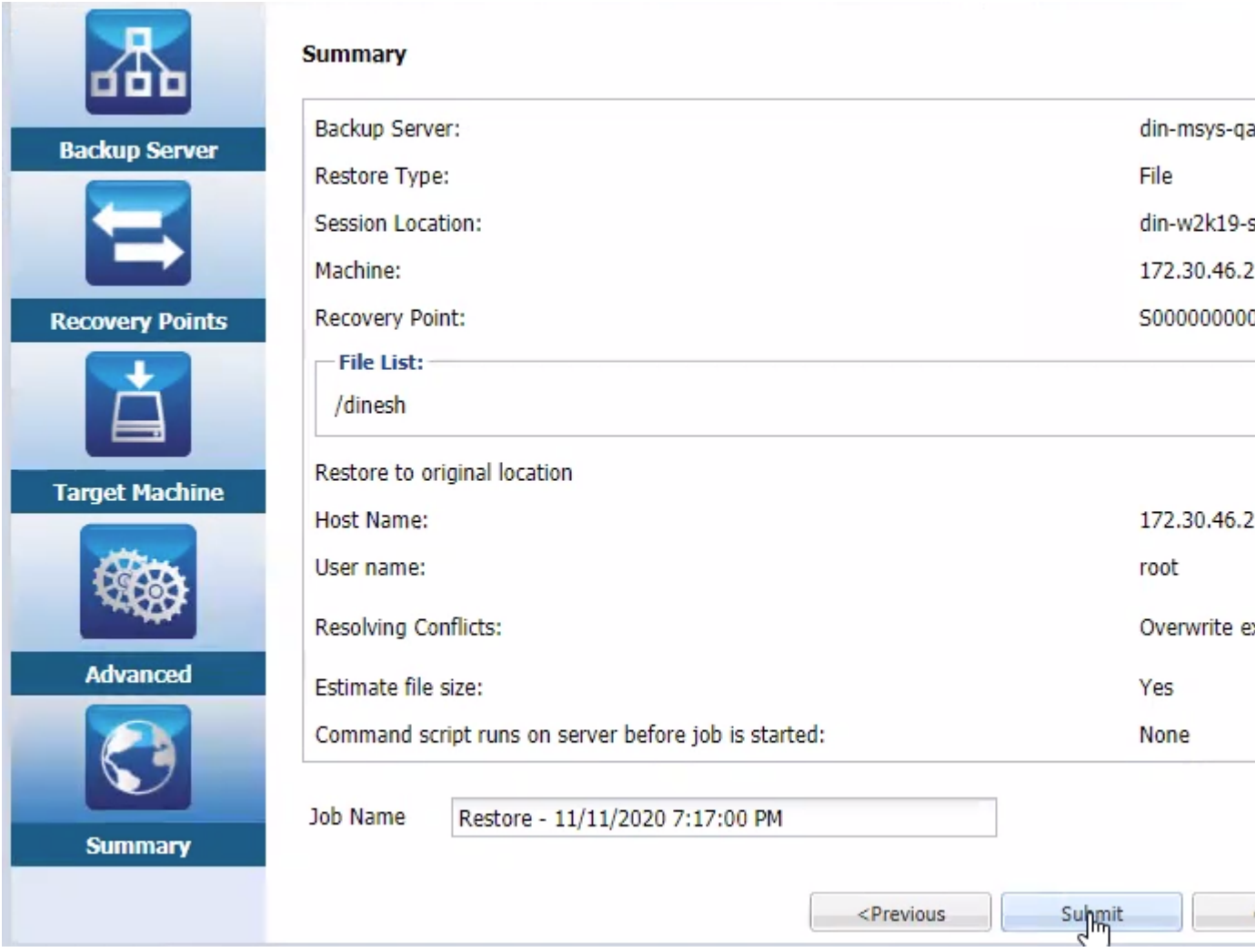
   Los scripts anteriores/posteriores se crean correctamente y se colocan en la carpeta prepost.

Creación y ejecución de la tarea de restauración

Cree y ejecute la tarea de restauración de modo que se pueda iniciar la recuperación de nivel de archivo. Verifique la información del punto de recuperación antes de restaurar los archivos. Si es necesario, vuelva atrás y cambie la configuración de restauración en el asistente.

Siga estos pasos:

1. En la página Resumen del Asistente de restauración, verifique los detalles de la restauración.



2. Realice uno de los procedimientos siguientes:
   - Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para cambiar el valor de configuración incorrecto.

- Si la información de resumen es correcta, introduzca un nombre de tarea y, a continuación, haga clic en **Enviar** para iniciar el proceso de restauración.

Nota: El campo Nombre de la tarea tiene un nombre predeterminado inicialmente. Se puede introducir el nombre de la tarea nuevo que elija pero no se puede dejar vacío este campo.

Se cierra el Asistente de restauración. Se puede ver el estado de la tarea en la página Estado de la tarea.

Se ha creado y ejecutado la tarea de restauración correctamente.

Verificación de la restauración de archivos

Después de la finalización de la tarea de restauración, verifique que todos los archivos se restauren en el nodo de destino. Compruebe las fichas **Historial de tareas** y **Registro de actividad** en el panel **Estado** para controlar el progreso del proceso de restauración.

Siga estos pasos:

1. Vaya al equipo de destino en el que se han restaurado los datos.
2. Compruebe que los datos obligatorios del punto de recuperación se hayan restaurado.

   Los archivos se han verificado correctamente.

   La recuperación de nivel de archivo se ha realizado correctamente.

Cómo realizar una recuperación de archivos desde copias de seguridad sin agente basadas en el host para nodos de Linux

Una recuperación de nivel de archivo restaura archivos y carpetas individuales desde un punto de recuperación. La restauración mínima consiste en restaurar un archivo del punto de recuperación. Esta opción es útil si se desea restaurar solo los archivos seleccionados y no todo el punto de recuperación.

Realice estas tareas para realizar una recuperación de nivel de archivo:

- Revisión de los requisitos previos
- Especificación del punto de recuperación
- Especificación de los detalles del equipo de destino
- Especificación de la configuración avanzada
- (Opcional) Gestión de scripts anteriores/posteriores para la automatización
- Creación y ejecución de la tarea de restauración
- Verificación de la restauración de archivos

Revisión de los requisitos previos

Tenga en cuenta las opciones siguientes antes de realizar una recuperación de nivel de archivo:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado, si hay.
- Tiene un nodo de destino válido para la recuperación de datos.
- Ha verificado que el servidor de copia de seguridad de Linux sea compatible con el sistema de archivos que desee restaurar.

  Por ejemplo, RedHat 7.x no es compatible con el sistema de archivos de *reiserfs.* Si el sistema operativo del servidor de copia de seguridad es RedHat 7.x y desea restaurar el sistema de archivos reiserfs, se deberá instalar el controlador del sistema de archivos para admitir reiserfs. También se puede utilizar el Live CD del Agente de Arcserve Unified Data Protection para Linux para realizar la restauración a nivel de archivo, ya que el Live CD es compatible con todos los tipos de sistemas de archivos.
- Se han instalado los paquetes siguientes en el servidor de copia de seguridad de Linux:
  - mdadm
  - kpartx
  - lvm2
  - Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Especificación del punto de recuperación

Cada vez que se realiza una copia de seguridad correcta, se creará un punto de recuperación. Especifique la información del punto de recuperación en el **Asistente de restauración** para que se puedan recuperar los datos exactos que desee. Se pueden restaurar archivos específicos o todos los archivos en función de sus requisitos.

Siga estos pasos:

1. Acceda al asistente de restauración de una de las formas siguientes:

   En Arcserve UDP:

   a. Iniciar sesión en Arcserve UDP.

   b. Haga clic en la ficha **recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos de agregados en el panel central.

   d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   e. Haga clic en **Restaurar** del menú desplegable **Acción**.

      Se abre la interfaz web del Agente de Arcserve Unified Data Protection para Linux. Se muestra el cuadro de diálogo de selección del tipo de restauración en la interfaz de usuario del agente.

   f. Seleccione el tipo de restauración y haga clic en **Aceptar**.

      Nota: Se inicia sesión automáticamente en el nodo del agente y el **Asistente de restauración** se abre desde el nodo del agente.

   En el Agente de Arcserve Unified Data Protection para Linux:

   a. Abra la interfaz web del Agente de Arcserve Unified Data Protection para Linux.

      Nota: Durante la instalación del Agente de Arcserve Unified Data Protection para Linux, recibirá la dirección URL para acceder al servidor y gestionarlo. Inicie sesión en el Agente de Arcserve Unified Data Protection para Linux.

   b. Haga clic en **Restaurar** en el menú **Asistente** y seleccione **Archivo de restauración**.

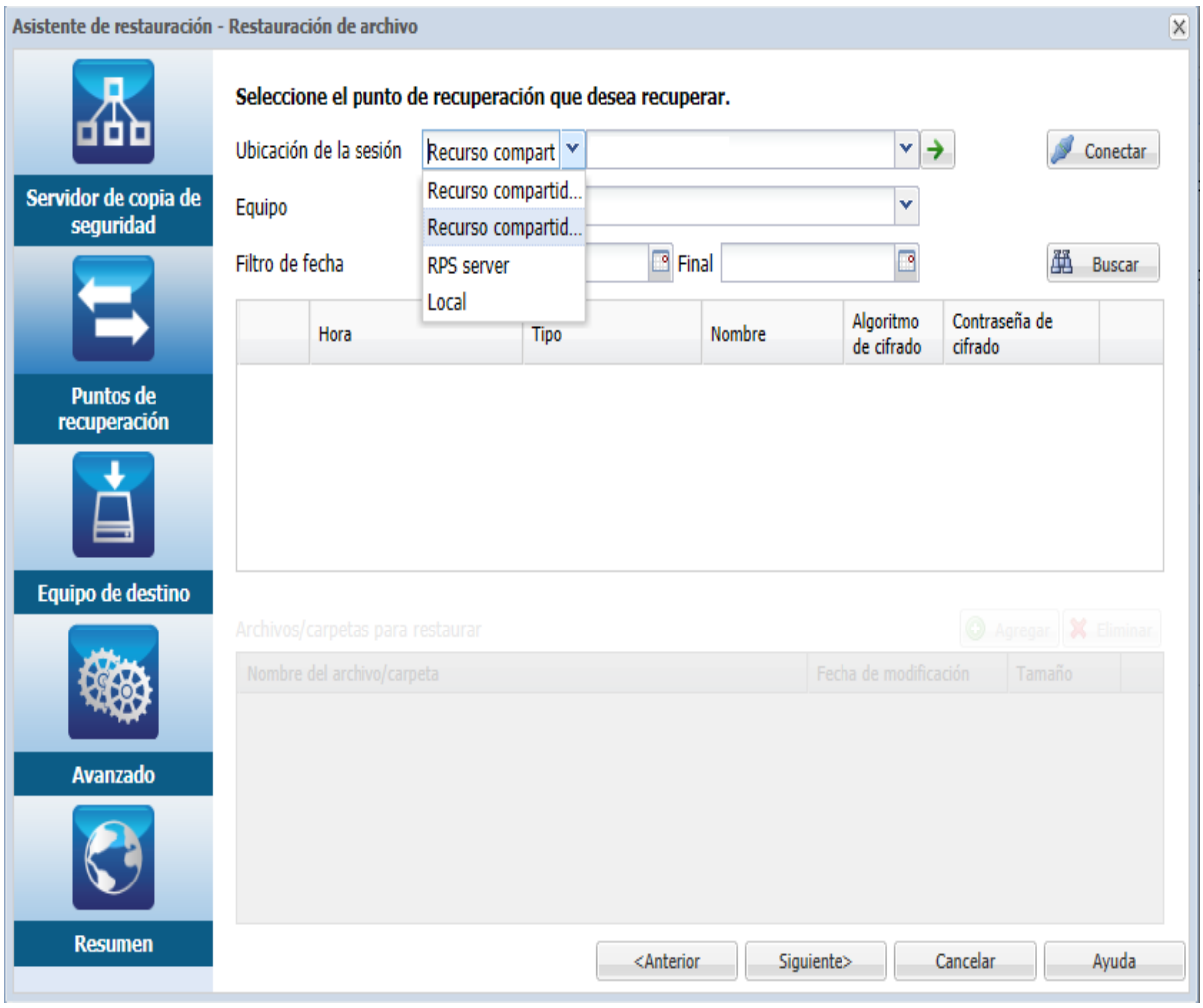
      Se abre **Asistente de restauración - Restauración de archivo.**

      Se puede ver el servidor de copia de seguridad en la página **Servidor de copia de seguridad** del **Asistente de restauración**. No se puede seleccionar ninguna opción en la lista desplegable **Servidor de copia de seguridad**.

2. Haga clic en **Siguiente**.

   Aparece la página **Puntos de recuperación** del **Asistente de restauración**.

   Importante: Si ha abierto el Asistente desde la Consola, los detalles del equipo y de la ubicación de la sesión se muestran automáticamente. Vaya al paso 5.



3. En la lista desplegable **Ubicación de la sesión**, seleccione **Recurso compartido de CIFS** o **RPS**.

   Nota: No se puede seleccionar Recurso compartido de NFS o Local para la restauración de sesiones de copia de seguridad sin agente basada en host.

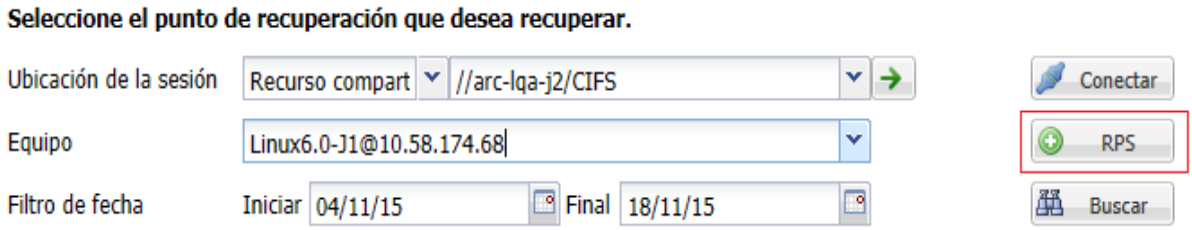
4. Realice uno de los pasos siguientes en función de la ubicación de la sesión:

   Para el recurso compartido de CIFS:

   a. Especifique la ruta completa del recurso compartido de CIFS y haga clic en **Conectar**.

b. Especifique el nombre de usuario y la contraseña para conectarse al recurso compartido de CIFS y haga clic en **Aceptar**.

   Se muestra la lista desplegable Equipo que incluye todos los equipos. Junto a la lista, aparece el botón RPS.



c. Seleccione el equipo de la lista desplegable y haga clic en RPS.

   Aparece el cuadro de diálogo **Información del servidor de puntos de recuperación**.

d. Proporcione los detalles del servidor de puntos de recuperación y haga clic en Sí.

   El cuadro de diálogo **Información del servidor de puntos de recuperación** se cierra. Todos los puntos de recuperación del equipo seleccionado se muestran debajo de la opción **Filtro de fecha.**

Para el servidor de puntos de recuperación:

a. Seleccione el servidor de puntos de recuperación y haga clic en Agregar.

   Aparece el cuadro de diálogo **Información del servidor de puntos de recuperación**.

b. Proporcione los detalles del servidor de puntos de recuperación y haga clic en Cargar.

c. Seleccione el almacén de datos de la lista desplegable y haga clic en **Sí**.

   El cuadro de diálogo **Información del servidor de puntos de recuperación** se cierra y aparece el Asistente.

d. Haga clic en **Conectar**.

   Se muestra la lista desplegable Equipo que incluye todos los equipos.

e. Seleccione el equipo de la lista desplegable.

   Todos los puntos de recuperación del equipo seleccionado se muestran debajo de la opción **Filtro de fecha.**

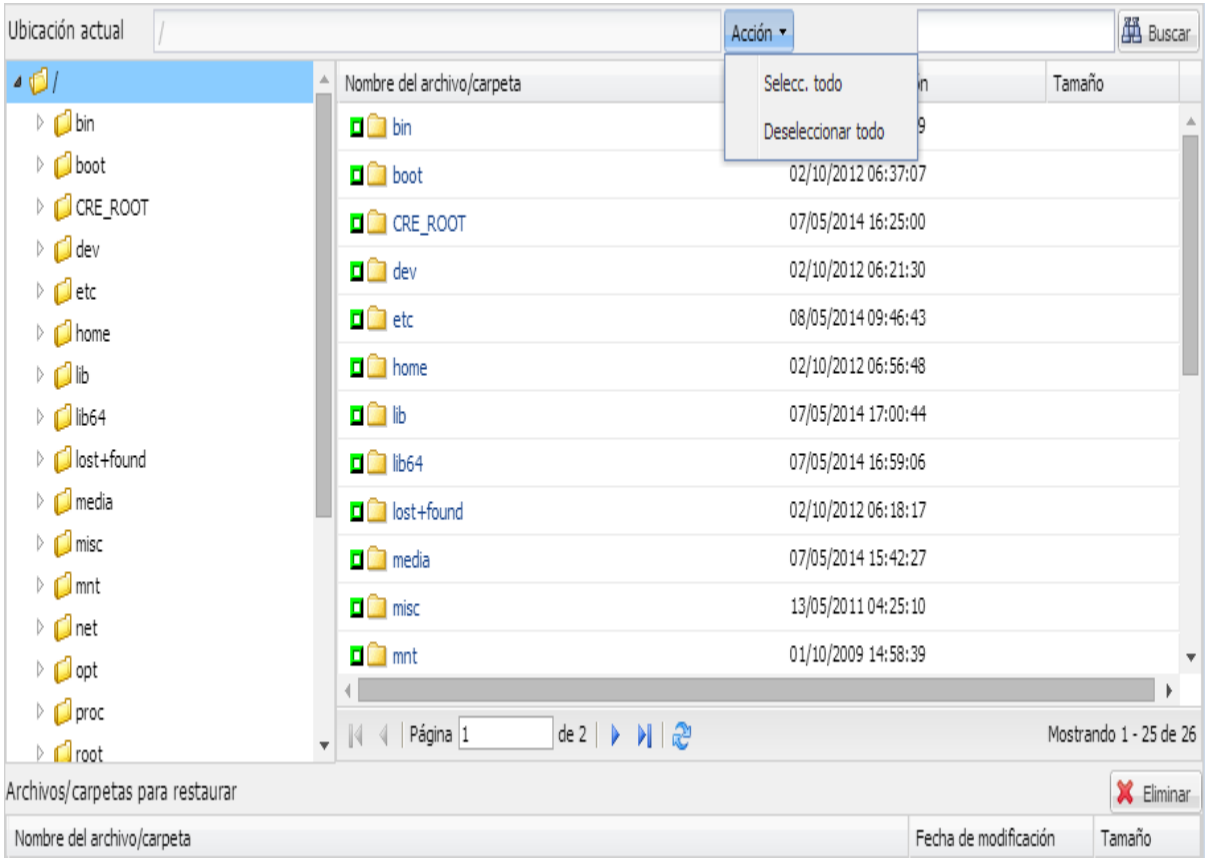
5. Aplique el filtro de fecha para que se muestren los puntos de recuperación que se han generado entre la fecha especificada y haga clic en **Buscar**.

Valor predeterminado: Las dos últimas semanas.

Se muestran todos los puntos de recuperación disponibles entre las fechas especificadas.

6. Seleccione el punto de recuperación que desee restaurar y haga clic en **Agregar**. Si se cifra el punto de recuperación, introduzca la contraseña de cifrado para restaurar datos.

   Aparece el cuadro de diálogo **Examinar <nombre de nodo>**.



Importante: Si aparece el mensaje de advertencia "Los archivos y las carpetas se muestran debajo del archivo del dispositivo. Haga clic para obtener más ayuda. En la Consola, consulte la siguiente nota para la resolución.

Nota: En el caso de algunos diseños de disco complejos, el archivo de dispositivo muestra el sistema de archivos. Este cambio en el comportamiento de visualización del sistema de archivos no afecta a la función de restauración a nivel de archivo de la máquina virtual de Linux basada en el host. Se puede explorar el sistema de archivos del archivo de dispositivo. También, se puede utilizar la función de búsqueda para buscar un directorio o archivo específicos.

7. Seleccione los archivos y las carpetas que desee restaurar y haga clic en **Aceptar**.

Nota: Si desea ubicar un archivo o una carpeta mediante el campo **Buscar**, asegúrese de que se selecciona la carpeta superior en la jerarquía. La búsqueda se realiza en todas las carpetas secundarias de la carpeta seleccionada.

El cuadro de diálogo **Examinar <nombre de nodo>** se cierra y vuelve a la página **Puntos de recuperación.** Los archivos y carpetas que se han seleccionado aparecen en **Archivos/carpetas para restaurar**.

8. Haga clic en **Siguiente**.

   Aparecerá la página **Equipo de destino**.

   Se especifica el punto de recuperación.

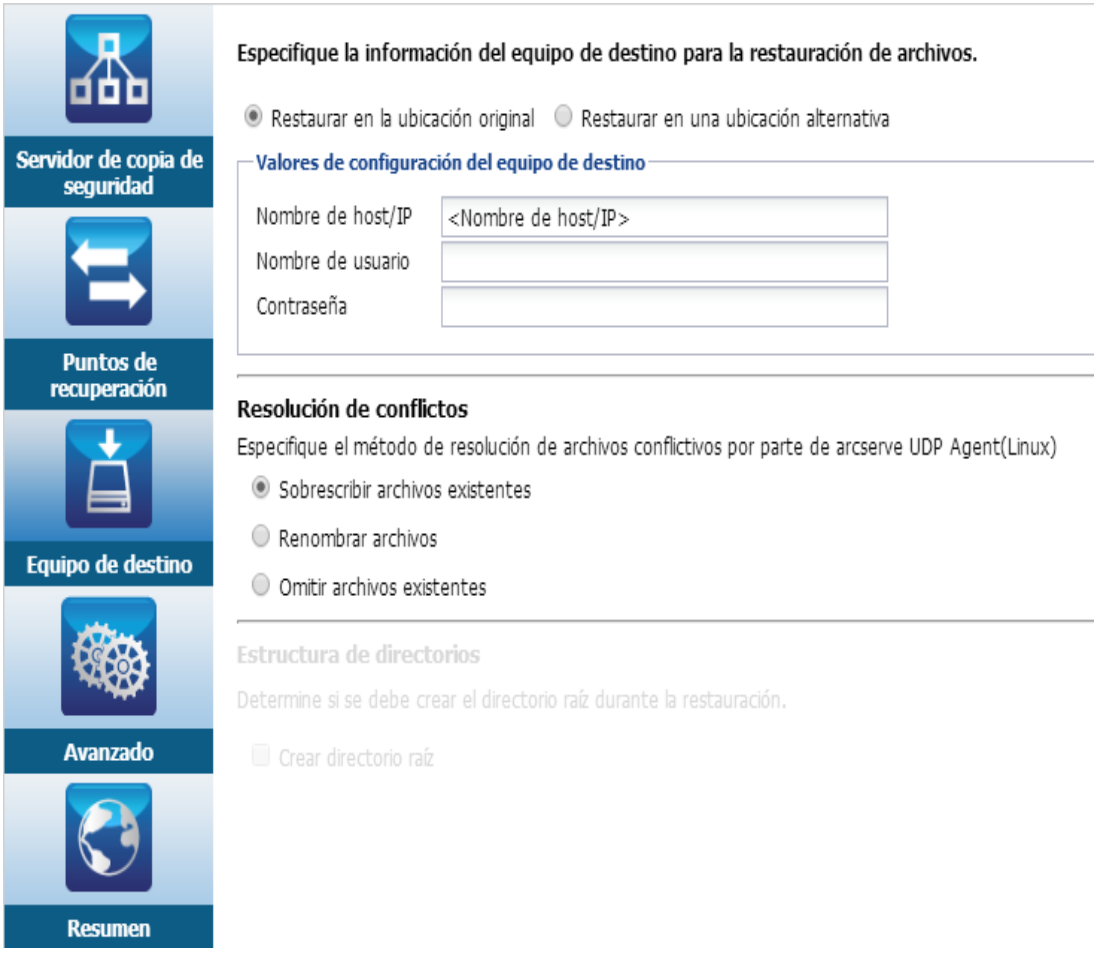
Especificación de los detalles de la máquina de destino

Especifique los detalles del nodo de destino para restaurar los datos en el nodo. Se pueden restaurar los archivos o las carpetas que se han seleccionado en el nodo de origen o en un nodo nuevo.

Para realizar una restauración en el nodo del cual se ha realizado la copia de seguridad de los datos, siga los pasos siguientes:

1. Seleccione **Restaurar en la ubicación original** de la página **Equipo de destino.**

   El campo **Nombre de host** en **Valores de configuración del equipo de destino** se rellena con el nombre del nodo de origen.



2. Introduzca el nombre de usuario y la contraseña del nodo.
3. Seleccione una de las opciones siguientes para resolver los archivos en conflicto:

Sobrescribir archivos existentes

Especifica si existe el archivo en el equipo de destino. A continuación, el archivo de copia de seguridad del punto de recuperación reemplazará el archivo existente.

Cambiar el nombre de los archivos

Especifica que, si el archivo existe en el equipo de destino, se creará a continuación un nuevo archivo con el mismo nombre de archivo y con la extensión de archivo *.d2dduplicate<x>.* <x> especifica el número de veces que se ha restaurado el archivo. Todos los datos se restaurarán en el nuevo archivo.

Omitir archivos existentes

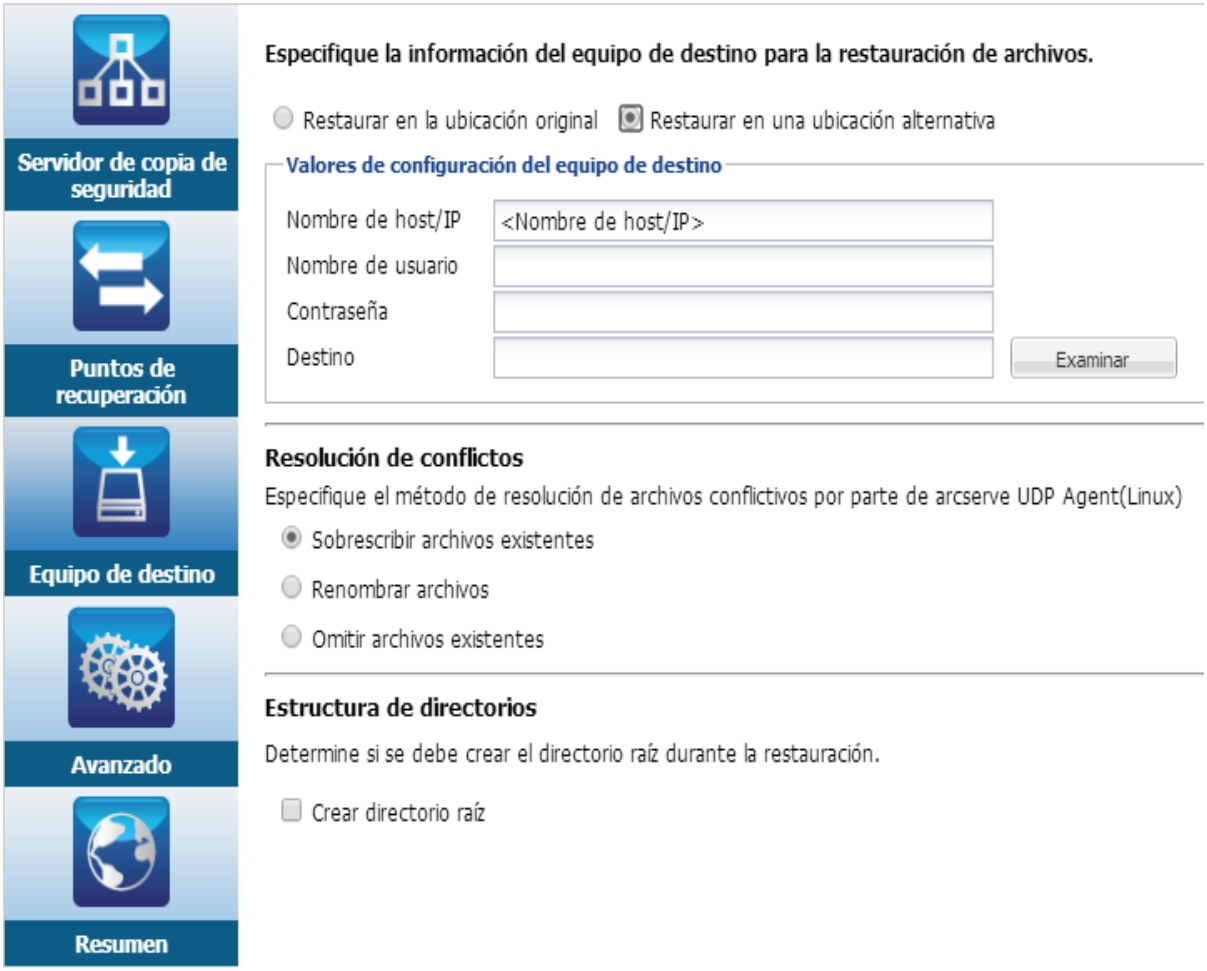
Especifica que existe el mismo archivo en el equipo de destino. A continuación, los archivos no se restauran desde el punto de recuperación.

4. Haga clic en **Siguiente**.

   Aparecerá la página **Configuración avanzada**.

Para restaurar en un nodo nuevo, siga estos pasos:

1. Seleccione **Restaurar en una ubicación alternativa** desde la página **Equipo de destino.**



2. Introduzca el nombre de host o la dirección IP del nodo de destino.
3. Introduzca el nombre de usuario y la contraseña del nodo.
4. Introduzca la ruta donde se restauran los datos o haga clic en **Examinar** para seleccionar la carpeta donde se restauran los datos y haga clic en **Aceptar.**
5. Seleccione una de las opciones siguientes para resolver los archivos en conflicto:

   Sobrescribir archivos existentes

   Especifica si existe el archivo en el equipo de destino. A continuación, el archivo de copia de seguridad del punto de recuperación reemplazará el archivo existente.

   Cambiar el nombre de los archivos

   Especifica que, si el archivo existe en el equipo de destino, se creará a continuación un nuevo archivo con el mismo nombre de archivo y con la extensión de archivo *.d2dduplicate<x>.* <x> especifica el número de veces

que se ha restaurado el archivo. Todos los datos se restaurarán en el nuevo archivo.

Omitir archivos existentes

Especifica que existe el mismo archivo en el equipo de destino. Como consecuencia, los archivos no se restauran desde el punto de recuperación.

6. (Opcional) Seleccione **Crear directorio raíz**.
7. Haga clic en **Siguiente**.

   Aparecerá la página **Configuración avanzada**.

Se especifican los detalles del equipo de destino.

Especificación de la configuración avanzada

Especifique la configuración avanzada para realizar una recuperación programada de los datos. La recuperación programada asegura que los datos se recuperen en la hora especificada incluso en su ausencia.

Siga estos pasos:

1. Establezca la fecha y la hora de inicio seleccionando una de las opciones siguientes:

   Ejecutar ahora

   Inicia la tarea de restauración de nivel de archivo tan pronto como se envíe la tarea.

   Establecer fecha y hora de inicio

   Inicia la tarea de restauración de nivel de archivo a la hora especificada después de haber enviado la tarea.

2. (Opcional) Seleccione la **Estimación del tamaño del archivo**.
3. (Opcional) Seleccione un script de la opción **Configuración de scripts anteriores/posteriores**.

   Estos scripts ejecutan comandos de script para realizar acciones antes del inicio de la tarea o cuando esta se finalice.

   Nota: Los campos **Configuración de scripts previos y posteriores** se rellenan solamente si ya se ha creado un archivo de script y se ha colocado en la siguiente ubicación:

   /opt/Arcserve/d2dserver/usr/prepost

   Nota: Para obtener más información acerca de cómo crear los scripts anteriores/posteriores, consulte *Gestión de scripts anteriores/posteriores para la automatización*.

4. Haga clic en **Siguiente**.

   Aparecerá la página **Resumen**.

   Se especifica la configuración avanzada.

(Opcional) Gestión de scripts anteriores/posteriores para la automatización

Los scripts previos/posteriores permiten ejecutar su propia lógica empresarial en las etapas específicas de una tarea en ejecución. Se puede especificar cuando se ejecutan los scripts en **Configuración previa/posterior** de los scripts del **Asistente de copia de seguridad** y el **Asistente de restauración** en la interfaz de usuario. Los scripts se pueden ejecutar en el servidor de copia de seguridad en función de la configuración.

La gestión de scripts anteriores/posteriores constituye un proceso de dos partes que consta de la creación del script anterior/posterior y la colocación de dicho script en la carpeta prepost.

Creación de scripts anteriores/posteriores

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un archivo de script mediante el uso de las variables de entorno en el lenguaje de generación de scripts preferido.

   Variables de entorno de scripts anteriores/posteriores

   Para crear un script, utilice las variables de entorno siguientes:

   D2D_JOBNAME

   Indica el nombre de la tarea.

   D2D_JOBID

   Identifica el ID de la tarea. El ID de la tarea es un número que se proporciona a la tarea cuando esta se ejecuta. Si se ejecuta la misma tarea de nuevo, obtendrá un nuevo número de tareas.

   D2D_TARGETNODE

   Identifica el nodo del cual se realiza copia de seguridad o que se restaura.

   D2D_JOBTYPE

   Identifica el tipo de tarea en ejecución. Los valores siguientes identifican la variable D2D_JOBTYPE:

   backup.full

   Identifica la tarea como copia de seguridad completa.

   backup.incremental

Identifica la tarea como copia de seguridad incremental.

backup.verify

Identifica la tarea como copia de seguridad de verificación.

restore.bmr

Identifica la tarea como una reconstrucción completa. Esta tarea es de restauración.

restore.file

Identifica la tarea como una restauración de nivel de archivo. Esta tarea es de restauración.

D2D_SESSIONLOCATION

Identifica la ubicación donde se almacenan los puntos de recuperación.

D2D_PREPOST_OUTPUT

Identifica un archivo temporal. El contenido de la primera línea del archivo temporal aparecerá en el registro de actividades.

D2D_JOBSTAGE

Indica la etapa de la tarea. Los valores siguientes identifican la variable D2D_ JOBSTAGE:

pre-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad antes de que se inicie la tarea.

post-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad después de que se complete la tarea.

pre-job-target

Identifica el script que se ejecuta en el equipo de destino antes de que se inicie la tarea.

post-job-target

Identifica el script que se ejecuta en el equipo de destino después de que se complete la tarea.

pre-snapshot

Identifica el script que se ejecuta en el equipo de destino antes de capturar la instantánea.

post-snapshot

Identifica el script que se ejecuta en el equipo de destino después de capturar la instantánea.

D2D_TARGETVOLUME

Identifica el volumen del cual se realiza copia de seguridad durante una tarea de copia de seguridad. Esta variable es aplicable para los scripts de instantáneas previas y posteriores para una tarea de copia de seguridad.

D2D_JOBRESULT

Identifica el resultado para un script de tarea de publicación. Los valores siguientes identifican la variable D2D_JOBRESULT:

success

Identifica el resultado como correcto.

fail

Identifica el resultado como incorrecto.

D2DSVR_HOME

Identifica la carpeta donde se instala el servidor de copia de seguridad. Esta variable es aplicable para los scripts que se ejecutan en el servidor de copia de seguridad.

El script se crea.

Nota: En todos los scripts, un valor de retorno de cero indica que se ha realizado correctamente, mientras que un valor de retorno distinto a cero indica que se han producido errores.

Colocación del script en la carpeta prepost y verificación

Todos los scripts previos/posteriores para un servidor de copia de seguridad se gestionan centralmente desde la carpeta prepost en la ubicación siguiente:

/opt/Arcserve/d2dserver/usr/prepost

Siga estos pasos:

1. Coloque el archivo en la siguiente ubicación del servidor de copia de seguridad:

   /opt/Arcserve/d2dserver/usr/prepost
2. Proporcione los permisos de ejecución al archivo de script.
3. Inicie sesión en la interfaz web del Agente de Arcserve Unified Data Protection para Linux.
4. Abra el **Asistente de copia de seguridad** o el **Asistente de restauración** y vaya a la ficha **Configuración avanzada**.

5. Seleccione el archivo de script en la lista desplegable **Configuración de scripts anteriores/posteriores** y, a continuación, envíe la tarea.
6. Haga clic en **Registro de actividad** y verifique que el script se ejecute en la tarea de copia de seguridad especificada.

   El script se ejecuta.

   Los scripts anteriores/posteriores se crean correctamente y se colocan en la carpeta prepost.

Creación y ejecución de la tarea de restauración

Cree y ejecute la tarea de restauración de modo que se pueda iniciar la recuperación de nivel de archivo. Verifique la información del punto de recuperación antes de restaurar los archivos. Si es necesario, se puede volver atrás y cambiar la configuración de restauración en el asistente.

Siga estos pasos:

1. Verifique los detalles de la restauración en la página **Resumen** del **Asistente de restauración**.
2. (Opcional) Seleccione **Anterior** para modificar la información que se ha introducido en cualquiera de las páginas del **Asistente de restauración**.
3. Introduzca un nombre de la tarea y haga clic en **Enviar**.

   El campo **Nombre de la tarea** tiene un nombre predeterminado inicialmente. Se puede introducir el nombre de la tarea nuevo que elija pero no se puede dejar vacío este campo.

   Se cierra el **Asistente de restauración**. Se puede ver el estado de la tarea en la ficha **Estado de la tarea**.

   Se ha creado y ejecutado la tarea de restauración correctamente.

Verificación de la restauración de archivos

Después de la finalización de la tarea de restauración, verifique que todos los archivos se restauren en el nodo de destino. Compruebe las fichas **Historial de tareas** y **Registro de actividad** en el panel **Estado** para controlar el progreso del proceso de restauración.

Siga estos pasos:

1. Vaya al equipo de destino en el que se han restaurado los datos.
2. Compruebe que los datos obligatorios del punto de recuperación se hayan restaurado.

   Los archivos se han verificado correctamente.

   La recuperación de nivel de archivo se ha realizado correctamente.

Cómo realizar la migración de la máquina virtual instantánea (del punto de recuperación de Linux) desde la nube al recurso local

Si se tiene el punto de recuperación de Linux en Amazon S3, se puede realizar una tarea de máquina virtual instantánea en AWS y, a continuación, migrar la máquina virtual instantánea desde AWS al recurso local.

Complete las tareas siguientes para realizar la migración de la máquina virtual instantánea:

- Revisión de los requisitos previos para la migración de la máquina virtual instantánea
- Realización de la migración de la máquina virtual instantánea desde la nube al recurso local

Revisión de los requisitos previos y consideraciones para la migración de la máquina virtual instantánea

Requisitos previos:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado para la restauración, si hay.
- Dispone de la cuenta de Amazon EC2 y Amazon S3.
- El servidor Samba está instalado en el servidor de copia de seguridad de Linux.

Consideraciones:

Esta función solo es compatible en el servidor de copia de seguridad de Linux que está instalado en RHEL, CentOS, Oracle Linux 7.x o SLES 12.x.

Realización de la migración de la máquina virtual instantánea desde la nube al recurso local

Se puede migrar la máquina virtual instantánea desde la nube al recurso local mediante tres procedimientos detallados. Haga clic en los vínculos de cada procedimiento y realice la migración completa.

- Para crear una máquina virtual instantánea en Amazon EC2, ejecute la máquina virtual instantánea desde el punto de recuperación de la máquina virtual de Linux en Amazon EC2.
- Instale el servidor de copia de seguridad de Linux en esta máquina virtual instantánea que se acaba de crear. Ejecute la copia de seguridad en la máquina virtual instantánea y realice la copia de seguridad en Amazon S3.
- Realice la copia de seguridad del equipo de Linux en Amazon S3.
- Ejecute la tarea de reconstrucción completa desde el punto de recuperación en Amazon S3 del que se ha realizado la copia de seguridad.

Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux

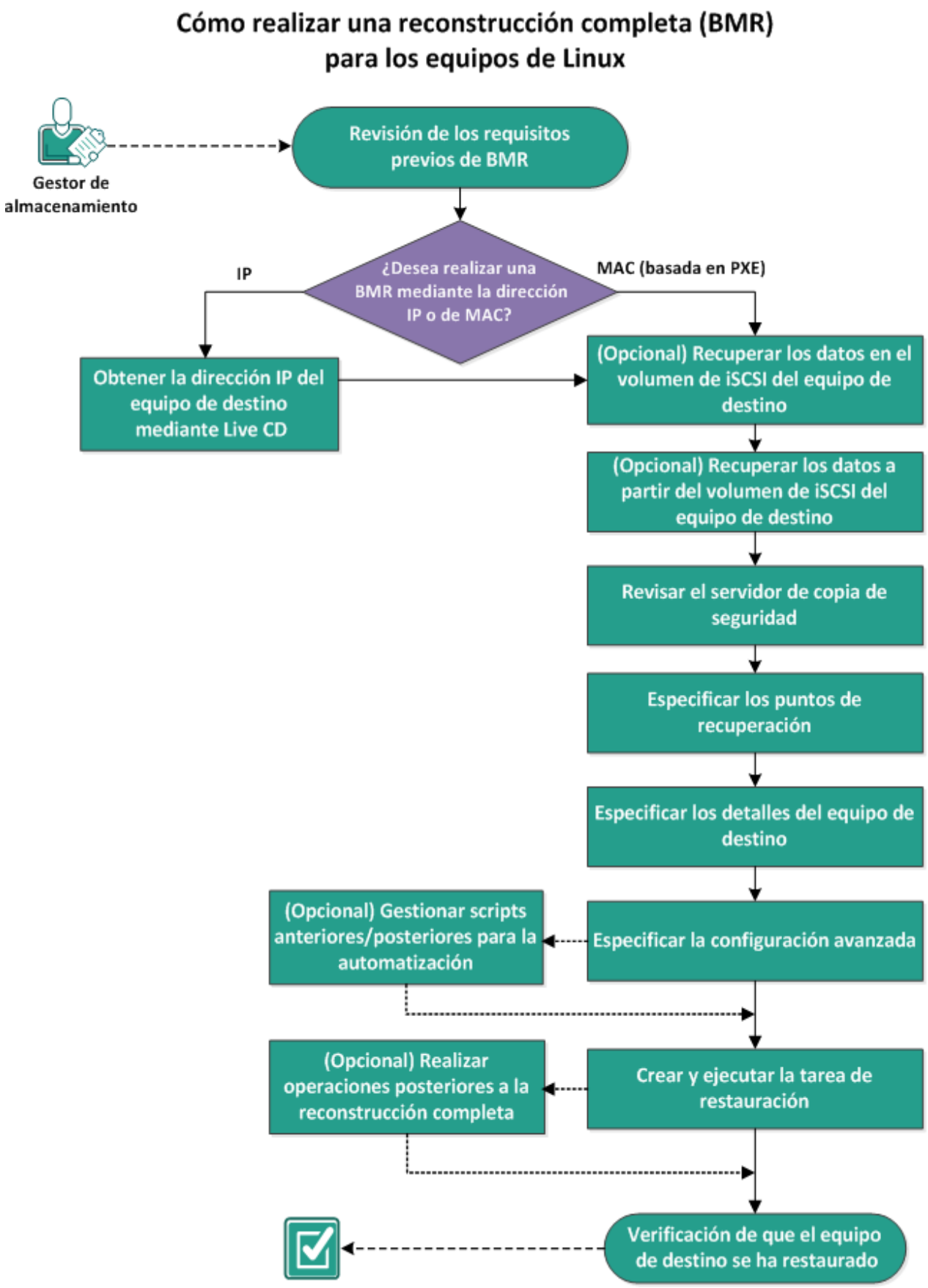
Una reconstrucción completa restaura las aplicaciones de software y el sistema operativo y recupera todos los datos de copia de seguridad. BMR es el proceso de restauración de un sistema informático *a partir de una reconstrucción completa*. La reconstrucción completa es un equipo sin ningún sistema operativo, controladores ni aplicaciones de software. Después de finalizar la restauración, el equipo de destino se reinicia automáticamente en el mismo entorno operativo que el nodo de origen de la copia de seguridad y se restaurarán todos los datos.

La reconstrucción completa es posible porque cuando se realiza una copia de seguridad de los datos, la copia de seguridad también captura la información relacionada con el sistema operativo, las aplicaciones instaladas y los controladores, entre otros.

Se puede realizar una reconstrucción completa mediante la dirección IP o la dirección de control de acceso a medios (MAC) del equipo de destino. Si se inicia el equipo de destino mediante el Live CD del Agente de Arcserve Unified Data Protection para Linux, se podrá obtener la dirección IP del equipo de destino.

Nota: El equipo se puede iniciar. Solo se configura una tarjeta NIC.

El diagrama siguiente muestra el proceso para realizar una reconstrucción completa:



Complete las tareas siguientes para realizar una reconstrucción completa:

- Revisión de los requisitos previos de BMR
- Obtención de la dirección IP del equipo de destino mediante Live CD
- (Opcional) Recuperación de los datos en el volumen de iSCSI del equipo de destino
- (Opcional) Recuperación de los datos a partir del volumen de iSCSI del equipo de destino
- Revisión del servidor de copia de seguridad
- Especificación de los puntos de recuperación
- Especificación de los detalles del equipo de destino
- Especificación de la configuración avanzada
- (Opcional) Gestión de scripts anteriores/posteriores para la automatización
- Creación y ejecución de la tarea de restauración
- (Opcional) Realización de operaciones posteriores a la reconstrucción completa
- Verificación de que el equipo de destino se ha restaurado

Revisión de los requisitos previos de BMR

Tenga en cuenta las opciones siguientes antes de realizar una reconstrucción completa:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado para la restauración, si hay.
- Tiene un equipo de destino válido para la reconstrucción completa.
- Se ha creado Live CD del Agente de Arcserve Unified Data Protection para Linux.
- Si desea realizar una reconstrucción completa mediante la dirección IP, se deberá obtener la dirección IP del equipo de destino mediante Live CD.
- Si desea realizar una reconstrucción completa de PXE mediante la dirección MAC, se debe disponer de la dirección MAC del equipo de destino.
- El punto de recuperación debe ser de la copia de seguridad basada en el agente de Linux.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Obtención de la dirección IP del equipo de destino mediante Live CD

Antes de realizar una reconstrucción completa mediante la dirección IP, es necesario obtener la dirección IP del equipo de destino. Un equipo de reconstrucción completa no tiene ninguna dirección IP al principio. Para obtener la dirección IP, se debe iniciar el equipo de reconstrucción completa utilizando el Live CD predeterminado, es decir, el Live CD del Agente de Arcserve Unified Data Protection para Linux, o el Live CD basado en CentOS. Después de obtener la dirección IP del equipo de destino, se puede configurar la IP estática de dicho equipo.

Siga estos pasos:

1. Inserte el Live CD o monte el archivo .iso del Live CD en la unidad de CD-ROM del nodo de destino.
2. Inicie el equipo de destino desde el CD-ROM.

   El equipo de destino se inicia en el entorno del Live CD del Agente de Arcserve Unified Data Protection para Linux. En la pantalla, aparece la dirección IP del equipo de destino.
3. Para configurar la IP estática del equipo de destino utilizando el Live CD predeterminado, siga estos pasos:
   a. En la pantalla del equipo de destino, pulse Intro para introducir el entorno de la shell.
   b. Ejecute el siguiente comando para configurar la IP estática:

      ifconfig <nombre de la NIC> <dirección IP estática> netmask <máscara de red>

      route add default gw <dirección IP de la puerta de enlace> <nombre de la NIC>

   Nota: El nombre de la tarjeta de interfaz de red (NIC) dependerá del hardware. Por ejemplo, los nombres de NIC habituales son eth0 o em0.
4. Para configurar la IP estática del equipo de destino utilizando el Live CD basado en CentOS, siga estos pasos:
   a. Abra una ventana de terminal en el equipo de destino haciendo clic en Aplicaciones, Herramientas del sistema, Terminal.
   b. Ejecute los siguientes comandos:

      sudo ifconfig <nombre de la NIC> <dirección IP estática> netmask <máscara de red>

      sudo route add default gw <dirección IP de la puerta de enlace> <nombre de la NIC>

Se configura la IP estática.

Se obtiene la dirección IP del equipo de destino.

Importante: Mantenga un registro de esta dirección IP puesto que se utilizará en el **Asistente de restauración** cuando se deban especificar los detalles del equipo de destino.

(Opcional) Recuperación de los datos en el volumen de iSCSI del equipo de destino

Se puede integrar el volumen de iSCSI en el equipo de destino y convertir este volumen en una parte del equipo de destino. A continuación se pueden restaurar datos en el volumen de iSCSI del equipo de destino. Si hace esto, se podrán gestionar datos y transferirlos a una red.

Importante: Cuando se integre el volumen de iSCSI con el equipo de destino, perderá todos los datos existentes del volumen de iSCSI.

Siga estos pasos:

1. Inserte el Live CD del Agente de Arcserve Unified Data Protection para Linux o monte el archivo .iso del Live CD del Agente de Arcserve Unified Data Protection para Linux en la unidad de CD-ROM del equipo de destino.
2. Inicie el equipo de destino desde el CD-ROM.

   El equipo de destino se inicia en el entorno del Live CD del Agente de Arcserve Unified Data Protection para Linux. En la pantalla, aparece la dirección IP del equipo de destino.
3. Introduzca el entorno de shell del equipo de destino.
4. Ejecute el comando siguiente para iniciar el daemon de iniciador iSCSI:

   /etc/init.d/iscsid start
5. Ejecute un script de detección para detectar el host de destino de iSCSI.

   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>

   El valor del puerto predeterminado del host de destino de iSCSI es 3260.
6. Tome nota del nombre completo de iSCSI (IQN) del host de destino de iSCSI que ha encontrado el script de detección antes de realizar el registro manual en el destino detectado.
7. Enumere el dispositivo de bloqueo disponible del nodo de destino.

   #fdisk -l
8. Inicie sesión en el destino detectado.

   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l

   Se puede ver un dispositivo de bloqueo en el directorio /dev del nodo de destino.
9. Ejecute el comando siguiente para obtener el nuevo nombre del dispositivo:

#fdisk -l

Se puede ver otro dispositivo llamado /dev/sd<x> en el nodo de destino.

El volumen iSCSI se integra con el volumen de destino.

(Opcional) Recuperación de los datos a partir del volumen de iSCSI del equipo de destino

Si se han almacenado sus datos en un volumen de destino de iSCSI, se puede conectar al volumen de iSCSI y recuperar datos. El volumen de iSCSI permite gestionar datos y transferirlos a una red.

Siga estos pasos:

1. Inserte el Live CD del Agente de Arcserve Unified Data Protection para Linux o monte el archivo .iso del Live CD del Agente de Arcserve Unified Data Protection para Linux en la unidad de CD-ROM del equipo de destino.
2. Inicie el equipo de destino desde el CD-ROM.

   El equipo de destino se inicia en el entorno del Live CD del Agente de Arcserve Unified Data Protection para Linux. En la pantalla, aparece la dirección IP del equipo de destino.
3. Introduzca el entorno de shell del equipo de destino.
4. Ejecute el comando siguiente para iniciar el daemon de iniciador iSCSI:

   /etc/init.d/iscsid start
5. Ejecute un script de detección para detectar el host de destino de iSCSI.

   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>

   El valor del puerto predeterminado del host de destino de iSCSI es 3260.
6. Tome nota del nombre completo de iSCSI (IQN) del host de destino de iSCSI que ha encontrado el script de detección antes de realizar el registro manual en el destino detectado.
7. Enumere el dispositivo de bloqueo disponible del nodo de destino.

   #fdisk -l
8. Inicie sesión en el destino detectado.

   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l

   Se puede ver un dispositivo de bloqueo en el directorio /dev del nodo de destino.
9. Ejecute el comando siguiente para obtener el nuevo nombre del dispositivo:

   #fdisk -l

   Se puede ver otro dispositivo llamado /dev/sd<x> en el nodo de destino.

Por ejemplo, tenga en cuenta que el nombre del dispositivo es /dev/sdc. Este nombre de dispositivo se utilizará para crear una partición y un sistema de archivos en los pasos siguientes.

10. Monte el volumen de iSCSI mediante los comandos siguientes:

    # mkdir /iscsi

    # mount /dev/sdc1 /iscsi

    Nota: Cuando se especifique la ubicación de la sesión en el asistente de restauración, será necesario seleccionar Local e introducir la ruta /iscsi.

    Ejemplo: <ruta>/iscsi

    El equipo de destino se puede conectar ahora al volumen de iSCSI y podrá recuperar datos del volumen de iSCSI.

Revisión del servidor de copia de seguridad

Cuando se abre el **Asistente de restauración**, revise el servidor de copia de seguridad donde se desea realizar la operación de restauración.

Siga estos pasos:

1. Acceda al asistente de restauración de una de las formas siguientes:

   Desde Arcserve UDP:

   a. Inicie sesión en el Arcserve UDP.

   b. Haga clic en la ficha **recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos de agregados en el panel central.

   d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   e. Haga clic en **Restaurar** del menú desplegable **Acción**.

      Se abre la interfaz web del Agente de Arcserve Unified Data Protection para Linux. Se muestra el cuadro de diálogo de selección del tipo de restauración en la interfaz de usuario del agente.

   f. Seleccione el tipo de restauración y haga clic en **Aceptar**.

      Nota: Se inicia sesión automáticamente en el nodo del agente y el **Asistente de restauración** se abre desde el nodo del agente.

   En el Agente de Arcserve Unified Data Protection para Linux:

   a. Abra la interfaz web del Agente de Arcserve Unified Data Protection para Linux.

      Nota: Durante la instalación del Agente de Arcserve Unified Data Protection para Linux, recibirá la dirección URL para acceder al servidor y gestionarlo. Inicie sesión en el Agente de Arcserve Unified Data Protection para Linux.

   b. Haga clic en **Restaurar** en el menú **Asistente** y seleccione **Reconstrucción completa (BMR)**.

      Se abre la página **Servidor de copia de seguridad** del **Asistente de restauración - BMR**.

2. Seleccione el servidor en la lista desplegable **Servidor de copia de seguridad** de la página **Servidor de copia de seguridad**.

   No se puede seleccionar ninguna opción en la lista desplegable **Servidor de copia de seguridad**.

3. Haga clic en **Siguiente**.

Aparece la página **Puntos de recuperación** del **Asistente de restauración - Reconstrucción completa (BMR)**.

Se especifica el servidor de copia de seguridad.

Especificación de los puntos de recuperación

Cada vez que se realiza una copia de seguridad correcta, se creará un punto de recuperación. Especifique la información del punto de recuperación en el **Asistente de restauración** para que se puedan recuperar los datos exactos que desee. Se pueden restaurar archivos específicos o todos los archivos en función de sus requisitos.

Importante: Para realizar una reconstrucción completa de un punto de recuperación, el volumen de raíz y el volumen de inicio deberán estar presentes en el punto de recuperación.

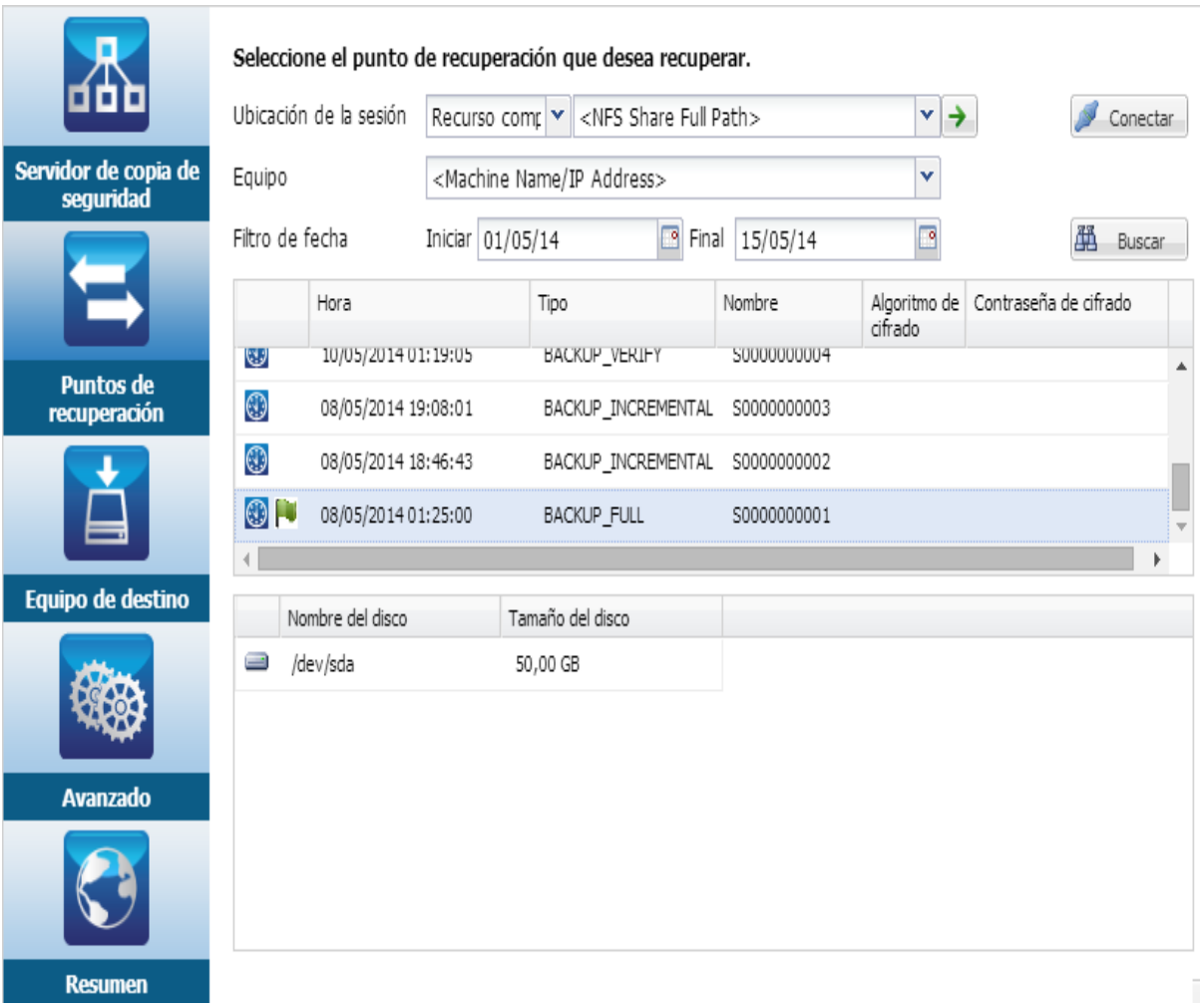
Siga estos pasos:

1. Realice uno de los pasos siguientes en función del almacenamiento de la copia de seguridad.
   - Realice los pasos siguientes para acceder a los puntos de recuperación si los puntos de recuperación se almacenan en un dispositivo móvil:
     a. Inicie el equipo de destino mediante Live CD.
     b. Inicie sesión en la interfaz web del Agente de Arcserve Unified Data Protection para Linux desde el Live CD.
     c. Abra el **Asistente de reconstrucción completa**.
     d. Vaya a la página **Puntos de recuperación**.
     e. Seleccione **Local** como la **Ubicación de la sesión** en la página **Puntos de recuperación** del **Asistente de reconstrucción completa**.
   - Realice los pasos siguientes si la ubicación de la sesión es un recurso compartido de NFS o de CIFS:
     a. Seleccione una sesión en la lista desplegable **Ubicación de la sesión** e introduzca la ruta completa del recurso compartido.

        Por ejemplo, tenga en cuenta la ubicación de la sesión como un recurso compartido de NFS, xxx.xxx.xxx.xxx como la dirección IP del recurso compartido de NFS y el nombre de la carpeta debe ser *Datos.* Introducirá xxx.xxx.xxx.xxx:/Data como ubicación compartida de NFS.

        Nota: Si los datos de la copia de seguridad se almacenan en Origen local, deberá convertirse primero el nodo de origen en un servidor de

NFS y, a continuación, compartir la ubicación de la sesión.



2. Haga clic en **Conectar**.

   Todos los nodos de los cuales se ha realizado copia de seguridad en esta ubicación aparecen en la lista desplegable **Equipo.**

3. Seleccione el nodo que desee restaurar en la lista desplegable **Equipo.**

   Aparecen todos los puntos de recuperación del nodo seleccionado.

4. Aplique el filtro de fecha para que se muestren los puntos de recuperación que se han generado entre la fecha especificada y haga clic en **Buscar**.

   Valor predeterminado: Las dos últimas semanas.

   Se muestran todos los puntos de recuperación disponibles entre las fechas especificadas.

5. Seleccione el punto de recuperación que desee restaurar y haga clic en **Siguiente**.

   Aparecerá la página **Equipo de destino**.

   Se especifica el punto de recuperación.

Especificación de los detalles del equipo de destino

Especifique los detalles del equipo de destino para que los datos se restauren en el equipo. Un equipo de destino es un equipo de reconstrucción completa donde se realizará una reconstrucción completa. Si se realiza una restauración mediante la dirección IP, será necesaria la dirección IP del equipo de destino que se ha registrado previamente al inicio de este proceso. Si se realiza una restauración mediante una dirección de control de acceso a medios (MAC), será necesaria la dirección de MAC del equipo de destino.

Siga estos pasos:

1. Introduzca la dirección MAC o la dirección IP del equipo de destino en el campo Dirección MAC/IP.
2. Introduzca un nombre en el campo Nombre del host.

   El equipo de destino utilizará este nombre como nombre del host después de que el proceso de restauración finalice.
3. Seleccione una de las opciones siguientes como red:

   DHCP

   Se configura la dirección IP automáticamente. Se trata de la opción predeterminada. Utilice esta opción si dispone de un servidor de protocolo de configuración dinámica de host (DHCP) para realizar la restauración con la red de DHCP.

   IP estática

   Se configura la dirección IP manualmente. Si se selecciona esta opción, introduzca la **Dirección IP**, la **Máscara de subred** y la **Puerta de enlace predeterminada** del equipo de destino.

   Importante: Asegúrese de que ningún otro equipo utilice la IP estática en la red durante el proceso de restauración.
4. (Opcional) Seleccione la opción **Activar la reconstrucción completa instantánea** para poder utilizar el equipo de destino instantáneamente.

   Cuando se activa esta opción, el Agente de Arcserve Unified Data Protection para Linux primero recupera todos los datos necesarios requeridos para iniciar el equipo. Después de que se inicie el equipo de destino, se recuperarán los datos restantes. La conexión de red debe estar disponible constantemente durante la reconstrucción completa instantánea.

   Ejemplo: si se tienen 100 GB de datos, se desea realizar una reconstrucción completa y *no* se selecciona esta opción, primero se recuperarán los 100 GB de datos y,

a continuación, se podrá utilizar el equipo de destino. Sin embargo, solo se necesita alrededor de 1 GB de datos para iniciar el equipo. Cuando se activa esta opción, primero se recuperan los datos de 1 GB necesarios para poder iniciar y utilizar el equipo. Una vez iniciado el equipo, se recuperan automáticamente los 99 GB de datos restantes.

Nota: Los datos necesarios para iniciar el equipo dependen de la configuración del sistema operativo. También se puede pausar o reanudar la recuperación automática de los datos si la opción **No recuperar los datos automáticamente después de que se inicie el equipo** no está seleccionada.

5. (Opcional) Seleccione la opción **No recuperar los datos automáticamente después de que se inicie el equipo** para detener la recuperación automática de los datos cuando se inicia el equipo de destino.

   Cuando se selecciona la opción **Activar la reconstrucción completa instantánea**, el comportamiento predeterminado es primero recuperar los datos necesarios e iniciar el equipo. Después de iniciar el equipo, los datos restantes se recuperan automáticamente. Si se actualizan los datos de origen durante la recuperación, seleccionando esta opción se recuperarán los datos hasta el punto anterior a su actualización.

6. Haga clic en **Siguiente**.

   Aparecerá la página **Configuración avanzada**.

   Se especifican los detalles del equipo de destino.

Especificación de la configuración avanzada

Especifique la configuración avanzada para realizar una reconstrucción completa programada de los datos. La reconstrucción completa programada garantiza que los datos se recuperen en la hora especificada incluso en su ausencia.

Siga estos pasos:

1. Establezca la fecha y la hora de inicio seleccionando una de las opciones siguientes:

   Ejecutar ahora

   Inicia la tarea de restauración en cuanto se envía la tarea.

   Establecer fecha y hora de inicio

   Inicia la tarea de restauración en la hora especificada después de haber enviado la tarea.

2. (Opcional) Seleccione un script de la opción **Configuración de scripts anteriores/posteriores** para el servidor de copia de seguridad y para el equipo de destino.

   Estos scripts ejecutan comandos de script para realizar acciones antes del inicio de la tarea o cuando esta se finalice.

   Nota: Los campos **Configuración de scripts previos y posteriores** se rellenan solamente si ya se ha creado un archivo de script y se ha colocado en la siguiente ubicación:

   /opt/Arcserve/d2dserver/usr/prepost

   Nota: Para obtener más información acerca de cómo crear los scripts anteriores/posteriores, consulte *Gestión de scripts anteriores/posteriores para la automatización*.

3. (Opcional) Seleccione **Mostrar más valores de configuración** para mostrar más valores de configuración para la reconstrucción completa.

4. (Opcional) Restablezca la contraseña del nombre de usuario especificado para el equipo de destino recuperado.

5. (Opcional) Introduzca la ruta completa de la ubicación de almacenamiento de copia de seguridad de los puntos de recuperación en **Acceso local del punto de recuperación**.

6. (Opcional) Introduzca el nombre completo del disco en el campo **Discos** para excluir la participación de los discos en el equipo de destino durante el proceso de recuperación.

7. (Opcional) Seleccione **Activar Wake-on-LAN** si está realizando una reconstrucción completa del protocolo Medio de ejecución anterior al inicio (PXE).

   Nota: La opción **Activar Wake-on-LAN** es aplicable solamente para equipos físicos. Se debe garantizar que se haya activado la configuración de Wake-on-LAN en la configuración de BIOS del equipo físico.

8. (Opcional) Seleccione la opción **Reiniciar** para reiniciar automáticamente el nodo de destino después de finalizar la reconstrucción completa.

9. Haga clic en **Siguiente**.

   Aparecerá la página **Resumen**.

   Se especifica la configuración avanzada.

(Opcional) Gestión de scripts anteriores/posteriores para la automatización

Los scripts previos/posteriores permiten ejecutar su propia lógica empresarial en las etapas específicas de una tarea en ejecución. Se puede especificar cuando se ejecutan los scripts en **Configuración previa/posterior** de los scripts del **Asistente de copia de seguridad** y el **Asistente de restauración** en la interfaz de usuario. Los scripts se pueden ejecutar en el servidor de copia de seguridad en función de la configuración.

La gestión de scripts anteriores/posteriores constituye un proceso de dos partes que consta de la creación del script anterior/posterior y la colocación de dicho script en la carpeta prepost.

Creación de scripts anteriores/posteriores

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un archivo de script mediante el uso de las variables de entorno en el lenguaje de generación de scripts preferido.

   Variables de entorno de scripts anteriores/posteriores

   Para crear un script, utilice las variables de entorno siguientes:

   D2D_JOBNAME

   Indica el nombre de la tarea.

   D2D_JOBID

   Identifica el ID de la tarea. El ID de la tarea es un número que se proporciona a la tarea cuando esta se ejecuta. Si se ejecuta la misma tarea de nuevo, obtendrá un nuevo número de tareas.

   D2D_TARGETNODE

   Identifica el nodo del cual se realiza copia de seguridad o que se restaura.

   D2D_JOBTYPE

   Identifica el tipo de tarea en ejecución. Los valores siguientes identifican la variable D2D_JOBTYPE:

   backup.full

   Identifica la tarea como copia de seguridad completa.

   backup.incremental

Identifica la tarea como copia de seguridad incremental.

backup.verify

Identifica la tarea como copia de seguridad de verificación.

restore.bmr

Identifica la tarea como una reconstrucción completa. Esta tarea es de restauración.

restore.file

Identifica la tarea como una restauración de nivel de archivo. Esta tarea es de restauración.

D2D_SESSIONLOCATION

Identifica la ubicación donde se almacenan los puntos de recuperación.

D2D_PREPOST_OUTPUT

Identifica un archivo temporal. El contenido de la primera línea del archivo temporal aparecerá en el registro de actividades.

D2D_JOBSTAGE

Indica la etapa de la tarea. Los valores siguientes identifican la variable D2D_ JOBSTAGE:

pre-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad antes de que se inicie la tarea.

post-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad después de que se complete la tarea.

pre-job-target

Identifica el script que se ejecuta en el equipo de destino antes de que se inicie la tarea.

post-job-target

Identifica el script que se ejecuta en el equipo de destino después de que se complete la tarea.

pre-snapshot

Identifica el script que se ejecuta en el equipo de destino antes de capturar la instantánea.

post-snapshot

Identifica el script que se ejecuta en el equipo de destino después de capturar la instantánea.

D2D_TARGETVOLUME

Identifica el volumen del cual se realiza copia de seguridad durante una tarea de copia de seguridad. Esta variable es aplicable para los scripts de instantáneas previas y posteriores para una tarea de copia de seguridad.

D2D_JOBRESULT

Identifica el resultado para un script de tarea de publicación. Los valores siguientes identifican la variable D2D_JOBRESULT:

success

Identifica el resultado como correcto.

fail

Identifica el resultado como incorrecto.

D2DSVR_HOME

Identifica la carpeta donde se instala el servidor de copia de seguridad. Esta variable es aplicable para los scripts que se ejecutan en el servidor de copia de seguridad.

El script se crea.

Nota: En todos los scripts, un valor de retorno de cero indica que se ha realizado correctamente, mientras que un valor de retorno distinto a cero indica que se han producido errores.

Colocación del script en la carpeta prepost y verificación

Todos los scripts previos/posteriores para un servidor de copia de seguridad se gestionan centralmente desde la carpeta prepost en la ubicación siguiente:

/opt/Arcserve/d2dserver/usr/prepost

Siga estos pasos:

1. Coloque el archivo en la siguiente ubicación del servidor de copia de seguridad:

   /opt/Arcserve/d2dserver/usr/prepost
2. Proporcione los permisos de ejecución al archivo de script.
3. Inicie sesión en la interfaz web del Agente de Arcserve Unified Data Protection para Linux.
4. Abra el **Asistente de copia de seguridad** o el **Asistente de restauración** y vaya a la ficha **Configuración avanzada**.

5. Seleccione el archivo de script en la lista desplegable **Configuración de scripts anteriores/posteriores** y, a continuación, envíe la tarea.
6. Haga clic en **Registro de actividad** y verifique que el script se ejecute en la tarea de copia de seguridad especificada.

   El script se ejecuta.

   Los scripts anteriores/posteriores se crean correctamente y se colocan en la carpeta prepost.

Creación y ejecución de la tarea de restauración

Cree y ejecute la tarea de restauración para que se pueda iniciar el proceso de reconstrucción completa. Antes de realizar una reconstrucción completa, verifique la información del punto de recuperación. Si es necesario, se puede volver y cambiar los valores de configuración de restauración.

Siga estos pasos:

1. Verifique los detalles de la restauración en la página **Resumen** del **Asistente de restauración**.
2. (Opcional) Seleccione **Anterior** para modificar la configuración de restauración en cualquiera de las páginas del **Asistente de restauración**.
3. Introduzca un nombre de la tarea y haga clic en **Enviar**.

   El campo **Nombre de la tarea** tiene un nombre predeterminado inicialmente. Se puede introducir el nombre de la tarea nuevo que elija pero no se puede dejar vacío este campo.

   Se cierra el **Asistente de restauración**. Se puede ver la tarea en la ficha **Estado de la tarea.** Si se utiliza la dirección IP para la reconstrucción completa, el equipo de destino se reiniciará automáticamente en el mismo sistema operativo que el origen de la copia de seguridad después de que el proceso de BMR finalice.

   Si se utiliza la dirección de MAC para la reconstrucción completa, el estado en la ficha **Estado de la tarea** se cambia a *Esperando el inicio del nodo de destino*.
4. (Opcional) Para realizar el proceso de BMR mediante la dirección de MAC, inicie el equipo de destino cuando vea el mensaje *Esperando el inicio del nodo de destino* en la ficha **Estado de la tarea.**

   Nota: Si el equipo de destino se inicia antes de enviar la tarea de restauración, se deberá reiniciar el equipo de destino. Asegúrese de que se configure BIOS para realizar un inicio desde la red.

   El estado en la columna **Estado de la tarea** cambia a **Restaurando el volumen**. Esto indica que la restauración está en curso. Después de finalizar la tarea de restauración, el equipo de destino se reiniciará automáticamente con el mismo sistema operativo que el origen de copia de seguridad.

   Se ha creado y ejecutado la tarea de restauración correctamente.

(Opcional) Realización de operaciones posteriores a la reconstrucción completa

Los temas siguientes son valores de configuración opcionales que es posible que deba ejecutar después de una reconstrucción completa:

Configuración de X Windows

Cuando se realiza una reconstrucción completa en un hardware distinto, X Windows del sistema operativo restaurado no funcionará correctamente y el nodo de destino mostrará un cuadro de diálogo de error. El cuadro de diálogo de error aparece porque la configuración de visualización ha cambiado. Para resolver este error, siga las instrucciones en el cuadro de diálogo de error para configurar la tarjeta gráfica. Después de esto, se podrá ver X Windows y la IU de escritorio.

Configure el nombre del dominio completamente calificado del sistema (FQDN)

Cuando se necesita un FQDN, se deberá configurar el FQDN. El proceso de reconstrucción completa no configura el FQDN automáticamente.

Número máximo de caracteres para FQDN: 63

Siga estos pasos para configurar el FQDN:

1. Edite el archivo */etc/hosts* y proporcione la dirección IP, el nombre FQDN y el nombre del servidor.

   #vi /etc/hosts

   ip_sistema nombreservidor.nombredominio.com nombreservidor

2. Reinicie el servicio de red.

   #/etc/init.d/network restart

3. Verifique el nombre de host y el nombre de FQDN.

   #hostname

   servername

   #hostname -f

   servername.domainname.com

   Se configura el FQDN.

Extensión del volumen de datos después de una reconstrucción completa en discos distintos

Cuando se realiza una reconstrucción completa en un disco mayor que el disco del nodo original, habrá una parte de espacio en disco que no se utiliza. La

operación de reconstrucción completa no procesa automáticamente el espacio en disco sin utilizar. Se puede formatear el espacio en disco a una partición separada o cambiar de tamaño la partición existente con el espacio en disco sin utilizar. El volumen que se desea cambiar de tamaño debe estar sin utilizar, de modo que se debe evitar cambiar de tamaño un volumen del sistema. En esta sección, nos centraremos en cómo extender un volumen de datos con el espacio en disco sin utilizar.

Nota: Para evitar la pérdida de datos, cambie el tamaño de los volúmenes inmediatamente después del proceso de reconstrucción completa. Se puede realizar también una copia de seguridad del nodo antes de iniciar la tarea de cambio de tamaño del volumen.

Cuando el equipo de destino se reinicie correctamente después de la reconstrucción completa, se podrá extender el volumen de datos.

Volumen de partición sin formato

Por ejemplo, se restaura un disco de 2 GB de la sesión en otro de 16 GB denominado */dev/sdb* con solamente una partición. La partición sin formato */dev/sdb1* se monta directamente en el directorio */data*.

Este ejemplo se utiliza para explicar el procedimiento de extensión del volumen de partición sin formato.

Lleve a cabo los pasos siguientes:

1. Compruebe el estado del volumen /dev/sdb1.

   # df –h /dev/sdb1

   /dev/sdb1 2.0G 40M 1.9G 3% /data

2. Desmonte el volumen /dev/sdb1.

   # umount /data

3. Cambie de tamaño /dev/sdb1 para ocupar el espacio en disco entero mediante el comando fdisk.

   Para realizar esta operación, primero suprima la partición existente y, a continuación, vuélvala a crear con el mismo número de sector de inicio. El mismo número de sector de inicio es responsable de evitar la pérdida de datos.

   # fdisk -u /dev/sdb

   Comando (m para obtener ayuda): p

   Disco /dev/sdb: 17,1 GB, 17179869184 bytes

255 cabezales, 63 sectores/pista, 2088 cilindros, 33554432 sectores totales

*Unidades = sectores de 1 * 512 = 512 bytes*

Device Boot Start End Blocks Id System

/dev/sdb1 63 4192964 2096451 83 Linux

Command (m for help): d

Partición seleccionada 1

Comando (m para obtener ayuda): n

Acción de comando

e extended

p primary partition (1-4)

p

Número de partición (1-4): 1

Primer sector (63-33554431, valor predeterminado 63):

Mediante el valor predeterminado 63

Último sector o +size o +sizeM o +sizeK (63-33554431, valor predeterminado 33554431):

Mediante el valor predeterminado 33554431

Comando (m para obtener ayuda): p

Disco /dev/sdb: 17,1 GB, 17179869184 bytes

255 cabezales, 63 sectores/pista, 2088 cilindros, 33554432 sectores totales

*Unidades = sectores de 1 * 512 = 512 bytes*

Device Boot Start End Blocks Id System

/dev/sdb1 63 33554431 16777184+ 83 Linux

Comando (m para obtener ayuda): w

La partición cambia al mismo número de sector de inicio que la partición original y el número de sector final es 33554431.

4. Cambie de tamaño el volumen mediante el comando resize2fs. Si es necesario, ejecute primero el comando e2fsck.

   # e2fsck -f /dev/sdb1

   # resize2fs /dev/sdb1

5. Monte el volumen en el punto de montaje y compruebe el estado del volumen de nuevo.

   # mount /dev/sdb1 /data

   # df –h /dev/sdb1

   /dev/sdb1 16G 43M 16G 1% /data

   El volumen se extiende a 16 GB y está listo para el uso.

Volumen de LVM:

Por ejemplo, se restaura un disco de 8 GB de la sesión en otro de 16 GB denominado */dev/sdc* con una partición solamente. La partición sin formato */dev/sdc1* se utiliza como único volumen físico del /volumen lógico de LVM */dev/mapper/VGTest-LVTest* cuyo punto de montaje es */lvm*.

Este ejemplo se utiliza para explicar el procedimiento de extensión del volumen de LVM.

Lleve a cabo los pasos siguientes:

1. Compruebe el estado del volumen /dev/mapper/VGTest-LVTest.

   # lvdisplay –m /dev/mapper/VGTest-LVTest

   ---Volumen lógico---

   LV Name /dev/VGTest/LVTest

   VG Name VGTest

   LV UUID udoBIx-XKBS-1Wky-3FVQ-mxMf-FayO-tpfPl8

   LV Write Access read/write

   LV Status available

   # open 1

   LV Size 7.88 GB

   Current LE 2018

   Segments 1

   Allocation inherit

   Read ahead sectors 0

   Block device 253:2

   --Segmentos---

   Extensión lógica 0 a 2017:

   Type linear

Physical volume /dev/sdc1

Physical extents 0 to 2017

El volumen físico es */dev/sdc1*, el grupo del volumen es *VGTest* y el volumen lógico es */dev/VGTest/LVTest o /dev/mapper/VGTest-LVTest.*

2. Desmonte el volumen /dev/mapper/VGTest-LVTest.

   # umount /lvm

3. Desactive el grupo del volumen en el cual se encuentra el volumen físico /dev/sdc1.

   # vgchange -a n VGTest

4. Cree una partición para ocupar el espacio en disco sin utilizar mediante el comando fdisk.

   # fdisk -u /dev/sdc

   Comando (m para obtener ayuda): p

   Disco /dev/sdc: 17,1 GB, 17179869184 bytes

   255 cabezales, 63 sectores/pista, 2088 cilindros, 33554432 sectores totales

   *Unidades = sectores de 1 * 512 = 512 bytes*

   Device Boot Start End Blocks Id System

   /dev/sdc1 63 16777215 8388576+ 83 Linux

   Comando (m para obtener ayuda): n

   Acción de comando

   e extended

   p primary partition (1-4)

   p

   Número de partición (1-4): 2

   Primer sector (16777216-33554431, valor predeterminado 16777216):

   Mediante el valor predeterminado 16777216

   Último sector o +size o +sizeM o +sizeK (16777216-33554431, valor predeterminado 33554431):

   Mediante el valor predeterminado 33554431

   Comando (m para obtener ayuda): p

   Disco /dev/sdc: 17,1 GB, 17179869184 bytes

255 cabezales, 63 sectores/pista, 2088 cilindros, 33554432 sectores totales

*Unidades = sectores de 1 * 512 = 512 bytes*

Device Boot Start End Blocks Id System

/dev/sdc1 63 16777215 8388576+ 83 Linux

/dev/sdc2 16777216 33554431 8388608 83 Linux

Comando (m para obtener ayuda): w

Se crea la partición /dev/sdc2.

5. Cree un nuevo volumen físico.

   # pvcreate /dev/sdc2

6. Extienda el tamaño del grupo del volumen.

   # vgextend VGTest /dev/sdc2

7. Active el grupo del volumen que ya se ha desactivado.

   # vgchange -a y VGTest

8. Extienda el tamaño del volumen lógico mediante el comando lvextend.

   # lvextend -L +8G /dev/VGTest/LVTest

9. Cambie de tamaño el volumen mediante el comando resize2fs. Si es necesario, ejecute primero el comando e2fsck.

   # e2fsck -f /dev/mapper/VGTest-LVTest

   # resize2fs /dev/mapper/VGTest-LVTest

10. Monte el volumen en el punto de montaje y compruebe el estado del volumen de nuevo.

    # mount /dev/mapper/VGTest-LVTest /lvm

    # lvdisplay -m /dev/mapper/VGTest-LVTest

    ---Volumen lógico---

    LV Name /dev/VGTest/LVTest

    VG Name VGTest

    LV UUID GTP0a1-kUL7-WUL8-bpbM-9eTR-SVzl-WgA11h

    LV Write Access read/write

    LV Status available

    # open 0

LV Size 15.88 GB

Current LE 4066

Segments 2

Allocation inherit

Read ahead sectors 0

Block device 253:2

---Segmentos---

Extensión lógica 0 a 2046:

Type linear

Physical volume /dev/sdc1

Physical extents 0 to 2046

Extensión lógica 2047 a 4065:

Type linear

Physical volume /dev/sdc2

Physical extents 0 to 2018

El volumen LVM se extiende a 16 GB y está listo para el uso.

Verificación de que el nodo de destino se ha restaurado

Después de finalizar la tarea de restauración, verifique que el nodo de destino se restaure con los datos relevantes.

Siga estos pasos:

1. Vaya al equipo de destino que se ha restaurado.
2. Verifique que el equipo de destino tiene toda la información de copia de seguridad.

   El equipo de destino se ha verificado correctamente.

   La reconstrucción completa se ha ejecutado correctamente en los equipos de Linux.

Cómo realizar una reconstrucción completa (BMR) de la migración para los equipos de Linux

Una reconstrucción completa de la migración es un proceso de dos partes donde primero se realiza la restauración de los datos en un equipo temporal y, a continuación, se restaurarán al equipo real. Una reconstrucción completa con la opción de reconstrucción completa instantánea activada permite recuperar datos en un equipo temporal. Se puede utilizar el equipo temporal hasta que el equipo real esté listo. Cuando se tiene el equipo real, una reconstrucción completa de la migración permite migrar los datos desde el equipo temporal al equipo real. Al realizar una reconstrucción completa de la migración, los datos que se crean en el equipo temporal se migrarán al equipo real.

Nota: Se puede realizar la reconstrucción completa de la migración con solo una copia de seguridad basada en el agente. Una copia de seguridad sin agente no es compatible con la reconstrucción completa de la migración.

Se puede realizar una reconstrucción completa mediante la dirección IP o la dirección de control de acceso a medios (MAC) del equipo de destino. Si se inicia el equipo de destino mediante el Live CD del Agente de Arcserve Unified Data Protection para Linux, se podrá obtener la dirección IP del equipo de destino.

Nota: El equipo se puede iniciar. Solo se configura una tarjeta NIC.

Complete las tareas siguientes para realizar una reconstrucción completa de la migración:

- Revisión de los requisitos previos para la reconstrucción completa de migración
- Realización de una reconstrucción completa en el equipo temporal
- Realización de una reconstrucción completa de la migración
- Verificación de que el equipo de destino se ha restaurado

Revisión de los requisitos previos para la reconstrucción completa de migración

Tenga en cuenta las opciones siguientes antes de realizar una reconstrucción completa de migración:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado para la restauración, si hay.
- Tiene un equipo de destino válido para la reconstrucción completa.
- Se ha creado Live CD del Agente de Arcserve Unified Data Protection para Linux.
- Si desea realizar una reconstrucción completa mediante la dirección IP, se deberá obtener la dirección IP del equipo de destino mediante Live CD.
- Si desea realizar una reconstrucción completa de PXE mediante la dirección MAC, se debe disponer de la dirección MAC del equipo de destino.
- El punto de recuperación debe ser de la copia de seguridad basada en el agente de Linux.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Realización de una reconstrucción completa en el equipo temporal

Antes de realizar una reconstrucción completa de la migración, se deben restaurar los datos desde el origen a un equipo temporal. Para restaurar los datos temporalmente, se puede realizar una reconstrucción completa en el equipo temporal. Después de que el equipo temporal esté listo para ser utilizado, se puede continuar trabajando en el equipo temporal.

Cuando el equipo real esté listo, se puede realizar una reconstrucción completa de la migración desde el equipo temporal al equipo real.

Nota: Para obtener más información sobre cómo realizar una reconstrucción completa, consulte Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux.

Siga estos pasos:

1. Acceda al asistente de restauración de una de las formas siguientes:

   En Arcserve UDP:

   a. Iniciar sesión en Arcserve UDP.

   b. Haga clic en la ficha **recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos de agregados en el panel central.

   d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   e. Haga clic en **Restaurar** del menú desplegable **Acción**.

      Se abre la interfaz web del Agente de Arcserve Unified Data Protection para Linux. Se muestra el cuadro de diálogo de selección del tipo de restauración en la interfaz de usuario del agente.

   f. Seleccione el tipo de restauración y haga clic en **Aceptar**.

      Nota: Se inicia sesión automáticamente en el nodo del agente y el **Asistente de restauración** se abre desde el nodo del agente.

   En el Agente de Arcserve Unified Data Protection para Linux:

   a. Abra la interfaz web del Agente de Arcserve Unified Data Protection para Linux.

      Nota: Durante la instalación del Agente de Arcserve Unified Data Protection para Linux, recibirá la dirección URL para acceder al servidor y gestionarlo.

   b. Inicie sesión en el Agente de Arcserve Unified Data Protection para Linux.

2. Haga clic en **Restaurar** en el menú **Asistente** y seleccione **Reconstrucción completa (BMR)**.

   Se abre la página **Servidor de copia de seguridad** del **Asistente de restauración - BMR**.

3. Proporcione todos los detalles en el **Asistente de restauración - Reconstrucción completa** y guarde el asistente.

4. Asegúrese de que se selecciona la casilla de verificación **Activar la reconstrucción completa instantánea** en la página **Equipo de destino** del asistente.

5. Asegúrese de que se selecciona la casilla de verificación **No recuperar los datos automáticamente después de que se inicie el equipo** en la página **Equipo de destino** del asistente.

6. Ejecute la tarea de reconstrucción completa.

   El equipo temporal se recupera utilizando la reconstrucción completa, con la opción de la reconstrucción completa instantánea activada. Se puede utilizar el equipo temporal hasta que el equipo real esté listo.

Realización de una reconstrucción completa de la migración

Cuando el equipo real esté listo, realice una reconstrucción completa de la migración. La reconstrucción completa de la migración restaura los datos originales de la sesión de copia de seguridad y los nuevos datos desde el equipo temporal al equipo real.

Siga estos pasos:

1. Haga clic en **Restaurar** en el menú **Asistente** y seleccione **Reconstrucción completa de la migración**.

   Aparece la página **Servidor de copia de seguridad** del **Asistente de restauración - Reconstrucción completa de la migración**.

2. Proporcione todos los detalles en el **Asistente de restauración - Reconstrucción completa de la migración**.

   Nota: Para obtener más información sobre cómo realizar una reconstrucción completa, consulte Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux.

3. Asegúrese de que la siguiente información se proporciona en la página **Servidor de copia de seguridad** del asistente.

   a. Seleccione la tarea de reconstrucción completa instantánea o la tarea de recuperación de la máquina virtual instantánea.

      Servidor local

      Especifica que el servidor de copia de seguridad se gestiona localmente. La tarea de reconstrucción completa para el equipo temporal se ejecuta en el servidor local.

      Servidor remoto

      Especifica que el servidor de copia de seguridad se gestiona remotamente. La tarea de reconstrucción completa para el equipo temporal se ejecuta en el servidor remoto. Se deben proporcionar los detalles del servidor remoto para conectarse al servidor remoto.

   b. Seleccione la tarea de restauración en la lista desplegable Nombre de la tarea.

      La lista muestra la tarea de recuperación de la máquina virtual instantánea o la tarea de reconstrucción completa instantánea, que se encuentran en la

fase de la tarea Listo para usar o Apagar, una vez que está preparada para usarse.

4. Guarde la tarea de reconstrucción completa.

   En la página principal, la **Fase de la tarea** en la ficha **Estado de la tarea** cambia a **Haga clic aquí para migrar datos**.

5. (Opcional) Inicie el equipo temporal mediante un Live CD cuando el tipo de tarea seleccionada sea la reconstrucción completa instantánea.

6. En la ficha **Estado de la tarea**, utilice **Haga clic aquí para migrar datos**.

   Comienza la migración de datos.

   Se ha realizado correctamente una reconstrucción completa de la migración.

Verificación de que el nodo de destino se ha restaurado

Después de finalizar la tarea de restauración, verifique que el nodo de destino se restaure con los datos relevantes.

Siga estos pasos:

1. Vaya al equipo de destino que se ha restaurado.
2. Compruebe que el equipo de destino tiene toda la información del equipo temporal, incluidos los datos nuevos que haya creado en el equipo temporal.

   El equipo de destino se ha verificado correctamente.

   La reconstrucción completa de la migración se ha ejecutado correctamente en los equipos de Linux basados en agente.

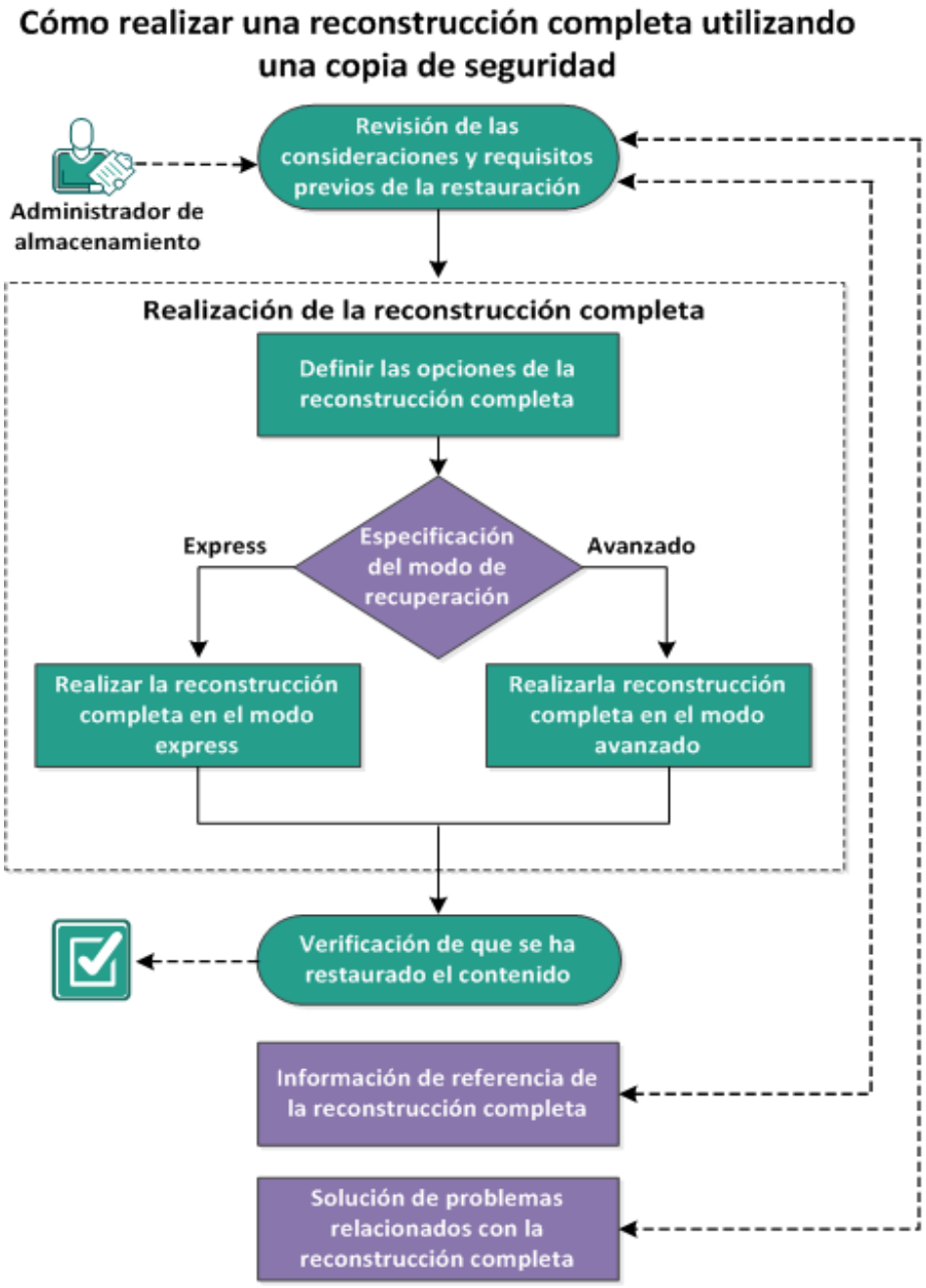
Cómo realizar una reconstrucción completa mediante una copia de seguridad

La reconstrucción completa es el proceso de restaurar un sistema de "reconstrucción completa" incluyendo la reinstalación del sistema operativo y de las aplicaciones de software, además de restaurar los datos y la configuración. El proceso de reconstrucción completa permite restaurar un equipo completo con un esfuerzo mínimo, incluso en un hardware diferente. La reconstrucción completa es posible porque durante el proceso de copia de seguridad de nivel de bloque, el Agente de Arcserve UDP (Windows) no solo captura los datos, sino también toda la información relacionada con las siguientes aplicaciones:

- Sistema operativo
- Aplicaciones instaladas
- Valores de configuración
- Controladores necesarios

Se realiza una copia de seguridad de toda la información relevante que es necesaria para realizar una compilación completa del sistema desde la reconstrucción completa en una serie de bloques que se almacenan en la misma ubicación que la copia de seguridad.

El diagrama siguiente ilustra el proceso sobre cómo realizar una reconstrucción completa mediante una copia de seguridad:



Complete las tareas siguientes para realizar una reconstrucción completa mediante una copia de seguridad:

1. Revisión de las consideraciones y requisitos previos de la reconstrucción completa
2. Definición de las opciones de la reconstrucción completa
   - Realización de la reconstrucción completa en el modo expreso
   - Realización de la reconstrucción completa en el modo avanzado
3. Verificación de que la reconstrucción completa ha sido correcta

4. Información de referencia de la reconstrucción completa
5. Solución de problemas relacionados con la recuperación completa

Revisión de las consideraciones y requisitos previos de la reconstrucción completa

Verifique que los requisitos previos siguientes existen antes de realizar una reconstrucción completa:

- Se debe tener una de las imágenes siguientes:
  - Una imagen ISO de BMR creada se graba en un CD/DVD
  - Una imagen ISO de BMR creada se graba en una unidad de USB

  Nota: Al utilizar el Agente de Arcserve UDP (Windows) se podrá utilizar una utilidad de kit de arranque para combinar una imagen de WinPE y una imagen del Agente de Arcserve UDP (Windows) a fin de crear una imagen ISO de reconstrucción completa. Esta imagen ISO se graba en un medio de arranque. Se puede utilizar cualesquiera de los medios de arranque siguientes (CD/DVD o unidad de USB) para inicializar el nuevo sistema informático y permitir el inicio del proceso de reconstrucción completa. Para garantizar que la imagen guardada es la versión más reciente, una práctica recomendable es la creación de una nueva imagen ISO cada vez que se actualiza el Agente de Arcserve UDP (Windows).
- Tener al menos una copia de seguridad completa disponible.
- Disponer de al menos 2 GB de memoria RAM instalados en la máquina virtual y en el servidor de origen que está recuperando.
- Para recuperar máquinas virtuales de VMware en otras que estén configuradas para comportarse como servidores físicos, compruebe que las herramientas de VMware estén instaladas en la máquina virtual de destino.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones sobre la restauración:

- Independientemente del método que ha utilizado para crear una imagen de kit de arranque, el proceso de reconstrucción completa es prácticamente el mismo para cada caso.

  Nota: El proceso de reconstrucción completa no puede crear espacios de almacenamiento. Si el equipo de origen ha tenido espacios de almacenamiento durante la reconstrucción completa, no se podrán crear nuevos en el equipo de destino. También se pueden restaurar estos volúmenes en discos/volúmenes regulares o crear espacios de almacenamiento manualmente antes de realizar

la reconstrucción completa. A continuación, ya se podrán restaurar los datos en los espacios de almacenamiento creados.

- Los discos dinámicos sólo se restauran en el nivel de disco. Si ha realizado la copia de seguridad de los datos en un volumen local de un disco dinámico, no será posible restaurar este disco dinámico durante la reconstrucción completa. En este escenario, para restaurar durante la reconstrucción completa se debe realizar una de las tareas siguientes y a continuación realizar la reconstrucción completa desde el punto de recuperación copiado:
  - Realizar la copia de seguridad en un volumen de otra unidad.
  - Realizar la copia de seguridad en un recurso compartido remoto.
  - Copiar un punto de recuperación en otra ubicación.

  Nota: Si se realiza una reconstrucción completa con varios discos dinámicos, esta podrá producir un error a causa de algunos errores inesperados (como un error al reiniciar los volúmenes dinámicos desconocidos, entre otros). Si esto ocurre, se debería restaurar solamente el disco del sistema mediante BMR y, a continuación, después de reiniciar el equipo, se podrá realizar una restauración de los otros volúmenes dinámicos en un entorno normal.
- (Opcional) Revise la información de referencia de la reconstrucción completa. Si desea obtener más información, consulte los siguiente temas:
  - Cómo funciona la reconstrucción completa
  - Sistemas operativos que admiten la conversión de UEFI/BIOS
  - Gestión del menú Operaciones de BMR

Revise las siguientes consideraciones:

- Si se actualiza a una versión más reciente de Arcserve UDP, se tendrá que volver a crear la imagen ISO de reconstrucción completa utilizando el nivel adecuado de Windows ADK o AIK para incluir la compatibilidad con las últimas funciones y correcciones de errores. Sin embargo, una vez que se crea una imagen ISO de reconstrucción completa, el archivo ISO puede utilizarse para el mismo nivel de sistema operativo. Los siguientes niveles de sistema operativo pueden utilizar el mismo ISO:
  - ISO creado con el WAIK Windows 7: Funciona para Windows 2003, Vista, 2008 y 2008 R2
  - ISO creado usando Windows 8/8.1 ADK: Funciona para Windows 8, 8.1, Server 2012 y 2012 Server R2
  - ISO creado con Windows 10 ADK: Funciona para Windows 10, Windows Server 2016 y Windows Server 2019

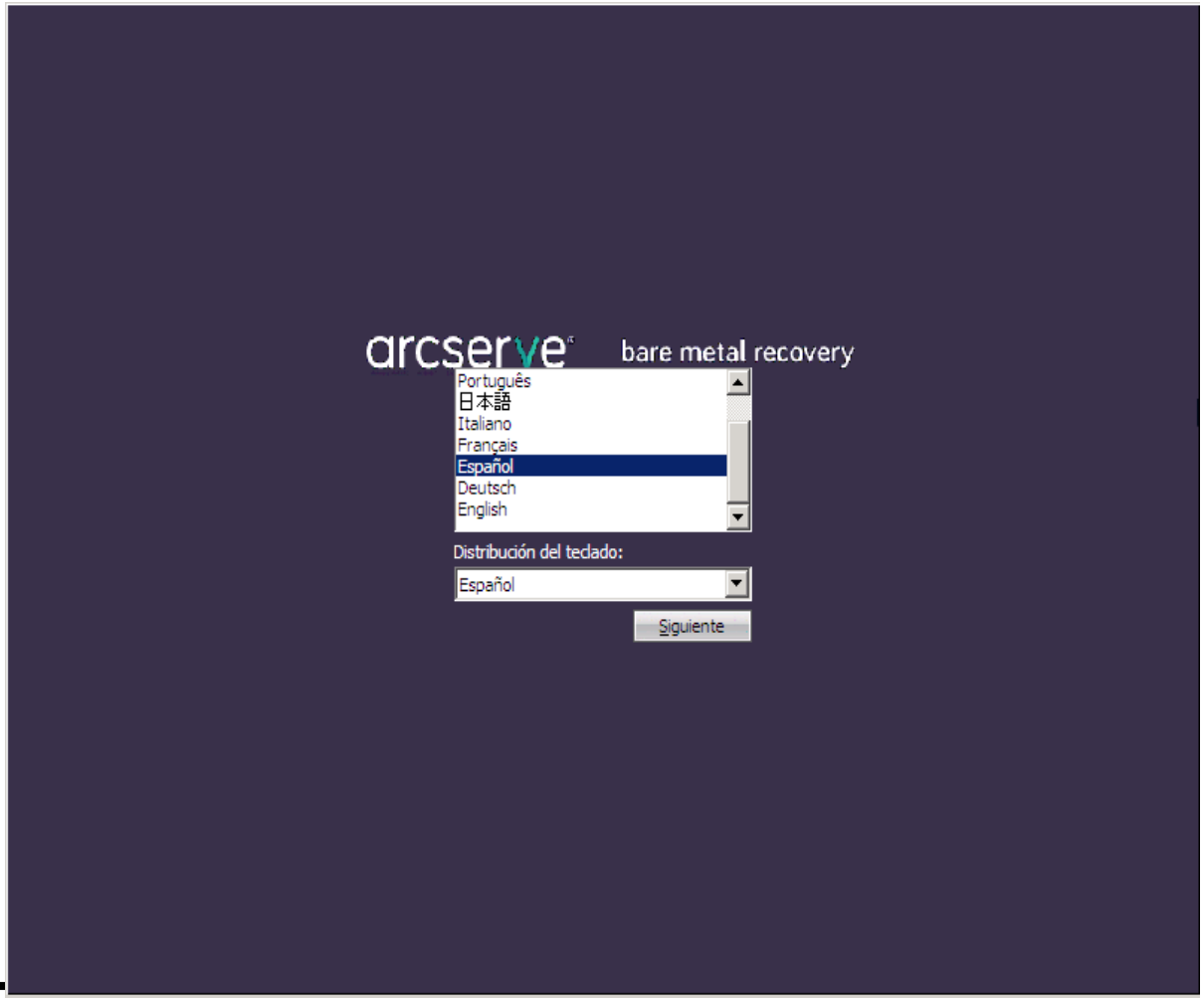
Definición de las opciones de la reconstrucción completa

Antes de iniciar el proceso de la reconstrucción completa, se deben especificar algunas opciones de la reconstrucción completa preliminares.

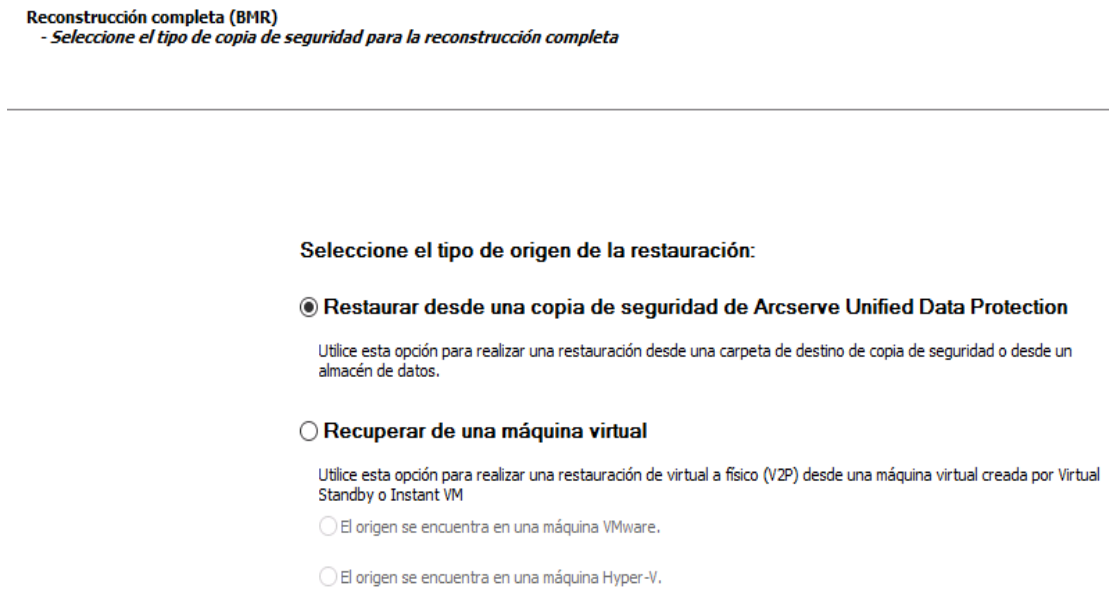
Siga estos pasos:

1. Inserte el medio de imagen de kit de arranque guardado y reinicie el equipo.
   - Si se utiliza una imagen ISO de BMR que se ha grabado en un CD/DVD, inserte el CD/DVD guardado.
   - Si se utiliza una imagen ISO de BMR que se ha grabado en una unidad de USB, inserte el USB guardado.

   Aparecerá la pantalla **Utilidad de instalación de BIOS**.
2. Desde la pantalla **Utilidad de instalación de BIOS**, seleccione la opción de unidad de CD-ROM o unidad de USB para iniciar el proceso de arranque. Seleccione una arquitectura (x86/x64) y pulse **Intro** para continuar.
3. Aparece la pantalla de selección del idioma del Agente de Arcserve UDP (Windows). Seleccione el idioma y haga clic en **Siguiente** para continuar.



El proceso de reconstrucción completa empezará y se mostrará la pantalla inicial del asistente de reconstrucción completa.



La pantalla del asistente para la reconstrucción completa le permite seleccionar el tipo de reconstrucción completa que se desea realizar:

- **Restaurar desde una copia de seguridad de Arcserve Unified Data Protection**

  Utilice esta opción para realizar una restauración desde una carpeta de destino de la copia de seguridad o desde un almacén de datos.

  Esta opción permite recuperar los datos de los cuales se ha realizado una copia de seguridad mediante el Agente de Arcserve UDP (Windows). Esta opción se utiliza en relación con las sesiones de copia de seguridad realizadas con el Agente de Arcserve UDP (Windows) o con la aplicación de copia de seguridad de máquina virtual basada en el host de Arcserve UDP.

  Si se selecciona esta opción, continúe este procedimiento desde aquí.

- **Recuperar de una máquina virtual**

  Utilice esta opción para realizar una restauración de virtual a-física (V2P) desde una máquina virtual de Virtual Standby. El término Virtual a física (V2P) hace referencia a la migración de un sistema operativo (SO), los programas de la aplicación y los datos desde una máquina virtual o partición de disco al disco duro principal de un equipo. El destino puede ser un único equipo o varios equipos.

- **El origen está en un equipo de VMware**

  Permite recuperar datos para un equipo para el cual se realiza la conversión virtual en una máquina virtual de VMware. Esta opción se utiliza junto con la aplicación Arcserve Central Virtual Standby.

  Nota: Para esta opción, solamente se pueden recuperar datos si la conversión virtual a un archivo VMDK (para VMware) se ha realizado mediante Arcserve Central Virtual Standby.

  Si se ha seleccionado esta opción, consulte Recuperar mediante una máquina virtual con Virtual Standby para VMware para continuar con este procedimiento.

  Para obtener más información, consulte Recuperar mediante una máquina virtual con Virtual Standby para VMware en la Ayuda en línea del Agente para Windows.

- **El origen está en un equipo de Hyper-V**

  Posibilita la recuperación de datos para un equipo para el cual se realiza la conversión virtual en una máquina virtual de Hyper-V. Esta opción se utiliza junto con la aplicación Arcserve Central Virtual Standby.

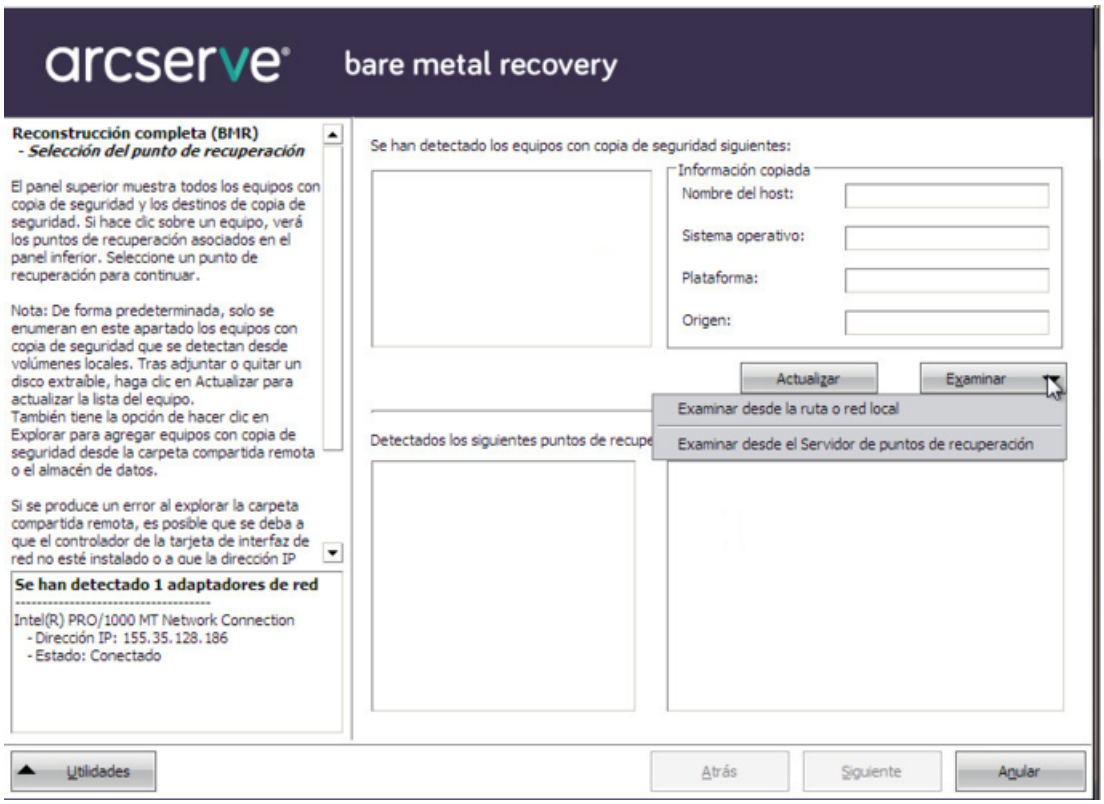
  Nota: Para esta opción, solamente se pueden recuperar datos si la conversión virtual a un archivo VHD (para Hyper-V) se ha realizado mediante Arcserve Central Virtual Standby.

  Si se ha seleccionado esta opción, consulte Recuperar mediante una máquina virtual con Virtual Standby para Hyper-V para continuar con este procedimiento.

  Para obtener más información, consulte Recuperar mediante una máquina virtual con Virtual Standby para Hyper-V en la Ayuda en línea del Agente para Windows.

4. Seleccione **Restaurar desde una copia de seguridad de Arcserve Unified Data Protection** y haga clic en **Siguiente**.

   Aparecerá la pantalla del asistente **Seleccionar un punto de recuperación**.



5. En la pantalla del asistente **Seleccionar un punto de recuperación**, haga clic en **Examinar** y seleccione **Examinar desde la red/ruta local** o **Examinar desde el servidor de punto de recuperación**.

   a. Si se selecciona **Examinar** desde la red/ruta local, seleccione el equipo (o volumen) que contiene los puntos de recuperación para la imagen de copia de seguridad.

      El Agente de Arcserve UDP para Windows permite realizar la recuperación desde cualquier unidad local o desde un recurso compartido de red.

      - Si se realiza la recuperación desde una copia de seguridad local, el asistente de reconstrucción completa detectará de forma automática y mostrará todos los volúmenes que contienen los puntos de recuperación.
      - Si se realiza la recuperación desde un recurso compartido remoto, se deberá explorar la ubicación remota en la que se deben almacenar los puntos de recuperación. Si existen varios equipos que contienen puntos de recuperación, aparecerán todos los equipos.

        También es posible que necesite información de acceso (nombre de usuario y contraseña) para el equipo remoto.

Nota: La red debe estar encendida y en ejecución para que sea posible explorar los puntos de recuperación remotos. Si es necesario también es posible comprobar/actualizar la información de configuración de la red o cargar los controladores que faltan desde el menú Utilidades.

- Si el módulo de reconstrucción completa no puede detectar ningún volumen de destino local, aparecerá automáticamente el cuadro de diálogo **Seleccionar una carpeta.** Proporcione el recurso compartido remoto donde se encuentran las copias de seguridad.
- Si está restaurando desde un destino de iSCSI, es posible que el módulo de reconstrucción completa no detecte este destino, con lo que será necesario realizar lo siguiente:

  1. Haga clic en **Utilidades**, seleccione **Ejecutar** en el menú emergente, escriba **cmd** y, a continuación, haga clic en **Aceptar**.

  2. En la ventana del símbolo del sistema, utilice los siguientes comandos de iSCSI de Windows para configurar conexiones de iSCSI:

  > net start msiscsi

  > iSCSICLI QAddTargetPortal <DirecciónPortalDestino>

  > iSCSICLI QLoginTarget <NombreDestino> [CHAP username] [CHAP password]

  Nota: CHAP = Protocolo de autenticación por desafío mutuo

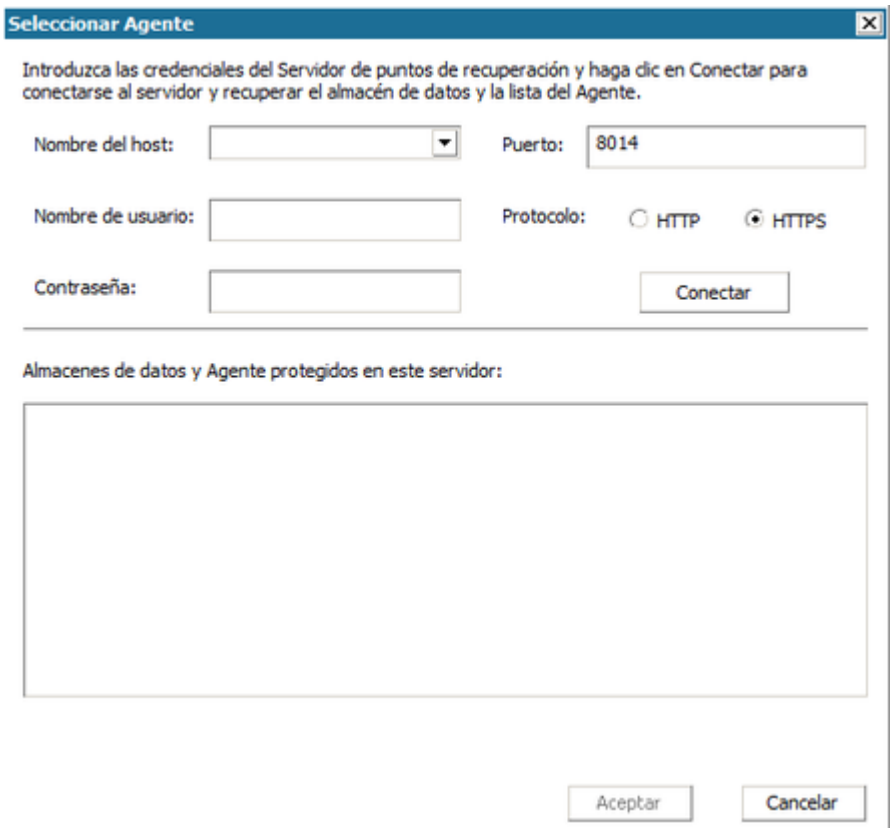
  Para obtener más información sobre las opciones de la línea de comandos iSCSI de Windows, consulte vínculo.

  Nota: Se pueden necesitar pasos extras en función del software de destino de iSCSI que se utilice. Para obtener más información, consulte el manual del software de destino de iSCSI.

  3. Se deben mostrar en la pantalla Reconstrucción completa los discos/volúmenes conectados a través del disco de iSCSI. El disco de iSCSI se puede utilizar ahora como el volumen de origen o el volumen de destino de la copia de seguridad.

  Nota: La reconstrucción completa no es compatible con el caso donde el SO está instalado en un disco de iSCSI. Solo se es compatible con los discos de datos.

b. Si se selecciona **Examinar el servidor de punto de recuperación**, se muestra el cuadro de diálogo **Seleccionar agente.** Proporcione el **Nombre de host del servidor de punto de recuperación**, el **Nombre de usuario**, la **Contraseña**, el **Puerto** y el **Protocolo**. Haga clic en **Conectar**.



6. Seleccione la carpeta o el nombre del agente bajo Almacén de datos donde están almacenados los puntos de recuperación para la copia de seguridad y haga clic en **Aceptar**.

   La pantalla del asistente de reconstrucción completa ahora muestra la información siguiente:

   - Nombre del equipo (en el panel superior izquierdo).
   - Información de copia de seguridad relacionada (en el panel superior derecho).
   - Todos los puntos de recuperación correspondientes (en el panel inferior izquierdo).

     Nota: Para los sistemas operativos compatibles, se puede realizar una reconstrucción completa de una copia de seguridad realizada en un equipo de UEFI a un equipo compatible con BIOS y viceversa. Consulte la sección Sistemas operativos que admiten la conversión de UEFI/BIOS para obtener un listado completo de los sistemas que admiten la conversión de firmware.
   - Para realizar la reconstrucción completa en un sistema de UEFI dentro de los sistemas operativos que no admiten la conversión de firmware, se deberá iniciar el equipo en el modo de UEFI. La reconstrucción completa no es

compatible con la restauración de un equipo con un firmware distinto. Para verificar que el firmware de arranque es UEFI y no BIOS, haga clic en **Utilidades**, **Acerca de**.

- Para los sistemas operativos que admiten la conversión de firmware si, después de seleccionar un punto de recuperación, se detecta que el equipo de origen no es el mismo firmware que el del sistema, se solicitará al usuario si desea convertir UEFI en un sistema compatible con BIOS o viceversa.

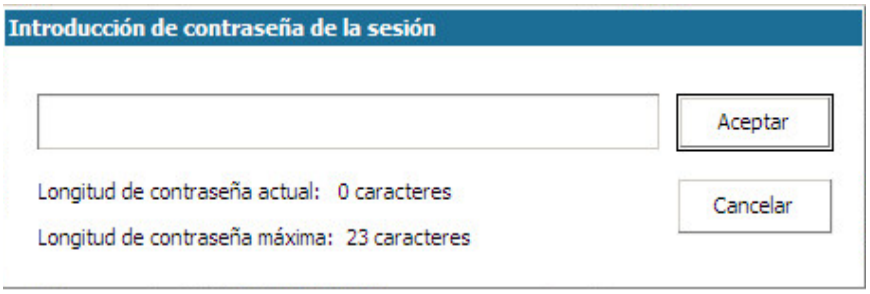


Nota: Arcserve UDP versión 5.0 Actualización 2 solo admite la reconstrucción completa en un disco más pequeño cuando se realiza una copia de seguridad de las sesiones desde Arcserve UDP versión 5.0 Actualización 2. Consulte el campo **Tamaño mínimo necesario** para el tamaño de disco de destino. La reconstrucción completa en un disco más pequeño solo se admite en el **modo avanzado**.

7. Seleccione el punto de recuperación para restaurar.

   Aparecerá la información relacionada con el punto de recuperación (en el panel inferior derecho). Incluye información acerca del tipo de copia de seguridad que se ha realizado (y guardado), el destino de la copia de seguridad y los volúmenes de los que se ha realizado copia de seguridad.

Si el punto de recuperación contiene sesiones cifradas (el icono de reloj de punto de recuperación dispondrá de un candado), aparecerá una pantalla que requiere contraseña. Introduzca la contraseña y haga clic en **Aceptar**.



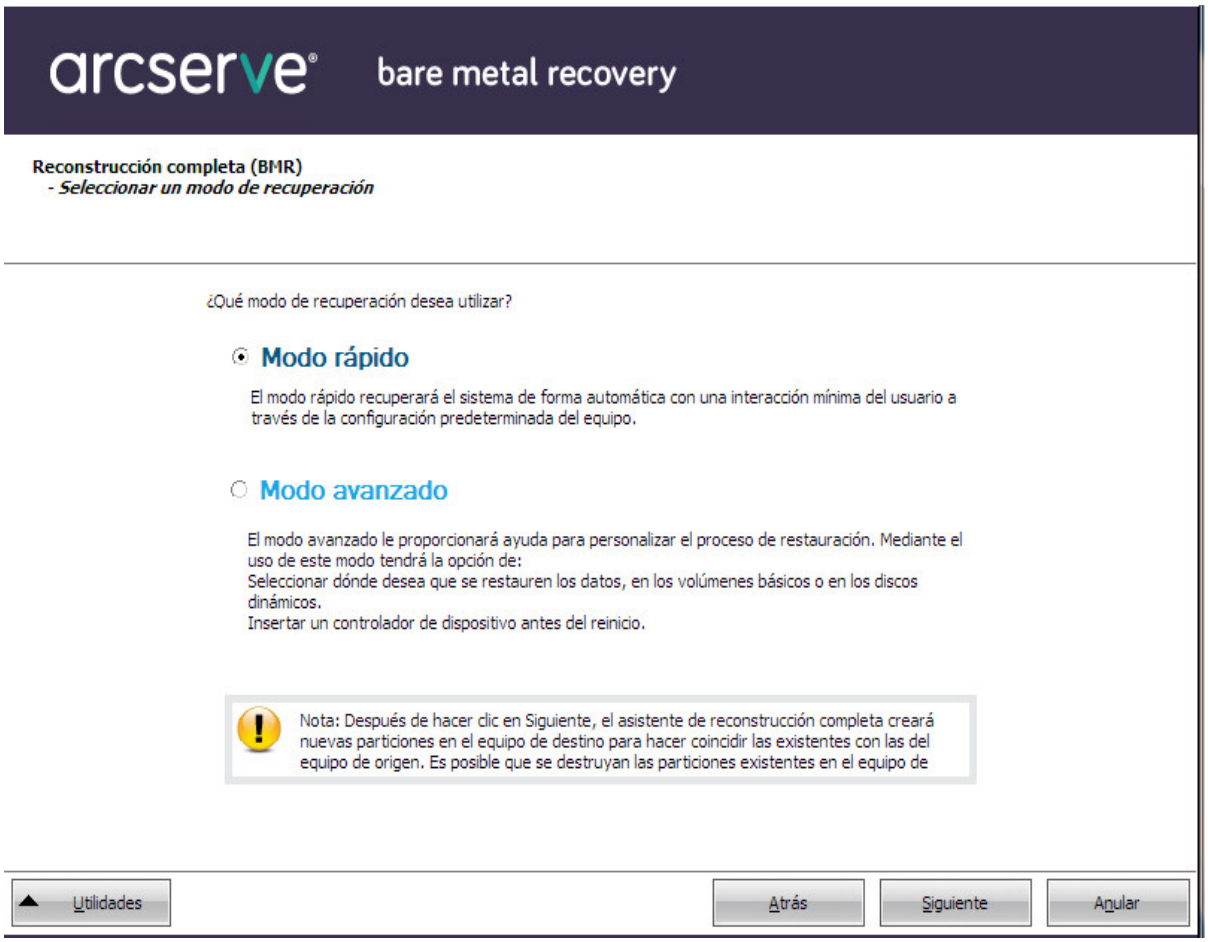
Notas:

Si se está realizando la restauración desde un servidor de puntos de recuperación de Arcserve UDP, se debe proporcionar la contraseña de sesión.

Si el equipo es un controlador de dominio, el Agente de Arcserve UDP para Windows admite la restauración no autoritativa del archivo de la base de datos de Active Directory durante la reconstrucción completa. (No se admite la restauración de clústeres de MSCS).

8. Compruebe que se trata del punto de recuperación que desee restaurar y haga clic en **Siguiente**.

   Aparecerá la pantalla del asistente de reconstrucción completa con las opciones de modo de recuperación disponibles.



Las opciones disponibles son **Modo avanzado** y **Modo rápido**.

- Seleccione Modo rápido si desea una interacción mínima durante el proceso de recuperación.
- Seleccione Modo avanzado si desea personalizar el proceso de recuperación.

  Valor predeterminado: Modo rápido.

Realización de la reconstrucción completa en el modo expreso

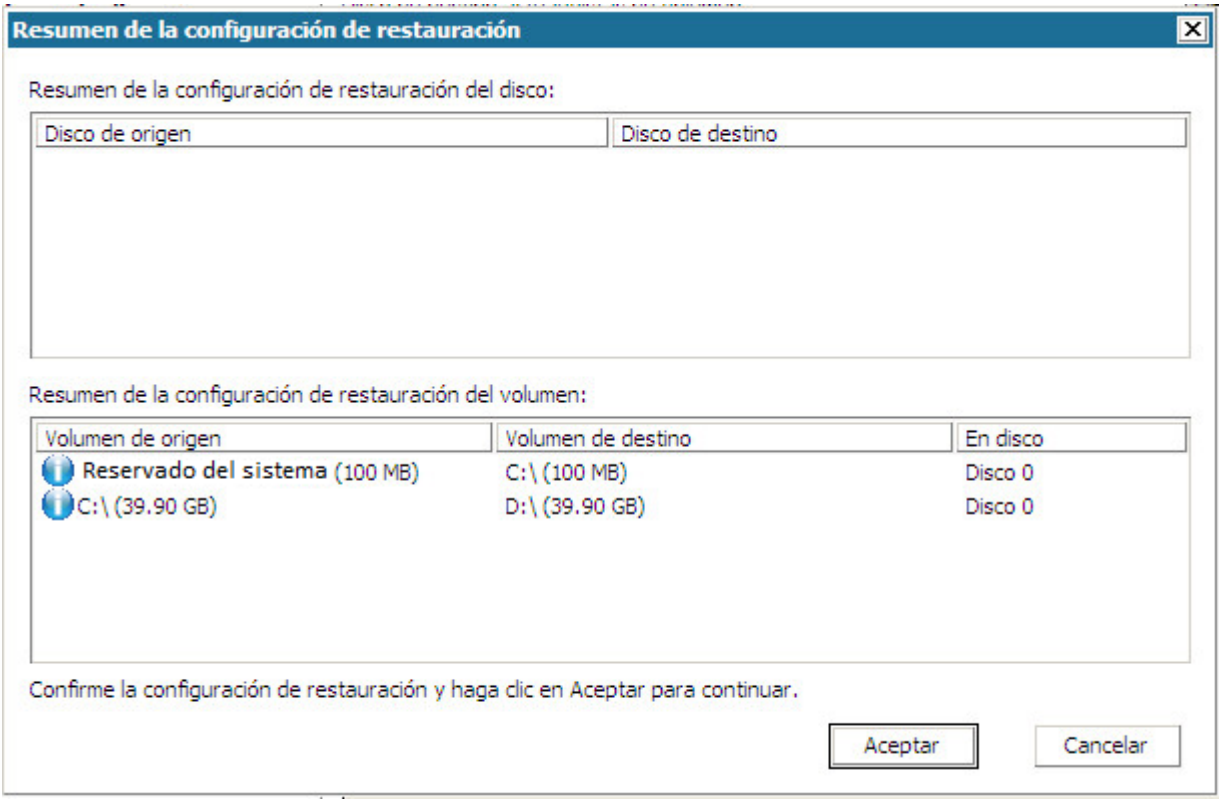
El modo rápido requiere una interacción mínima durante el proceso de recuperación.

Siga estos pasos:

1. En el cuadro de diálogo **Seleccionar un modo de recuperación**, seleccione **Modo rápido** y haga clic en **Siguiente**.

   Aparecerá la pantalla **Resumen de la configuración de restauración del disco** que muestra un resumen de los volúmenes para restaurar.

   Nota: En la parte inferior de la ventana de resumen de restauración, las letras de unidad de la columna **Volumen de destino** se generan de forma automática desde el entorno de preinstalación de Windows (WinPE). Es posible que sean diferentes de las letras de unidad que se enumeran en la columna **Volumen de origen.** Sin embargo, los datos se restaurarán en el volumen adecuado incluso si las letras de unidad son diferentes.

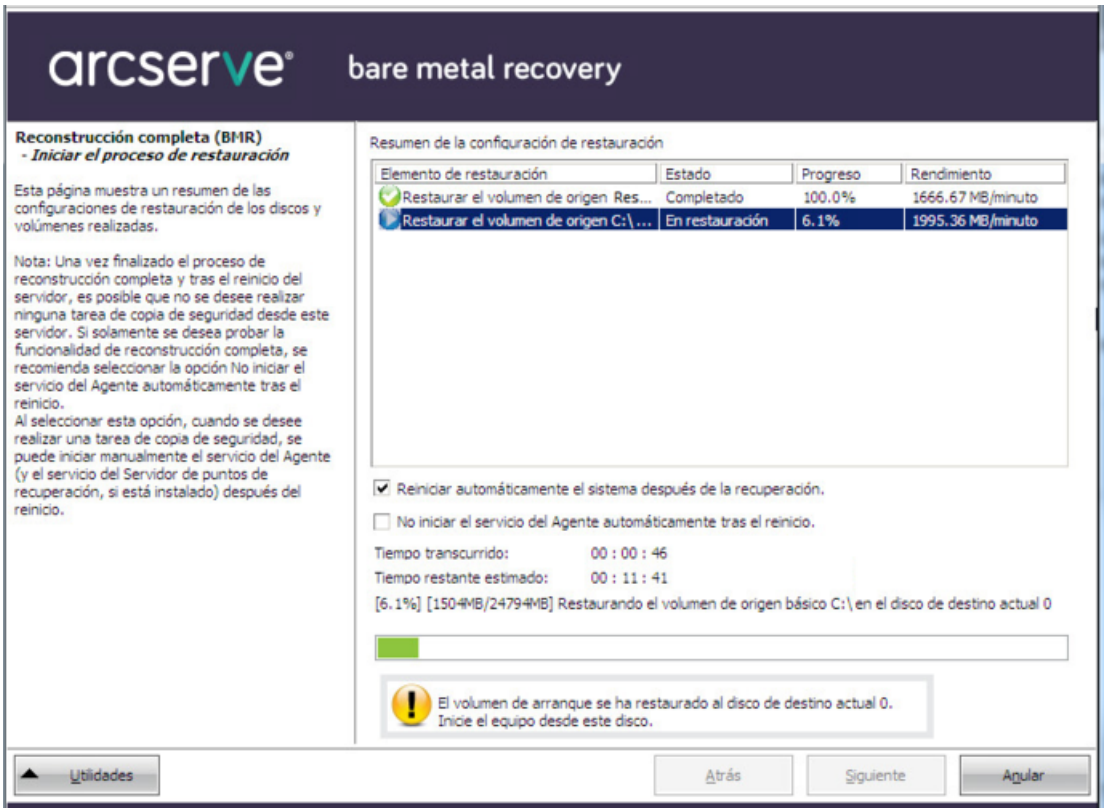


2. Cuando haya comprobado que la información de resumen es correcta, haga clic en **Aceptar**.

Se iniciará el proceso de restauración. La pantalla del asistente de reconstrucción completa mostrará el estado de restauración para cada volumen.

- Esta operación puede tardar unos minutos, según el tamaño del volumen restaurado.
- En el proceso se restauran por bloques todos los datos de los que había realizado copia de seguridad para el punto de recuperación y se crea, además, una réplica del equipo de origen en el equipo de destino.
- De forma predeterminada, se selecciona la opción de reiniciar el equipo de forma automática después de la recuperación. Si es necesario, es posible deseleccionar la opción y reiniciar el equipo manualmente más tarde.

  Importante: Si se realiza una restauración autoritativa de un Active Directory después de una reconstrucción completa, se debe eliminar la selección de la opción **Reiniciar automáticamente el sistema después de la recuperación** y para obtener más información, consulte Cómo realizar una restauración autoritativa de Active Directory después de una reconstrucción completa.
- Si es necesario, se puede seleccionar No iniciar el servicio del agente automáticamente después del reinicio.
- Si es necesario, tiene la opción de cancelar o abortar la operación en cualquier momento.



3. Desde el menú **Utilidades** podrá acceder al **Registro de actividades** de reconstrucción completa y utilizar la opción **Guardar** para guardar el registro de actividad.

   De forma predeterminada, el registro de actividad se guardará en la ubicación siguiente:

   X:\windows\system32\dr\log

   Nota: Para evitar obtener un error de Windows, no debe guardar el registro de actividad en el escritorio o crear una carpeta nueva en el escritorio usando la opción **Guardar como** de la ventana de registro de actividad de reconstrucción completa.

4. Si restaura un hardware diferente (el adaptador de SCSI/FC que se ha utilizado para conectar los discos duros puede haberse modificado) y no se ha detectado ningún tipo de controlador compatible en el equipo original, aparecerá la página de inserción de controladores para proporcionar los controladores para los dispositivos.

   Es posible buscar y seleccionar controladores para insertarlos en el sistema recuperado, de modo que incluso al realizar la recuperación en un equipo con un hardware diferente, todavía sea posible recuperar el equipo después de la reconstrucción completa.

   Al finalizar el proceso de reconstrucción completa, aparecerá una notificación de confirmación.

Realización de la reconstrucción completa en el modo avanzado

La opción **Modo avanzado** permite personalizar el proceso de recuperación.

Siga estos pasos:

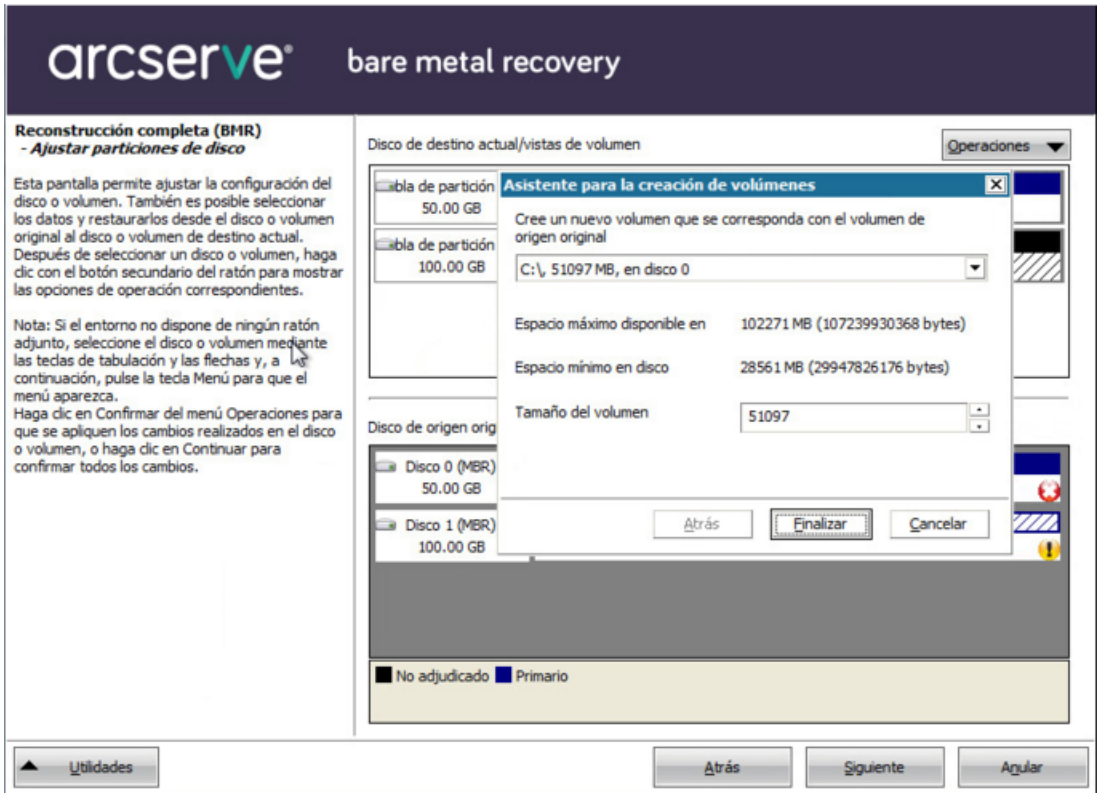
1. En el cuadro de diálogo **Seleccionar un modo de recuperación**, seleccione **Modo avanzado** y haga clic en **Siguiente**.

   La utilidad de reconstrucción completa se inicia buscando el equipo para recuperar y mostrará información de la partición de disco correspondiente.

   El panel superior muestra la configuración de disco que tiene en el equipo (de destino) actual y el panel inferior muestra la información de partición de disco que tenía en el equipo (de origen) original.

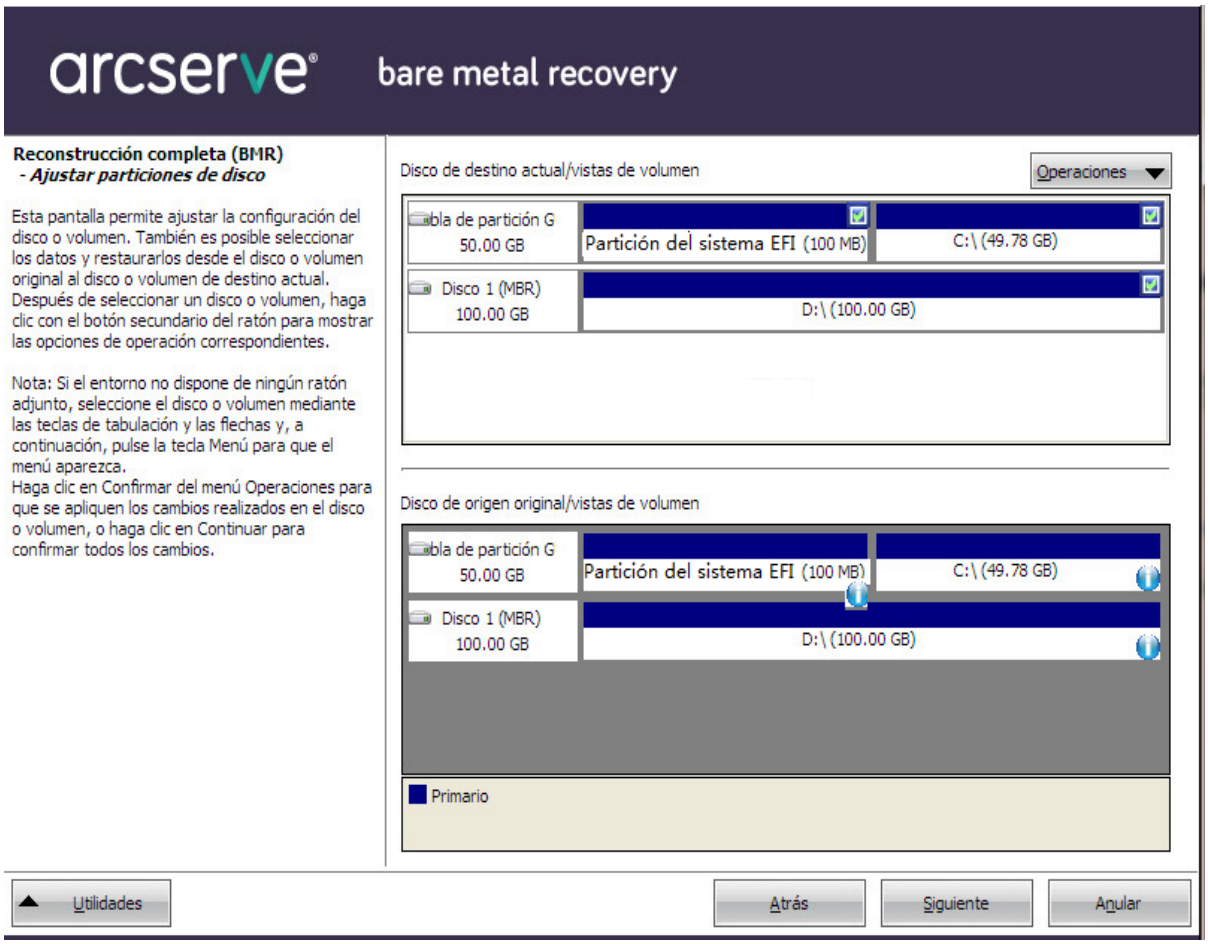
   Importante: Un icono X rojo que muestra un volumen de origen en el panel inferior indica que este volumen contiene información del sistema y no se ha asignado al volumen de destino. El volumen de información del sistema desde el disco de origen debe asignarse al disco de destino y restaurarse durante la reconstrucción completa o es posible que se produzca un error al reiniciar.

   Se pueden crear volúmenes a un disco más pequeño en función del valor sugerido del **Espacio mínimo en disco obligatorio**. En el ejemplo, el tamaño original del volumen es 81568 MB. Cuando se crea el volumen en el disco de destino, el tamaño mínimo sugerido es de 22752 MB. En este caso, se puede crear el volumen original con un tamaño de 22752 MB.



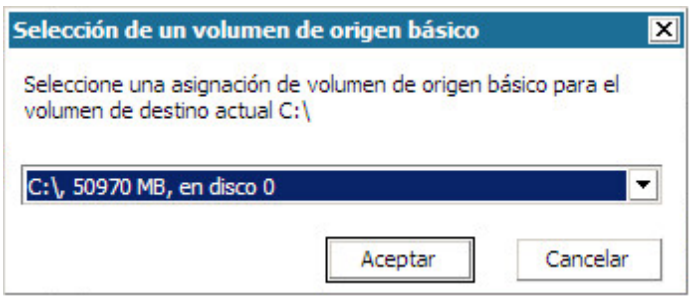
Nota: Si se realiza la reconstrucción completa y se restaura el volumen del sistema en un disco que no está configurado como el disco de arranque, se producirá un error al inicializar el equipo después de que finalice la reconstrucción completa. Asegúrese de que se restaura el volumen del sistema en un disco de arranque configurado correctamente.

Nota: Al realizar la restauración en otro disco/volumen, la capacidad de disco/volumen nuevo puede ser del mismo tamaño, mayor que la del disco/volumen original, o inferior que la del disco/volumen original. Además, el cambio de volúmenes no es para discos dinámicos.



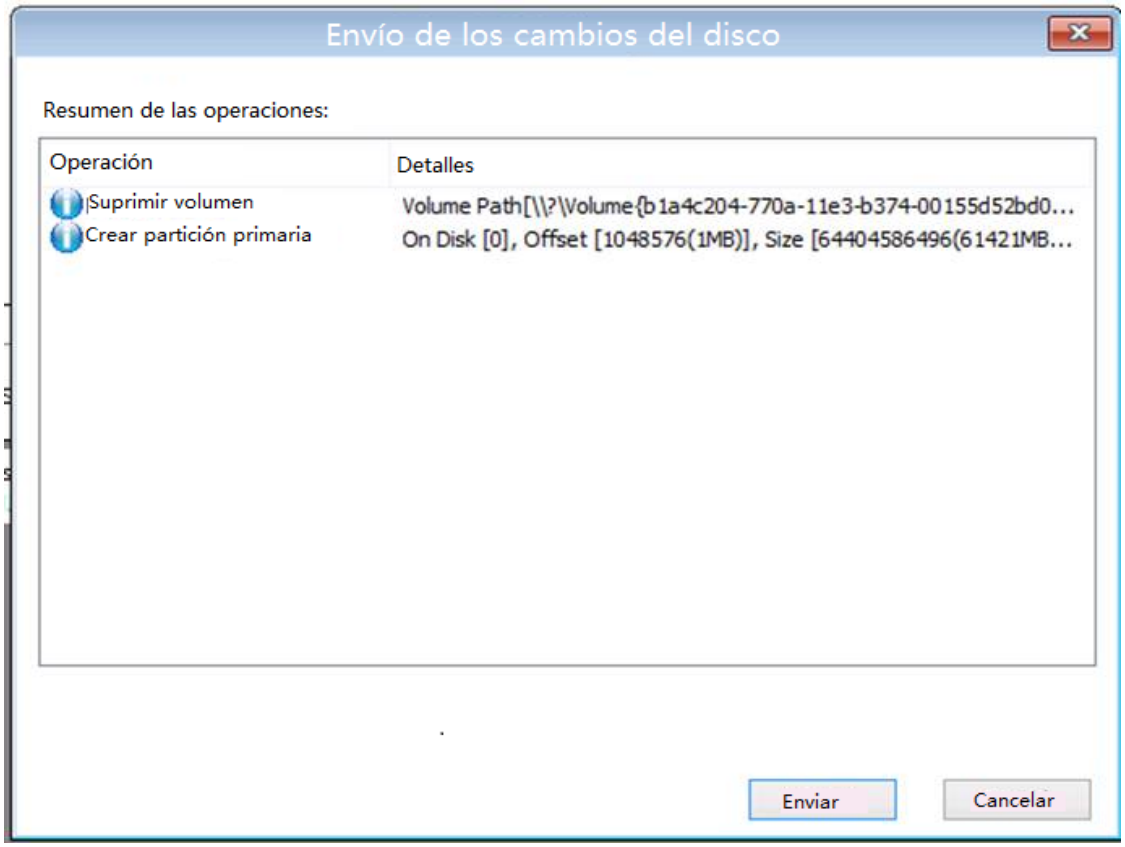
2. Si la información de disco actual no es correcta, acceda al menú **Utilidades** y compruebe los posibles controladores que faltan.
3. Si es necesario, en el panel de volumen/disco de destino se puede hacer clic en el menú desplegable **Operaciones** para visualizar las opciones disponibles. Para obtener más información sobre estas opciones, consulte la sección Gestión del menú Operaciones de BMR.
4. Haga clic en todos los volúmenes de destino y, desde el menú emergente, seleccione la opción **Asignar volumen desde** para asignar un volumen de origen en el volumen de destino.

   Aparecerá el cuadro de diálogo **Seleccionar un volumen de origen básico**.



5. Desde el cuadro de diálogo **Seleccionar un volumen de origen básico**, haga clic en el menú desplegable y seleccione el volumen de origen disponible para asignar al volumen de destino seleccionado. Haga clic en **Aceptar**.
   - En el volumen de destino aparecerá una marca de verificación que indica que se ha asignado al volumen de destino.
   - En el volumen de origen, los cambios del icono con una X roja al icono verde indican que el volumen de origen se ha asignado a un volumen de destino.
6. Cuando esté seguro de que todos los volúmenes que desea restaurar y de que todos los volúmenes que contienen información del sistema están asignados a un volumen de destino, haga clic en **Siguiente**.

   Se mostrará la pantalla **Enviar cambios de disco**, que muestra un resumen de las operaciones seleccionadas. Aparecerá la información correspondiente a cada volumen nuevo creado.



7. Cuando haya comprobado que la información de resumen es correcta, haga clic en **Enviar**. (Si la información no es correcta, haga clic en **Cancelar**).

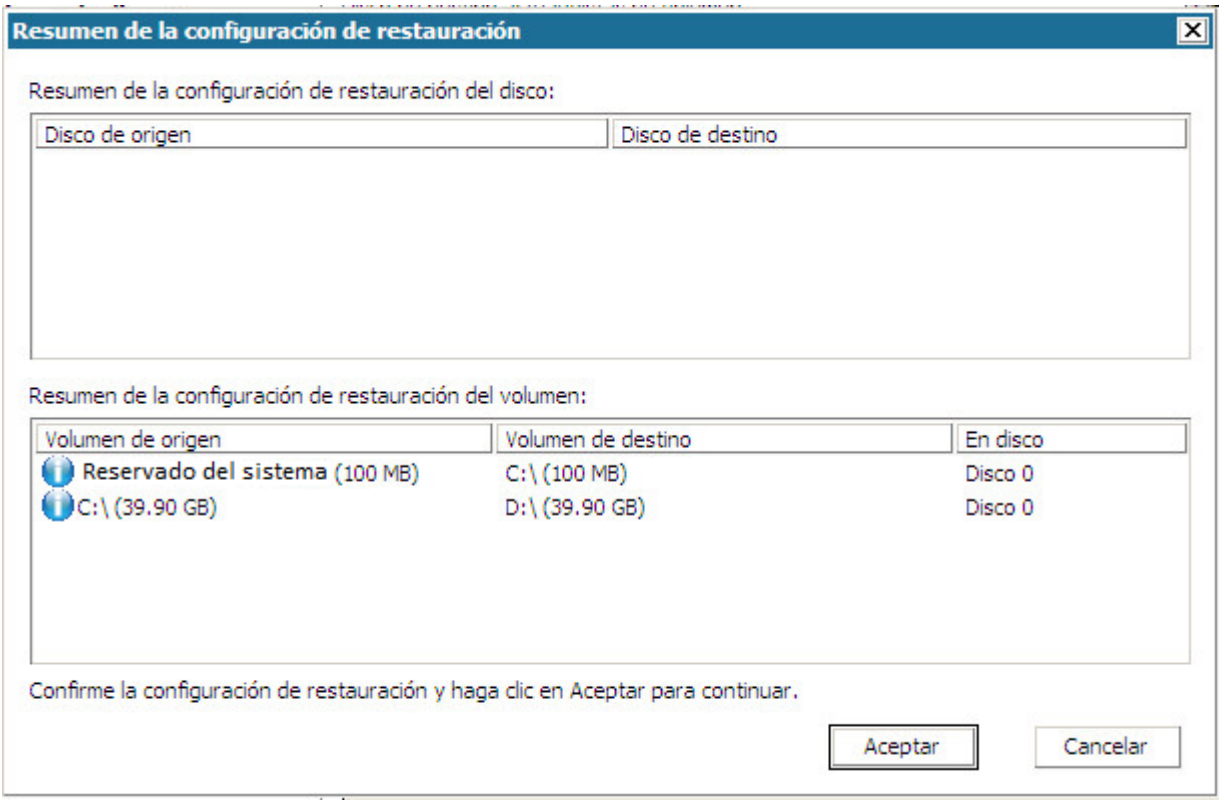
   Nota: Las operaciones en el disco duro no tendrán efecto hasta enviarlas.

   En el equipo de destino, los nuevos volúmenes se crean en el disco de destino y se asignan al equipo de origen correspondiente.

8. Cuando los cambios finalicen, haga clic en **Aceptar**.

   Aparecerá la pantalla Resumen de la configuración de restauración del disco que muestra un resumen de los volúmenes para restaurar.

   Nota: En la parte inferior de la ventana de resumen de restauración, las letras de unidad de la columna "Volumen de destino" se generan de forma automática desde el entorno de preinstalación de Windows (WinPE). Es posible que sean diferentes de las letras de unidad que se enumeran en la columna "Volumen de origen". Sin embargo, los datos se restaurarán en el volumen adecuado incluso si las letras de unidad son diferentes.



9. Cuando haya comprobado que la información de resumen es correcta, haga clic en **Aceptar**.

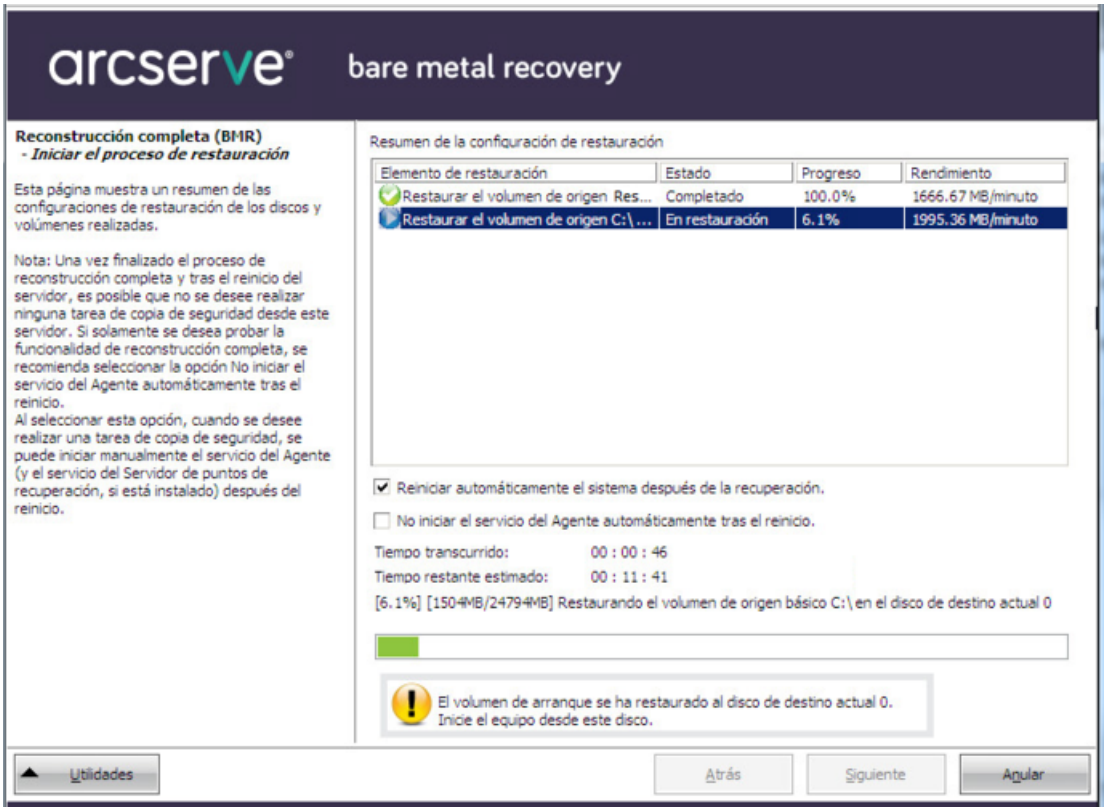
   Se iniciará el proceso de restauración. La pantalla del asistente de reconstrucción completa mostrará el estado de restauración para cada volumen.

   - Esta operación puede tardar unos minutos, según el tamaño del volumen restaurado.
   - En el proceso se restauran por bloques todos los datos de los que había realizado copia de seguridad para el punto de recuperación y se crea, además, una réplica del equipo de origen en el equipo de destino.

- De forma predeterminada, se selecciona la opción de reiniciar el equipo de forma automática después de la recuperación. Si es necesario, es posible deseleccionar la opción y reiniciar el equipo manualmente más tarde.

  Importante: Si se realiza una restauración autoritativa de un Active Directory después de una reconstrucción completa, se debe eliminar la selección de la opción **Reiniciar automáticamente el sistema después de la recuperación** y para obtener más información, consulte Cómo realizar una restauración autoritativa de Active Directory después de una reconstrucción completa.

- Si es necesario, se puede seleccionar No iniciar el servicio del agente automáticamente después del reinicio.
- Si es necesario, tiene la opción de cancelar o abortar la operación en cualquier momento.



10. Desde el menú **Utilidades** podrá acceder al **Registro de actividades** de reconstrucción completa y utilizar la opción **Guardar** para guardar el registro de actividad.

    De forma predeterminada, el registro de actividad se guardará en la ubicación siguiente:

    X:\windows\system32\dr\log.

    Nota: Para evitar obtener un error de Windows, no se debe guardar el registro de actividad en el escritorio o crear una carpeta nueva en el escritorio usando la

opción **Guardar como** de la ventana **Registro de actividades** de reconstrucción completa.

11. Si restaura un hardware diferente (el adaptador de SCSI/FC que se ha utilizado para conectar los discos duros puede haberse modificado) y no se ha detectado ningún tipo de controlador compatible en el equipo original, aparecerá la página de inserción de controladores para proporcionar los controladores para los dispositivos.

    Es posible buscar y seleccionar controladores para insertarlos en el sistema recuperado, de modo que incluso al realizar la recuperación en un equipo con un hardware diferente, todavía sea posible recuperar el equipo después de la reconstrucción completa.

12. Al finalizar el proceso de reconstrucción completa, aparecerá una notificación de confirmación.

Verificación de que la reconstrucción completa ha sido correcta

Para verificar si la reconstrucción completa ha sido correcta, realice las tareas siguientes:

- Reinicie el sistema operativo.
- Verifique que todos los sistemas y las aplicaciones funcionan correctamente.
- Verifique que todos los valores de configuración de la red están configurados correctamente.
- Verifique que la BIOS se ha configurado para arrancar desde el disco en el que se ha restaurado el volumen de arranque.
- Cuando se completa la reconstrucción completa, tenga en cuenta las siguientes condiciones:
  - La primera copia de seguridad que se realiza después de una reconstrucción completa es una copia de seguridad de verificación.
  - Una vez que el equipo haya reiniciado, es posible que sea necesario configurar los adaptadores de redes de manera manual si se ha realizado la restauración en un hardware diferente.

    Nota: Cuando se reinicia el equipo, aparecerá la pantalla Recuperación de errores de Windows indicando que Windows no se ha apagado correctamente. Si esto ocurre, se podrá ignorar esta advertencia de forma segura y continuar con el inicio de Windows del modo habitual.
  - Para discos dinámicos, si el estado del disco es sin conexión, éste se puede cambiar a en línea de forma manual desde la interfaz de usuario de gestión de discos (a la cual se accede mediante la ejecución de la utilidad de control Diskmgmt.msc).
  - Para discos dinámicos, si los volúmenes dinámicos están en estado de redundancia con errores, es posible volver a sincronizar los volúmenes de forma manual desde la interfaz de usuario de gestión de discos (a la cual se accede mediante la ejecución de la utilidad de control Diskmgmt.msc).

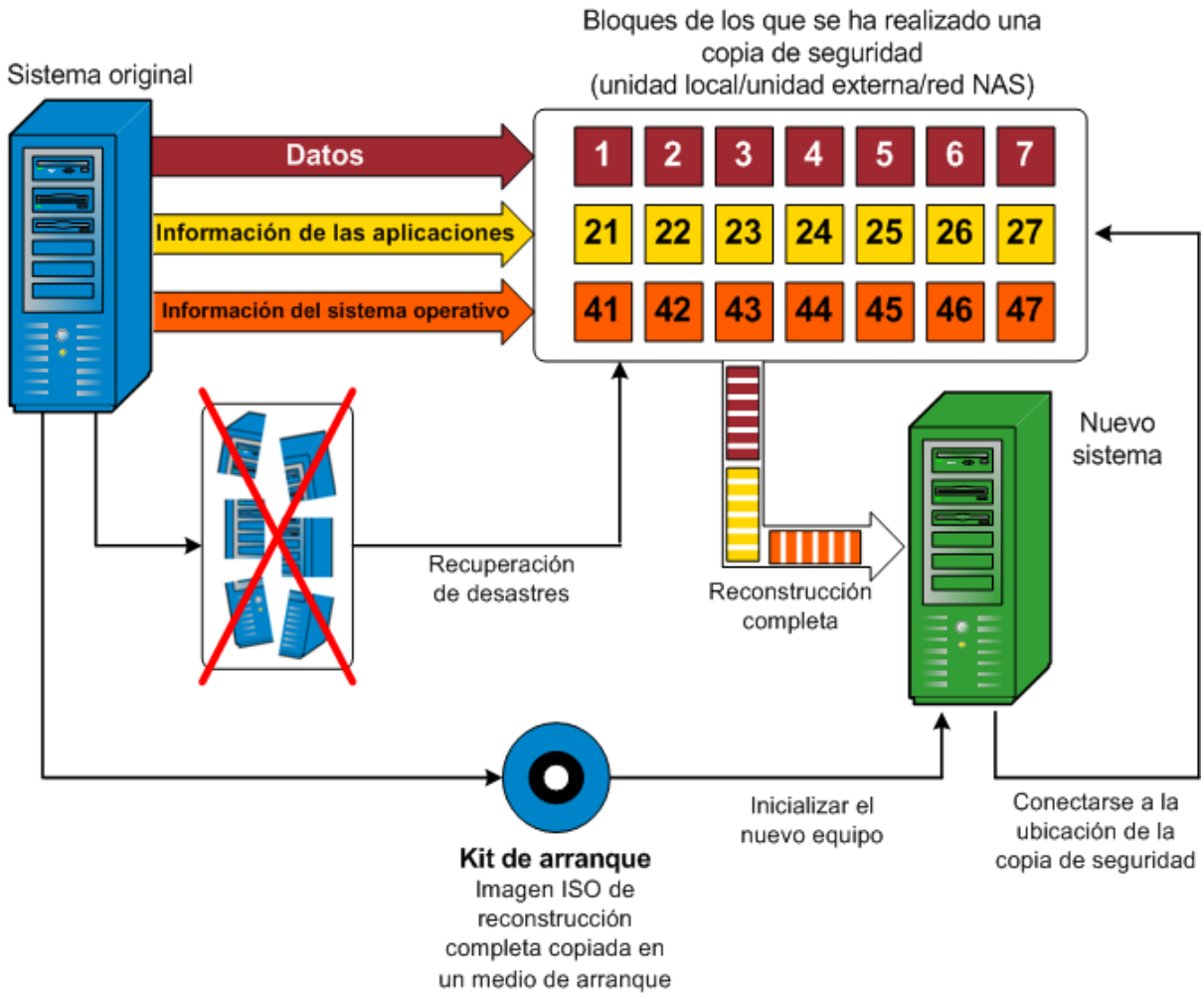
Información de referencia de la reconstrucción completa

- Cómo funciona la reconstrucción completa
- Sistemas operativos que admiten la conversión de UEFI/BIOS
- Gestión del menú Operaciones de BMR

Cómo funciona la reconstrucción completa

La reconstrucción completa es el proceso de restauración de un sistema desde la "reconstrucción completa" incluyendo la reinstalación del sistema operativo y de las aplicaciones de software, además de restaurar los datos y la configuración. Los motivos más comunes para realizar una reconstrucción completa son porque se produce un error en el disco duro o se llena y se desea actualizar (migrar) a una unidad mayor o migrar a un equipo de hardware más reciente. La reconstrucción completa es posible porque durante el proceso de copia de seguridad de nivel de bloque el Agente de Arcserve UDP (Windows) no solo captura los datos, sino toda la información relacionada con el sistema operativo, las aplicaciones instaladas, la configuración, los controladores necesarios, entre otros. Se realiza una copia de seguridad de toda la información relevante que es necesaria para realizar una compilación completa del sistema desde la reconstrucción completa en una serie de bloques que se almacenan en la misma ubicación que la copia de seguridad.

Nota: Los discos dinámicos sólo se restaurarán en el nivel de disco. Si se ha realizado la copia de seguridad de los datos en un volumen de un disco dinámico, no será posible restaurar este disco dinámico (incluidos sus volúmenes) durante la reconstrucción completa.



Cuando se realiza una reconstrucción completa se utiliza el disco de arranque del Agente de Arcserve UDP (Windows) para iniciar el sistema y permitir que comience el proceso de recuperación completa. Al iniciar la reconstrucción completa, el Agente de Arcserve UDP (Windows) solicitará que se seleccione o proporcione una ubicación válida desde la cual se podrán recuperar los bloques con copia de seguridad y también un punto de recuperación para la restauración. Si es necesario, también se solicitarán los controladores válidos para el nuevo sistema. Cuando se proporciona información de conexión y configuración, el Agente de Arcserve UDP (Windows) empieza a sacar la imagen de copia de seguridad específica desde la ubicación de copia de seguridad y a restaurar todos los bloques con copia de seguridad al nuevo sistema (los bloques vacíos no se restaurarán). Una vez se ha restaurado por completo la imagen de la reconstrucción completa en el nuevo sistema, el equipo volverá a estar en el estado en que se encontraba en el momento en que se realizó la última copia de seguridad y se podrán continuar las copias de seguridad del Agente de Arcserve UDP (Windows) según lo programado. (Después de la reconstrucción completa, la primera copia de seguridad será una Copia de seguridad de verificación).

Sistemas operativos que admiten la conversión de UEFI/BIOS

Si se detecta que el sistema operativo del equipo de origen no es el mismo firmware que el del sistema, se solicitará al usuario si desea convertir UEFI en un sistema compatible con BIOS-compatible o BIOS en sistema compatible con UEFI. La tabla siguiente clasifica todos los sistemas operativos y el tipo de conversión compatible:

Usuario del sistema operativo (SO)	CPU	uEFI a BIOS	BIOS a uEFI
Microsoft Windows (ningún SP)	x86	No	No
Microsoft Windows (ningún SP)	x64	No	No
Windows Vista SP1	x86	No	No
Windows Vista SP1	x64	Sí	Sí
Windows Server 2008	x86	No	No
Windows Server 2008	x64	Sí	Sí
Windows Server 2008 R2	x64	Sí	Sí
Windows 7	x86	No	No
Windows 7	x64	Sí	Sí
Windows 8	x86	No	No
Windows 8	x64	Sí	Sí
Windows Server 2012	x64	Sí	Sí
Windows 8.1	x86	No	No
Windows 8.1	x64	Sí	Sí
Windows 10	x86	No	No
Windows 10	x64	Sí	Sí
Windows Server 2012 R2	x64	Sí	Sí
Windows Server 2016	x64	Sí	Sí
Windows Server 2019	x64	Sí	Sí

Gestión del menú Operaciones de BMR

El menú Operaciones de BMR está formado por los tres tipos de operaciones siguientes:

- Operaciones específicas del disco
- Operaciones específicas de Volume/Partition
- Operaciones específicas de reconstrucción completa

Operaciones específicas del disco:

Para realizar operaciones específicas del disco, seleccione el encabezado de disco y haga clic en **Operaciones**.

Limpiar disco

Esta operación se utiliza y es para limpiar todas las particiones de un disco y es

- un método alternativo para suprimir todos los volúmenes de un disco. Con la operación **Limpiar disco** no es necesario suprimir cada volumen uno a uno.
- Se utiliza para suprimir las particiones que no sean de Windows. Debido a una limitación de VDS, no se puede suprimir la partición que no es de Windows de la IU, pero se puede utilizar esta operación para limpiarlas todas.

  Nota: Durante la reconstrucción completa, cuando el disco de destino tiene particiones que no son de Windows o particiones de OEM, no se puede seleccionar esta partición y suprimirla de la IU de reconstrucción completa. Normalmente esto ocurriría cuando se instalaba Linux/Unix en el disco de destino. Para solucionar este problema, se deben realizar las tareas siguientes:
- Seleccione el encabezado de disco en la IU de reconstrucción completa, haga clic en **Operaciones** y utilice la operación **Limpiar disco** para borrar todas las particiones del disco.
- Abra un símbolo del sistema y escriba **Diskpart** para abrir la consola de comandos de Diskpart. Después escriba "seleccionar disco X" , donde "X" es el número del disco, y "limpiar" para borrar todas las particiones del disco.

Convertir en MBR

Esta operación se utiliza para convertir un disco en MBR (registro de arranque maestro). Está disponible solamente cuando el disco seleccionado es un

disco de tabla de partición GUID (GPT) y no hay ningún volumen en este disco.

Convertir en tabla de partición GUID

Esta operación se utiliza para convertir un disco en una tabla de partición GUID. Está disponible solamente cuando el disco seleccionado es un disco de MBR y no hay ningún volumen en este disco.

Convertir en básico

Esta operación se utiliza para convertir un disco en básico. Está disponible solamente cuando el disco seleccionado es un disco dinámico y no hay ningún volumen en este disco.

Convertir en dinámico

Esta operación se utiliza para convertir un disco en un disco dinámico. Está disponible solamente cuando el disco seleccionado es un disco básico.

Disco en línea

Esta operación se utiliza para conectar el disco. Está disponible solamente cuando el disco seleccionado está en estado sin conexión.

Propiedades de disco

Esta operación se utiliza para ver las propiedades detalladas del disco. Está siempre disponible, y cuando se selecciona esta operación aparece un cuadro de diálogo **Propiedades de disco**.

Operaciones específicas de Volume/Partition:

Para realizar operaciones de volumen/partición, seleccione el área del cuerpo de disco y haga clic en **Operaciones**. Desde este menú se pueden crear nuevas particiones para que se correspondan con las particiones de disco en el volumen de origen.

Crear partición primaria

Esta operación se utiliza para crear una partición en un disco básico. Está disponible solamente cuando el área seleccionada es un espacio en disco no adjudicado.

Crear partición lógica

Esta operación se utiliza para crear una partición lógica en un disco básico de MBR. Está disponible solamente cuando el área seleccionada es una partición extendida.

Crear partición extendida

Esta operación se utiliza para crear una partición extendida en un disco básico de MBR. Está disponible solamente cuando el disco es un disco de MBR y el área seleccionada es un espacio en disco no adjudicado.

Crear una partición reservada del sistema

Esta operación se utiliza para crear la partición reservada del sistema en un sistema de firmware de BIOS y construye una relación de asignación con la partición del sistema de EFI de origen. Está disponible solamente cuando se restaura un sistema de UEFI en un sistema de BIOS.

Nota: Si ha realizado la conversión previamente de UEFI a un sistema compatible con BIOS, utilice la opción operación Crear una partición reservada del sistema para cambiar el tamaño del disco de destino.

Crear partición del sistema de EFI

Esta operación se utiliza para crear la partición del sistema de EFI en un disco básico de GPT. Está disponible solamente cuando el firmware del equipo de destino es UEFI y el disco seleccionado es un disco básico de GPT.

Nota: Si ha realizado la conversión previamente de BIOS a un sistema compatible con BIOS, utilice la operación Crear partición del sistema de EFI para cambiar el tamaño del disco de destino.

Nota: Los sistemas compatibles con UEFI también requieren que la partición de arranque resida en un disco de GPT (tabla de particiones GUID). Si utiliza un disco de MBR (registro de arranque maestro), se debe convertir este disco en un disco de GPT y, a continuación, utilizar la operación Crear partición del sistema de EFI para cambiar el tamaño del disco.

Cambiar el tamaño del volumen

Esta operación se utiliza para cambiar el tamaño de un volumen. Es un método alternativo de Windows "Extender volumen/Reducir volumen". Está disponible solamente cuando el área seleccionada es una partición de disco válida.

Suprimir el volumen

Esta operación se utiliza para suprimir un volumen. Está disponible solamente cuando el área seleccionada es un volumen válido.

Suprimir la partición extendida

Esta operación se utiliza para suprimir la partición extendida. Está disponible solamente cuando el área seleccionada es una partición extendida.

Propiedades del volumen

Esta operación se utiliza para ver las propiedades detalladas del volumen. Cuando se selecciona esta operación, aparece el cuadro de diálogo **Propiedades del volumen**.

Operaciones específicas de BMR:

Estas operaciones son específicas de BMR. Para realizar operaciones de reconstrucción completa, seleccione el encabezado de disco o el área del cuerpo de disco y haga clic en **Operaciones**.

Asignar disco desde

Esta operación se utiliza para construir una relación de asignación entre los discos dinámicos de origen y de destino. Está disponible solamente cuando el disco seleccionado es un disco dinámico.

Nota: Al asignar a otro disco, la capacidad de cada volumen de destino asignado debe ser del mismo tamaño o mayor que la del volumen de origen correspondiente.

Asignar volumen desde

Esta operación se utiliza para construir una relación de asignación entre el volumen básico de origen y de destino. Está disponible solamente cuando el volumen seleccionado es un volumen básico.

Nota: Al asignar a otro disco, la capacidad de cada volumen de destino asignado debe ser del mismo tamaño o mayor que la del volumen de origen correspondiente.

Confirmar

Esta operación está siempre disponible. Todas las operaciones se guardan en la memoria caché y no modifican los discos de destino hasta que se selecciona la operación **Confirmar**.

Restablecer

Esta operación está siempre disponible. La operación **Restablecer** se utiliza para cancelar las operaciones y restaurar el diseño del disco a su estado predeterminado. Esta operación limpia todas las operaciones guardadas en la memoria caché. Restablecer significa volver a cargar la información de diseño del disco de destino y de origen desde el archivo de configuración y el sistema operativo actual, y rechazar cualquier información de diseño del disco modificado por el usuario.

Solución de problemas relacionados con la recuperación completa

Al detectar un problema, el Agente de Arcserve UDP (Windows) genera un mensaje para ayudarle a identificar y resolver el problema. El **registro de actividades** del Agente de Arcserve UDP (Windows) contiene estos mensajes. Se puede acceder a él a través de la opción **Ver registros** que se encuentra en la interfaz de usuario de la página principal. Además, cuando se intenta llevar a cabo una acción incorrecta, el Agente de Arcserve UDP (Windows) suele mostrar un mensaje emergente que le ayuda a identificar el problema y resolverlo de forma rápida.

- Rendimiento lento durante la reconstrucción completa
- Después de la reconstrucción completa, el sistema operativo no reconoce volúmenes dinámicos.
- Imposibilidad de reiniciar la máquina virtual de Hyper-V después de la reconstrucción completa
- Imposibilidad de reiniciar la máquina virtual de VMware después de la reconstrucción completa
- No se puede iniciar el servidor después de realizar una reconstrucción completa.
- Se ha producido un error al enviar la tarea de reconstrucción completa al servidor de punto de recuperación

Rendimiento lento durante la reconstrucción completa

Este problema puede estar causado porque los controladores de SATA tienen AHCI activado.

Durante la reconstrucción completa, el Agente de Arcserve UDP (Windows) instalará controladores para dispositivos desconocidos importantes. Si el dispositivo ya tiene un controlador instalado, el Agente de Arcserve UDP (Windows) no actualizará el controlador de nuevo. Para algunos dispositivos, Windows 7PE puede disponer de controladores, pero estos controladores pueden no ser los mejores y provocar que la reconstrucción completa se ejecute de manera lenta.

Para solucionar este problema, se deben realizar las tareas siguientes:

- Compruebe si la carpeta de agrupación de controlador contiene los controladores de disco más nuevos. Si es así y realiza una restauración en el equipo original, instale el controlador nuevo desde la carpeta de agrupación de controlador. Si se realiza una restauración en un equipo alternativo, descargue los últimos controladores de disco de Internet y cárguelos antes de iniciar la recuperación de datos. Para cargar el controlador, puede utilizar la utilidad "drvload.exe", que se incluye en PE de Windows.
- Cambie el modo operativo del dispositivo de Interfaz avanzada de controlador de host (AHCI) a modo de compatibilidad. (El modo de compatibilidad proporciona un mejor rendimiento).

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Después de la reconstrucción completa, el sistema operativo no reconoce los volúmenes dinámicos

Para guardar discos dinámicos de forma coherente, el sistema operativo de Windows sincroniza automáticamente los metadatos del Administrador de discos lógicos (LDM) en cada disco dinámico. De modo que cuando la reconstrucción completa restaura un disco dinámico y lo conecta, el sistema operativo actualizará automáticamente los metadatos de LDM en este disco. Esto puede dar lugar a que el sistema operativo no reconozca un volumen dinámico y que falte después del reinicio.

Para solucionar este problema, al realizar la reconstrucción completa con discos dinámicos múltiples, no deben realizarse operaciones de disco previas de reconstrucción completa como la limpieza, la supresión de un volumen, etc.

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Imposibilidad de reiniciar la máquina virtual de Hyper-V después de la reconstrucción completa

Si ha realizado una reconstrucción completa en un equipo de Hyper-V formado por más de un disco conectado a un controlador de Electrónica de Dispositivo Integrada (IDE), y el servidor no se reinicia, realice el siguiente procedimiento de solución de problemas:

1. Compruebe que el disco que contiene el volumen del sistema es el disco principal.

   La BIOS Hyper-V busca el volumen del sistema en el disco principal (disco 1) que está conectado al canal principal. Si el volumen del sistema no está ubicado en el disco principal, la máquina virtual no se reiniciará.

   Nota: Verifique que el disco que contiene el volumen del sistema esté conectado a un controlador de IDE. Hyper-V no puede reiniciarse desde un disco de SCSI.

2. Si es necesario, modifique la configuración de Hyper-V para conectarse al disco que contiene el volumen del sistema al canal principal de IDE y reinicie de nuevo la máquina virtual.

   Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Imposibilidad de reiniciar la máquina virtual de VMware después de la reconstrucción completa

Si ha realizado una reconstrucción completa en un equipo de VMware formado por más de un disco conectado a un controlador de Electrónica de Dispositivo Integrada (IDE) o un adaptador de SCSI y el servidor no se reinicia, realice el siguiente procedimiento de resolución de problemas:

1. Compruebe que el disco que contiene el volumen del sistema es el disco principal.

   La BIOS VMware busca el volumen del sistema en el disco principal (disco 0) que está conectado al canal principal. Si el volumen del sistema no está ubicado en el disco principal, la máquina virtual no se reiniciará.

2. Si es necesario, modifique la configuración de VMware para conectarse al disco que contiene el volumen del sistema al canal principal de IDE y reinicie de nuevo la máquina virtual.

3. Si el disco es SCSI, compruebe que el disco que contiene el volumen de arranque sea el primer disco que se conecte al adaptador de SCSI. Si no, asigne al disco de arranque desde la BIOS de VMware.

4. Asegúrese de que el disco que contiene el volumen de arranque sea uno de los ocho primeros, dado que la BIOS de VMware sólo detecta 8 discos durante el arranque. Si existen más de 7 discos en el disco que contienen volúmenes del sistema conectados al adaptador de SCSI, la máquina virtual no podrá reiniciarse.

   Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

No se puede iniciar el servidor después de realizar una reconstrucción completa.

Síntoma

Cuando el equipo de origen es un servidor Active Directory que realiza una reconstrucción completa en una máquina física con un hardware distinto o a una máquina virtual en un servidor Hyper-V, el servidor no se inicia y aparecerá una pantalla azul con el siguiente mensaje:

DETENCIÓN: los servicios del directorio c00002e2 no podrán iniciarse a causa del error siguiente: no funciona el dispositivo adjunto al sistema. Estado del error: 0xc0000001.

Solución

Reinicie el sistema en el entorno PE de BMR, cambie el nombre de todos los archivos *.log en la carpeta C:\Windows\NTDS y reinicie el sistema. Por ejemplo, renombre el archivo edb.log a edb.log.old y reinicie el sistema.

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Se ha producido un error al enviar la tarea de reconstrucción completa al servidor de punto de recuperación

Solamente se es compatible con una tarea de reconstrucción completa cuando se restaura desde el mismo servidor de punto de recuperación para el mismo nodo (copia de seguridad del agente o copia de seguridad basada en host). El controlador de tareas controla esta acción en el servidor de punto de recuperación.

Si el equipo donde la tarea de reconstrucción completa se está ejecutando se cierra o reinicia inesperadamente, el controlador de tareas del servidor de punto de recuperación esperará 10 minutos y, a continuación, se excederá el tiempo de espera. Durante este tiempo no se puede iniciar otra reconstrucción completa para el mismo nodo del mismo servidor de punto de recuperación.

Si se anula la reconstrucción completa desde la interfaz de usuario de la reconstrucción completa, este problema no existe.

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

El equipo de destino de la reconstrucción completa se inicia en la pantalla de las opciones de recuperación del sistema después de llevar a cabo una reconstrucción completa

Síntoma

Si se realiza una reconstrucción completa en una máquina virtual en un servidor ESX, a veces el equipo de destino de la reconstrucción completa se inicia en la pantalla de las opciones de recuperación del sistema.

Solución

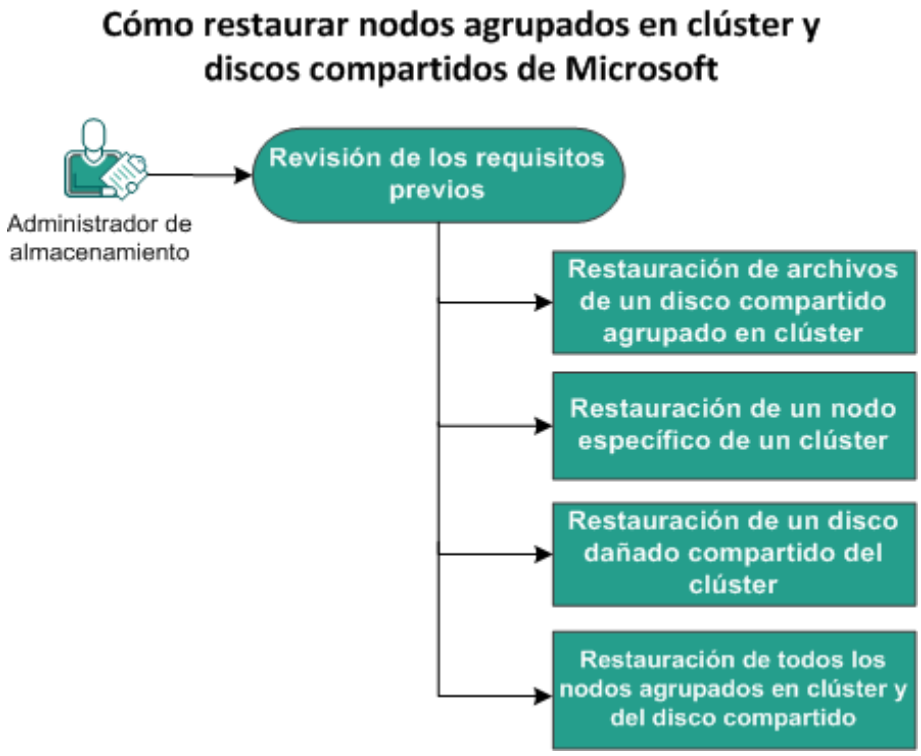
Para solucionar este problema, desactive editores VSS específicos con VMware Tools en la máquina virtual instantánea del equipo y, a continuación, vuelva a realizar una reconstrucción completa.

Cómo restaurar los nodos agrupados en clúster y los discos compartidos de Microsoft

Si se tiene un entorno agrupado en clúster y los nodos agrupados en clúster y el disco compartido no están funcionando correctamente, se pueden recuperar fácilmente los nodos y discos. Se pueden restaurar los elementos siguientes:

- Archivos y carpetas individuales de discos compartidos
- Nodos específicos de un clúster
- Disco compartido entero
- Configuración de clúster entera (todos los nodos agrupados en clúster y el disco compartido)

El diagrama siguiente ilustra el proceso para restaurar los nodos agrupados en clúster y los discos compartidos:



Siga estos pasos para restaurar los nodos agrupados en clúster y los discos compartidos de Microsoft:

- Revisión de los requisitos previos
- Restauración de archivos de un disco compartido agrupado en clúster
- Restauración de un nodo específico de un clúster

- Restauración de un disco dañado compartido del clúster
- Restauración de todos los nodos agrupados en clúster y del disco compartido

Revisión de los requisitos previos

Verifique que se han completado los requisitos previos siguientes:

- Se tiene un punto de recuperación válido para llevar a cabo la restauración.
- Se tiene una imagen ISO válida para una recuperación completa.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Restauración de archivos de un disco compartido agrupado en clúster

El disco compartido pertenece a uno de los nodos del clúster. Cuando se recupera cualquier archivo del disco compartido (no del disco de quórum del clúster), es necesario encontrar el nodo principal del disco compartido. Después de identificar el nodo principal, se pueden recuperar archivos al nodo principal del disco compartido.

Nota: Después de que suceda una conmutación por error, se tendrá que explorar el punto de recuperación de un agente diferente para descubrir el punto de recuperación deseado.

Siga estos pasos:

1. Inicie sesión en el agente que posee el disco compartido.
2. Abra el Asistente de restauración y seleccione Buscar archivos/carpetas para restauración.

   Nota: Para obtener más información sobre cómo restaurar los archivos y las carpetas, consulte Cómo restaurar archivos y carpetas.
3. Seleccione todos los archivos del Asistente de restauración que se desean restaurar a la ubicación original.
4. Complete las configuraciones del Asistente de restauración y envíe la tarea.

   Los archivos se recuperarán.
5. Inicie sesión en el nodo principal del disco compartido y verifique que los archivos se hayan recuperado.

   Los archivos del disco compartido se han recuperado.

Restauración de un nodo específico de un clúster

Si un nodo específico de un clúster está bloqueado, se puede realizar una reconstrucción completa solamente para ese nodo. Normalmente, en este escenario el disco compartido está en un buen estado y no necesita una recuperación.

Siga estos pasos:

1. Prepare la imagen BMR (CD/DVD o unidad de USB).
2. Elimine todas las conexiones entre el nodo que se desea recuperar y los discos compartidos.

   Ejemplo: Desconecte la conexión del canal de fibra óptica.
3. Realice una reconstrucción completa del nodo del clúster.

   Nota: Para obtener más información sobre cómo realizar una reconstrucción completa, consulte Cómo realizar una reconstrucción completa mediante una copia de seguridad.

   El nodo específico de un clúster se recupera.
4. Compruebe el estado del nodo recuperado en la consola de gestión del clúster y garantice que funciona como parte del clúster.

   El nodo específico de un clúster se recupera.

Restauración de un disco dañado compartido del clúster

El disco compartido pertenece a uno de los nodos del clúster. Si el disco compartido está dañado o roto, se pueden restaurar archivos o carpetas específicos del disco compartido, sin recuperar los nodos agrupados en clúster. Normalmente, en este escenario el disco de quórum y todos los nodos del clúster están en un buen estado.

Siga estos pasos:

1. Reemplace el disco dañado manualmente y vuelva a configurar el disco compartido del clúster.
2. Identifique al agente que es el propietario del disco compartido e inicie sesión en dicho agente.
3. Abra el Asistente de restauración y seleccione Buscar archivos/carpetas para restauración.

   Nota: Para obtener más información sobre cómo restaurar los archivos y las carpetas, consulte Cómo restaurar archivos y carpetas.
4. Seleccione todos los archivos del Asistente de restauración que se desean restaurar a la ubicación original.
5. Complete las configuraciones del Asistente de restauración y envíe la tarea.

   El disco compartido se ha recuperado.
6. Compruebe el estado del disco compartido en la consola de gestión del clúster y garantice que funciona como parte del clúster.

   El disco compartido se ha recuperado.

Restauración de todos los nodos agrupados en clúster y del disco compartido

Si toda la configuración del clúster está dañada o no funciona, se puede recuperar todo el clúster entero. La recuperar de todo el clúster entero es un proceso dos partes. Primero recupere los nodos agrupados en clústeres individuales utilizando la reconstrucción completa. A continuación, recupere los archivos y las carpetas del disco compartido.

Nota: Para los discos de quórum, reconstruya el disco utilizando la consola de gestión del clúster en lugar de recuperarlo mediante el Asistente de restauración en el Agente de Arcserve UDP (Windows).

Siga estos pasos:

1. Prepare la imagen BMR (CD/DVD o unidad de USB).
2. Elimine todas las conexiones entre el nodo que se desea recuperar y los discos compartidos.

   Ejemplo: Desconecte la conexión del canal de fibra óptica.
3. Realice una reconstrucción completa del nodo del clúster.

   Nota: Para obtener más información sobre cómo realizar una reconstrucción completa, consulte Cómo realizar una reconstrucción completa mediante una copia de seguridad.

   El nodo específico de un clúster se recupera.
4. Compruebe el estado del nodo recuperado en la consola de gestión del clúster y garantice que funciona como parte del clúster.

   El nodo específico de un clúster se recupera.
5. Repita los pasos para recuperar todos los nodos agrupados en clúster.

   Todos los nodos agrupados se han recuperado. Ahora recupere el disco compartido.
6. Reemplace el disco dañado manualmente y vuelva a configurar el disco compartido del clúster.
7. Identifique al agente que es el propietario del disco compartido e inicie sesión en dicho agente.
8. Abra el Asistente de restauración y seleccione Buscar archivos/carpetas para restauración.

Nota: Para obtener más información sobre cómo restaurar los archivos y las carpetas, consulte Cómo restaurar archivos y carpetas.

9. Seleccione todos los archivos del Asistente de restauración que se desean restaurar a la ubicación original.
10. Complete las configuraciones del Asistente de restauración y envíe la tarea.

    El disco compartido se ha recuperado.
11. Verifique los archivos del disco compartido y asegúrese de que los archivos se hayan recuperado.

    Todo el clúster entero se ha recuperado.

Cómo restaurar un Active Directory

Es necesario restaurar un sesión con copia de seguridad de Active Directory si dispone de alguno de los escenarios siguientes:

- Desea recuperar un atributo del objeto de Active Directory desde una sesión de Active Directory con copia de seguridad (no únicamente la última sesión de copia de seguridad).
- Desea recuperar el objeto de Active Directory desde una sesión de Active Directory con copia de seguridad (no únicamente la última sesión de copia de seguridad).
- Desea recuperar varios atributos u objetos de Active Directory desde una sesión de Active Directory con copia de seguridad (no únicamente la última sesión de copia de seguridad).

Importante: Para realizar una recuperación granular de Active Directory, se necesita una copia de seguridad basada en el agente.

Lista de objetos de Active Directory recuperados por la restauración a nivel del objeto		
Unidad de organización	Sitio	Clase de elementos perdidos y encontrados
Usuario	Contenedor de sitio	Clase de dominio integrada
Grupo	Vínculo de sitio	Clase de zona DNS
Equipo	Puente de vínculo de sitio	Clase de dominio
Contacto	Configuración de sitio	Clase de DNS de dominio
Conexión	Contenedor de subred	Clase de DMD
Carpeta compartida	Dominio de confianza	Clase de unidad organizativa
Impresora	Clase de configuración	Clase de Containerecifiers

El escenario describe cómo se puede restaurar un Active Directory.



Realice las tareas siguientes para restaurar un Active Directory:

1. Revisión de las consideraciones y requisitos previos de la restauración
2. Restauración de un Active Directory
3. Verificación de que Active Directory se ha restaurado

Revisión de las consideraciones y requisitos previos de la restauración

Verifique que los requisitos previos siguientes existen antes de realizar una restauración:

- Ya se ha realizado la copia de seguridad de los volúmenes que incluyen la carpeta de base de datos de Active Directory y la carpeta Archivos de registro.
- Tiene el Agente de Arcserve UDP (Windows) instalado en el controlador de dominios.
- Se ha realizado una copia de seguridad basada en el agente.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones sobre la restauración:

- Si desea garantizar que se pueden explorar y seleccionar archivos/carpetas para la restauración para un punto de recuperación sin haber creado un catálogo del sistema de archivos, antes de realizar la copia de seguridad será necesario conceder permisos de acceso a la cuenta o al grupo para todas las carpetas y todos los archivos de los volúmenes con acceso de lectura o lista.
- Se puede realizar una restauración de Active Directory únicamente en el Agente de Arcserve UDP (Windows).

Restauración de Active Directory

Después de haber instalado Active Directory en distintos volúmenes y haber realizado una copia de seguridad de ambos volúmenes, podrá restaurar los volúmenes junto con Active Directory. Este escenario describe cómo se pueden restaurar los volúmenes de Active Directory con copia de seguridad.

Nota: Verifique que han completado los requisitos previos y que se ha realizado una copia de seguridad de los volúmenes de Active Directory.

Siga estos pasos:

1. Acceda al cuadro de diálogo Selección del método de recuperación de una de las formas siguientes:

   Desde Arcserve UDP:

   a. Inicie sesión en Arcserve UDP.

   b. Haga clic en la ficha **recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos de agregados en el panel central.

   d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   e. Haga clic en **Restaurar** del menú desplegable **Acción**.

      El cuadro de diálogo Selección del método de restauración se abre.

      Nota: Se inicia sesión automáticamente en el nodo del Agente y el cuadro de diálogo Selección del método de restauración se abre desde el nodo del Agente.

   Desde el Agente de Arcserve UDP (Windows):

   a. Inicie sesión en el Agente de Arcserve UDP para Windows.

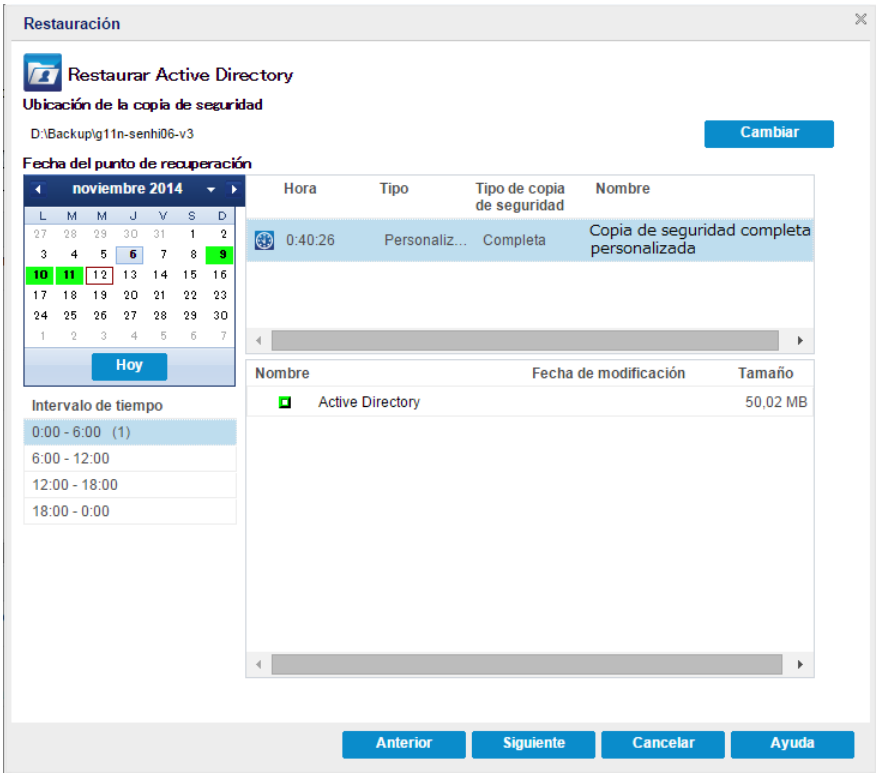
   b. En la página principal, seleccione **Restaurar**.

   El cuadro de diálogo Selección del método de restauración se abre.

2. En la pantalla Restauración, seleccione Restaurar Active Directory.

   Aparece el cuadro de diálogo Restaurar Active Directory.

3. En la pantalla Restaurar Active Directory, realice los pasos siguientes:



a. En el calendario, seleccione la fecha de copia de seguridad para Active Directory que desee restaurar.

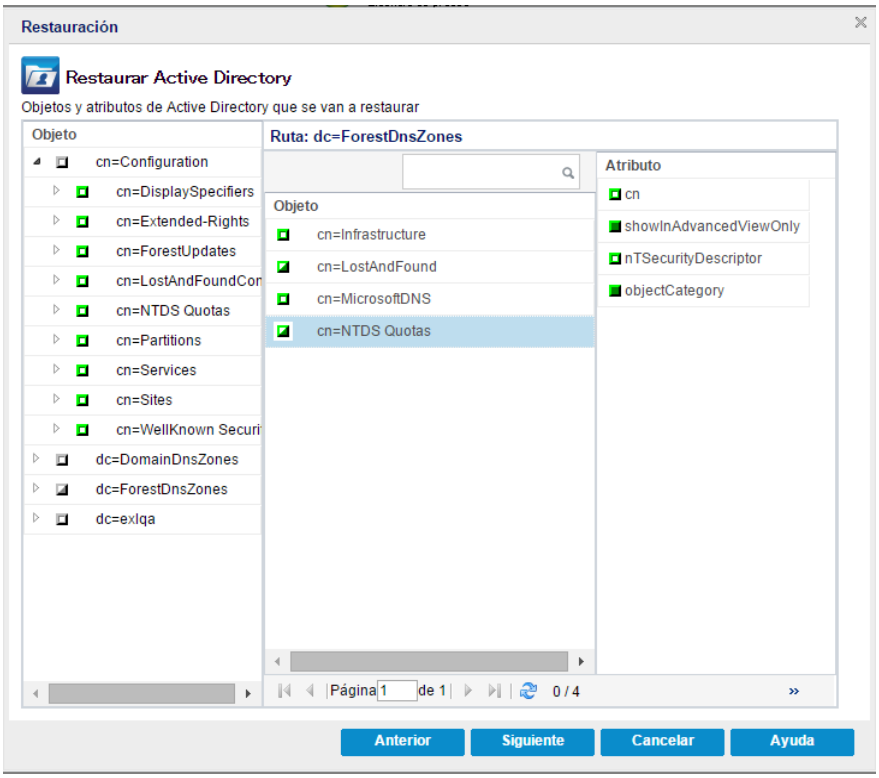
b. En el Intervalo de tiempo, seleccione Hora de copia de seguridad.

c. En la pantalla Restaurar Active Directory, seleccione un punto de recuperación identificado con Hora, Tipo, Tipo de copia de seguridad y Nombre.

d. En la sección Nombre, seleccione una sesión de copia de seguridad de Active Directory para restaurar.

4. Haga clic en Siguiente.

5. Seleccione las opciones siguientes para definir los objetos, la ruta y los atributos para restaurar:



a. En la columna Objeto, seleccione el nombre de un objeto. Aparecerán las rutas relacionadas con el objeto seleccionado.

b. En la columna Ruta, seleccione una ruta. Aparecerán los atributos relacionados con la ruta seleccionada.

   Nota: Se puede utilizar el icono de búsqueda para explorar la ruta.

c. En la columna Atributo, seleccione uno o más atributos.

6. Haga clic en Siguiente.

   Aparecerá el cuadro de diálogo Opciones de restauración.

7. En las Opciones de restauración, seleccione los objetos siguientes si es necesario:

   a. Si el objeto seleccionado se ha renombrado después de la copia de seguridad, seleccione la opción Restaurar con el nombre original para restaurar el objeto renombrado.

      Nota: Si no se selecciona esta opción, el objeto no se restaurará.

   b. Si el objeto seleccionado se ha desplazado a otro contenedor después de la copia de seguridad, seleccione la opción Restaurar en la ubicación original para restaurar el objeto desplazado.

      Nota: Si no se selecciona esta opción, el objeto no se restaurará.

c. Si el objeto seleccionado se ha suprimido permanentemente después de la copia de seguridad, haga clic en la opción Restaurar con el nuevo ID de objeto para restaurar el objeto que se ha suprimido de forma permanente.

   Nota: Utilice esta opción para que el objeto restaurado mantenga el nuevo ID de objeto.

8. Haga clic en Siguiente.

   Aparecerá la pantalla Resumen de la restauración.

9. Revise los detalles y realice una de las acciones siguientes:

   - Haga clic en Anterior si se desea modificar los detalles.
   - Haga clic en Finalizar para ejecutar restauración.

   Aparece un mensaje de estado para informarle en el momento en que la tarea de restauración haya finalizado. Si la restauración es incorrecta, consulte los registros e inténtelo de nuevo.

Verificación de que Active Directory se ha restaurado

Después de finalizar el proceso de restauración, puede utilizar la utilidad Usuarios y equipos de Active Directory para comprobar que el (objeto y/o atributo) de Active Directory se haya restaurado en el destino especificado.

Nota: La utilidad de Active Directory se ha instalado automáticamente con el Active Directory.

Cómo restaurar datos de Active Directory utilizando la utilidad Restauración de nivel de objeto de Active Directory de Arcserve UDP

Después de haber instalado Active Directory en distintos volúmenes y haber realizado una copia de seguridad de ambos volúmenes utilizando una tarea de copia de seguridad sin agente basada en el host, es posible que desee restaurar objetos y atributos de Active Directory de forma granular. En este escenario se describe cómo restaurar los objetos y atributos de Active Directory de los que se ha realizado la copia de seguridad a partir de sus volúmenes.

Antes de realizar una restauración, asegúrese de que están disponibles los siguientes requisitos previos:

- La utilidad Restauración de nivel de objeto de Active Directory está disponible en la siguiente ubicación:

  <Ruta de instalación de Arcserve UDP>\Engine\BIN\

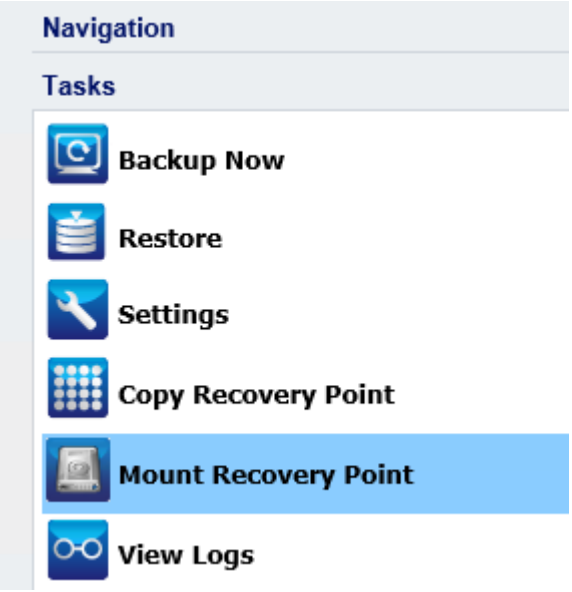
  Nota: La herramienta se instala con el Agente de Arcserve UDP.
- La tarea de restauración está configurada para ejecutarse desde el equipo proxy de copia de seguridad basada en el host.

  Nota: Si desea ejecutar la tarea de restauración en cualquier otro equipo, busque el punto de recuperación desde el destino de la copia de seguridad.
- La ruta de acceso a la base de datos de Active Directory (NTDS.dit) se identifica para realizar la tarea de restauración.

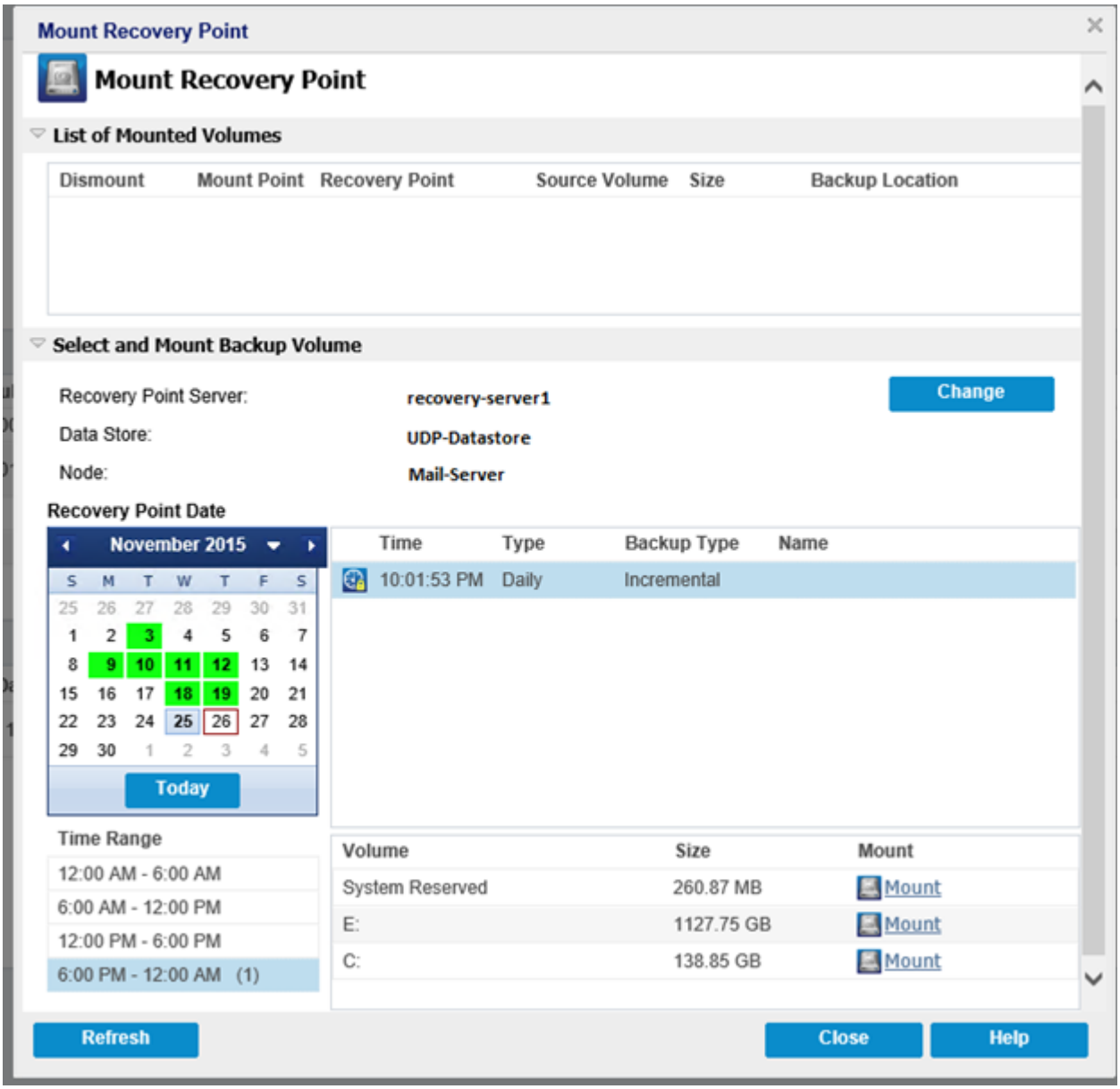
  Nota: De forma predeterminada, la ruta de acceso a NTDS.dit es C:\Windows\NTDS\NTDS.dit.

Siga estos pasos:

1. En la Consola del Agente de Arcserve UDP en el equipo proxy de la copia de seguridad basada en el host, seleccione la tarea Montar punto de recuperación. Aparecerá el cuadro de diálogo Montar punto de recuperación.

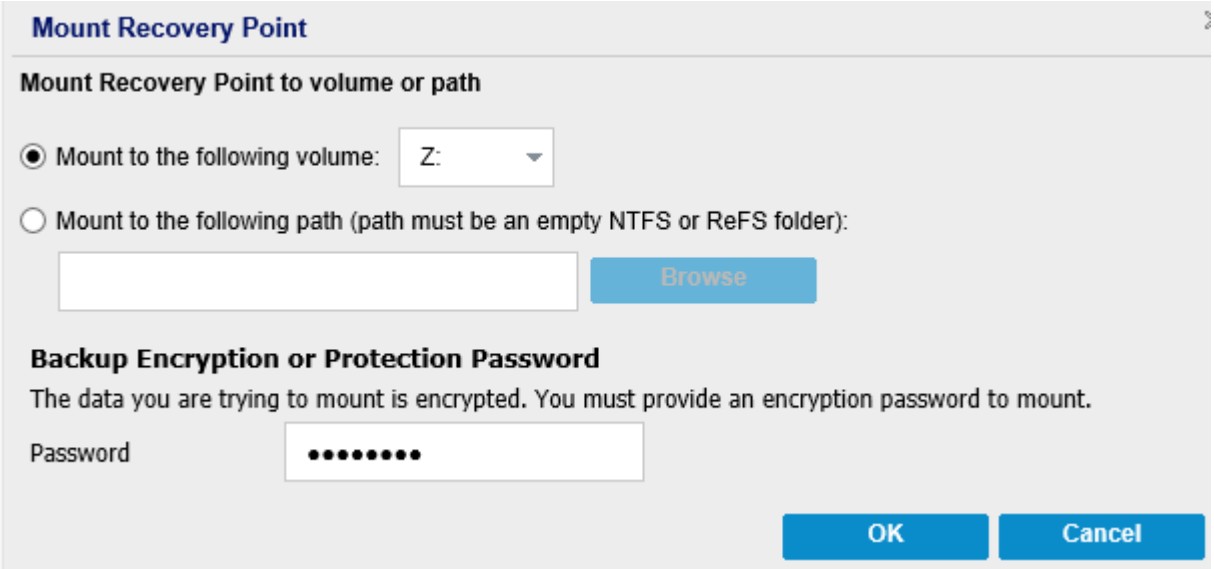


2. Seleccione la fecha del punto de recuperación.
3. Para obtener el volumen que contiene la base de datos de Active Directory, haga clic en **Montar**.



Nota: Si el servidor que está ejecutando la tarea de restauración no es el proxy HBBU, haga clic en **Cambiar** para seleccionar el servidor de puntos de recuperación, el almacén de datos y el servidor de Active Directory apropiados.

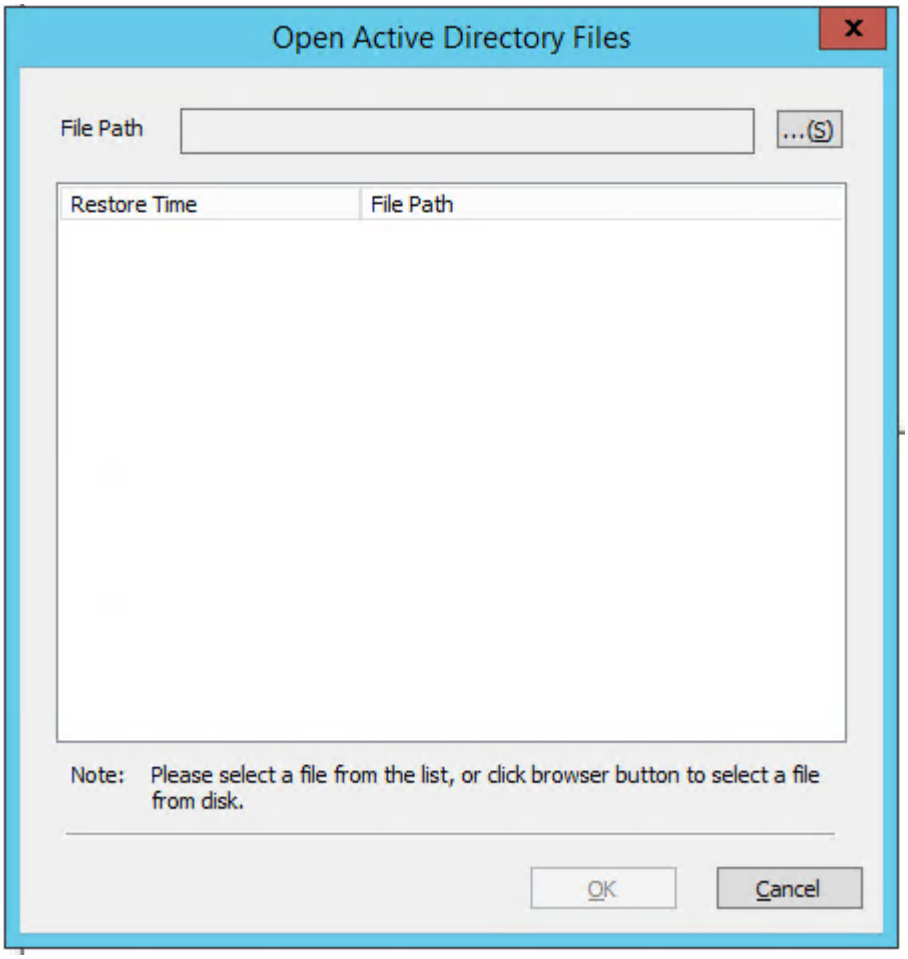
4. Seleccione la letra de unidad de disco para montar el volumen y haga clic en **Aceptar**.



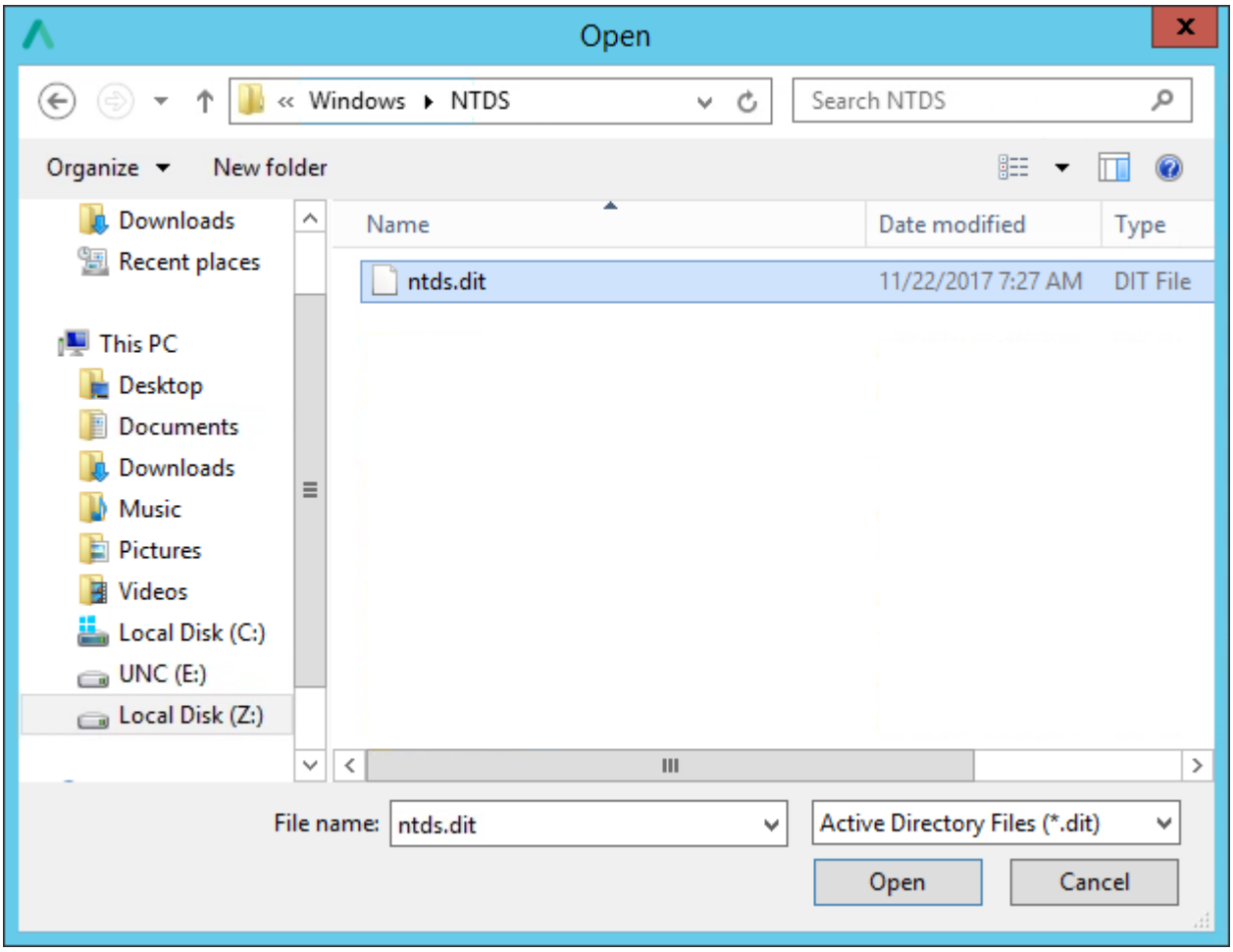
5. Inicie la utilidad Restauración de nivel de objeto de Active Directory desde la siguiente ubicación:

   <Ruta de instalación de Arcserve UDP>\Engine\BIN\AD_restore.exe

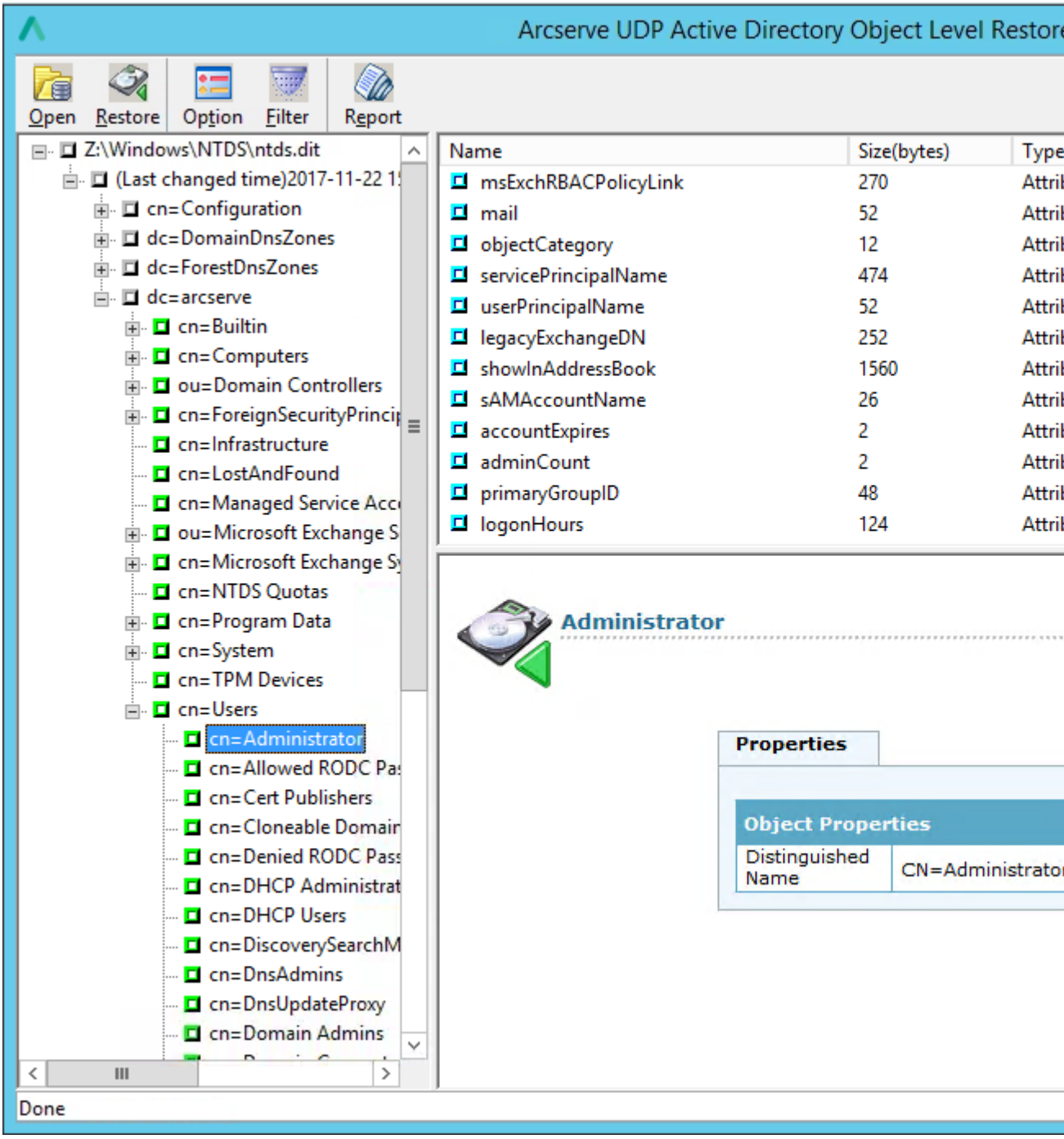
6. Haga clic en **Abrir** para abrir la ventana de selección.



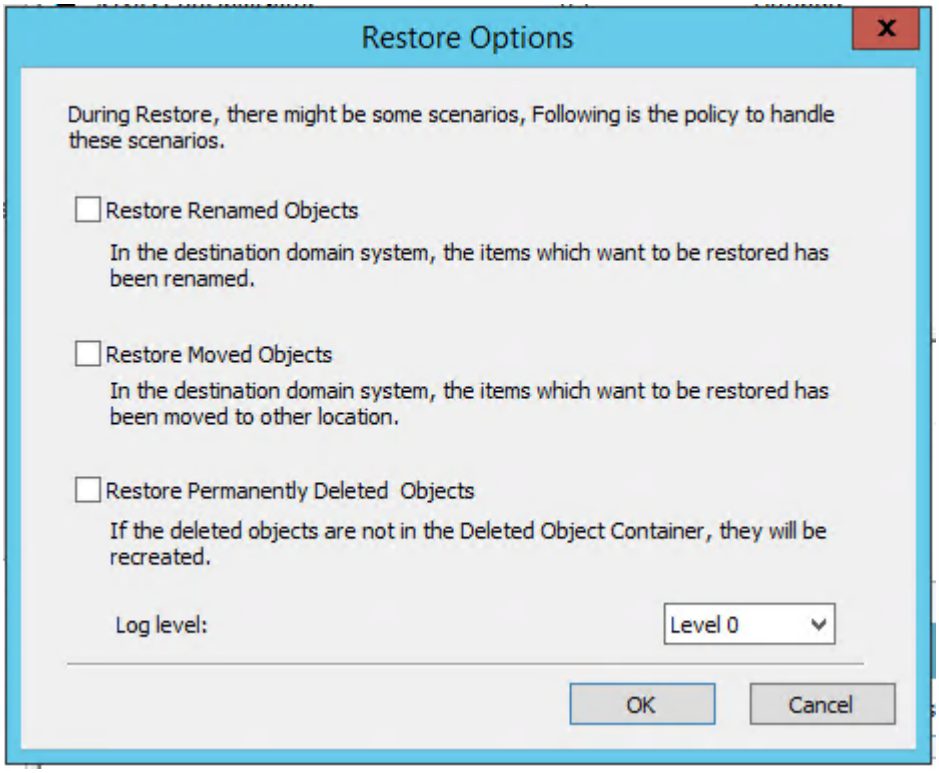
7. Haga clic en el icono ...(S), examine la base de datos de Active Directory (NTDS.dit) en el punto de recuperación montado, haga clic en **Abrir** y, a continuación, haga clic en **Aceptar**.



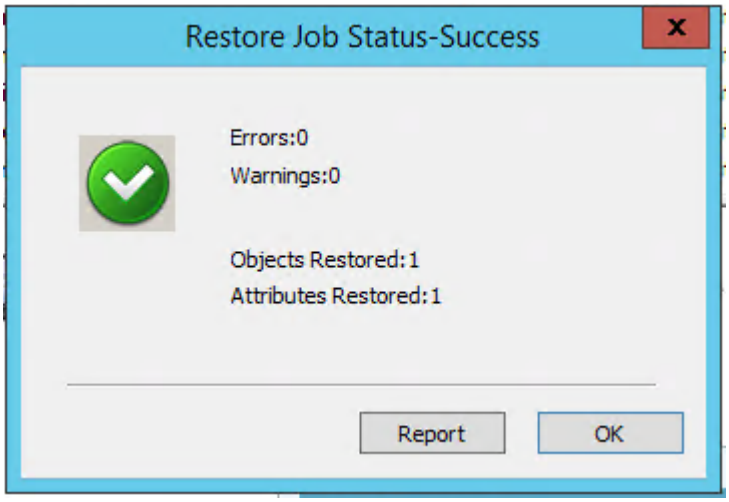
8. Busque y seleccione los objetos o atributos de Active Directory que desea restaurar.



9. Haga clic en **Opciones** para realizar ajustes en el comportamiento pre-determinado, según sea necesario.



10. Cuando esté listo, haga clic en **Aceptar** para ejecutar la tarea de restauración.
11. Una vez finalizada la tarea de restauración, se muestra una ventana de resultados. Haga clic en **Informe** si desea ver los detalles o en **Aceptar** para cerrar.



Notas:

- De forma predeterminada, la utilidad utiliza el usuario que ha iniciado sesión en Windows para establecer la conexión.
- Si se notifica un error, la acción recomendada es iniciar sesión en el equipo con una cuenta que tenga derechos de administrador del dominio para realizar la restauración.

12. Cuando se complete la tarea de restauración, desmonte el volumen que se ha utilizado para la recuperación.
13. Para desmontar el volumen, en la Consola del Agente de Arcserve UDP en el equipo de copia de seguridad basada en el host, haga clic en **Montar punto de recuperación** y, a continuación, haga clic en **Desmontar**.



Cómo restaurar los datos de Microsoft Office 365

Esta sección incluye los siguientes temas:

Cómo restaurar los datos del buzón de correo de Exchange Online

Se pueden restaurar los datos del buzón de correo de Exchange Online (correos electrónicos, calendarios, contactos, notas, tareas, etc.) desde la nube de Microsoft utilizando cualquier equipo. Se pueden restaurar datos desde el punto de recuperación a la ubicación original o a una ubicación alternativa.

Realice las tareas siguientes para restaurar los datos del buzón de correo de Exchange Online:

1. Selección de los elementos del buzón de correo Exchange Online que se deben restaurar
2. Definición de las opciones de restauración
3. Restauración de los elementos recuperables
4. Restauración del contenido del punto de recuperación
5. Verificación de que se ha restaurado el contenido

Selección de los elementos de correo de Exchange Online que se deben restaurar

Se pueden restaurar los datos de correo de Exchange Online desde un punto de recuperación. Cuando se selecciona una fecha de recuperación y, a continuación, se especifica el tiempo, se muestran todos los puntos de recuperación asociados para esa duración. Tiene la opción de explorar y seleccionar el contenido de la copia de seguridad (incluyendo las aplicaciones) que se debe restaurar.

Siga estos pasos:

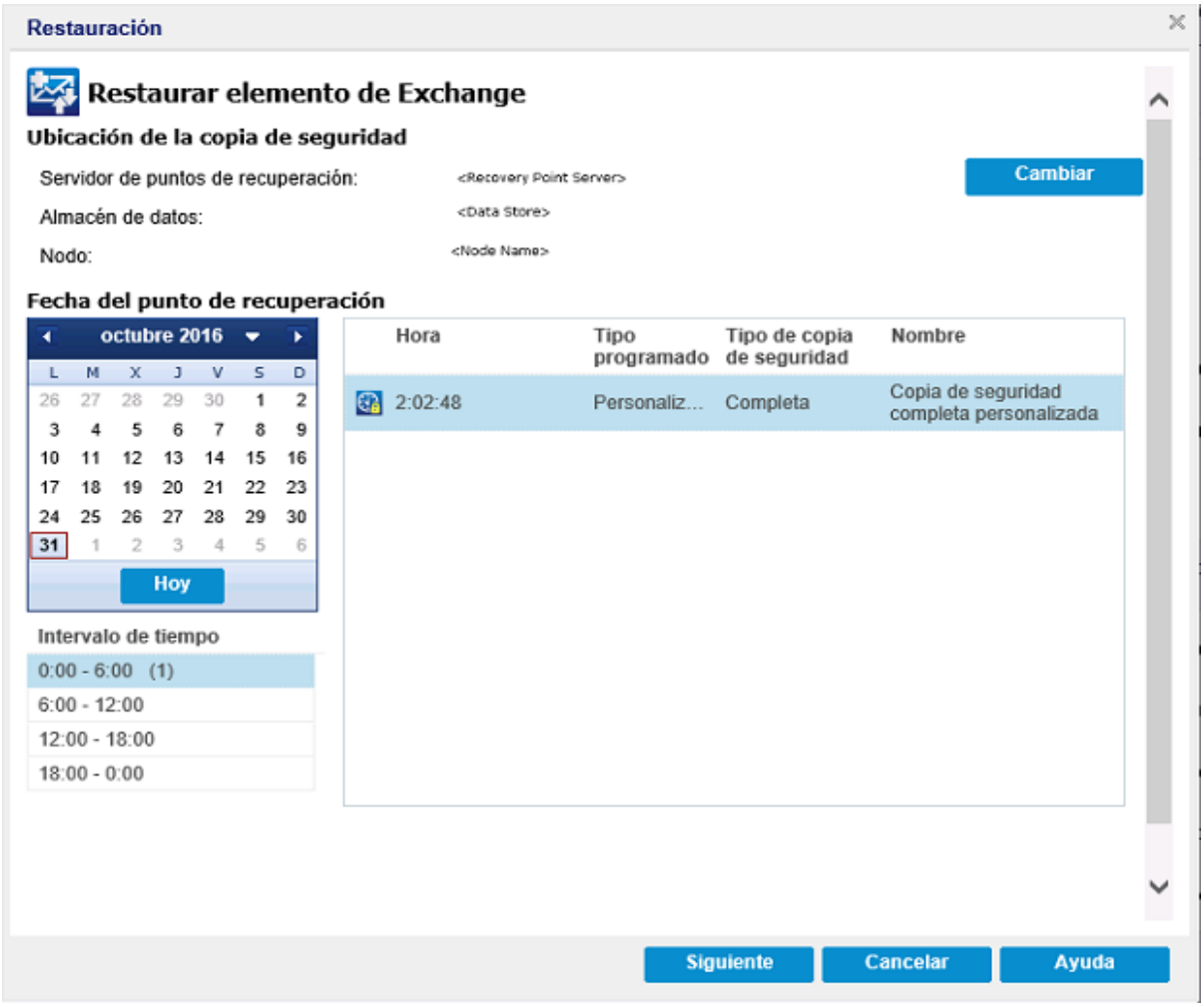
1. Inicie sesión en Arcserve UDP.
2. Haga clic en la ficha **recursos**.
3. Seleccione **Todos los nodos** en el panel izquierdo.

   Se muestran todos los nodos de agregados en el panel central.
4. En el panel central, seleccione el nodo Exchange Online y, a continuación, haga clic en **Acciones**.
5. Haga clic en **Restaurar** del menú desplegable Acción.

   Se abre el cuadro de diálogo Restaurar elemento de Exchange.

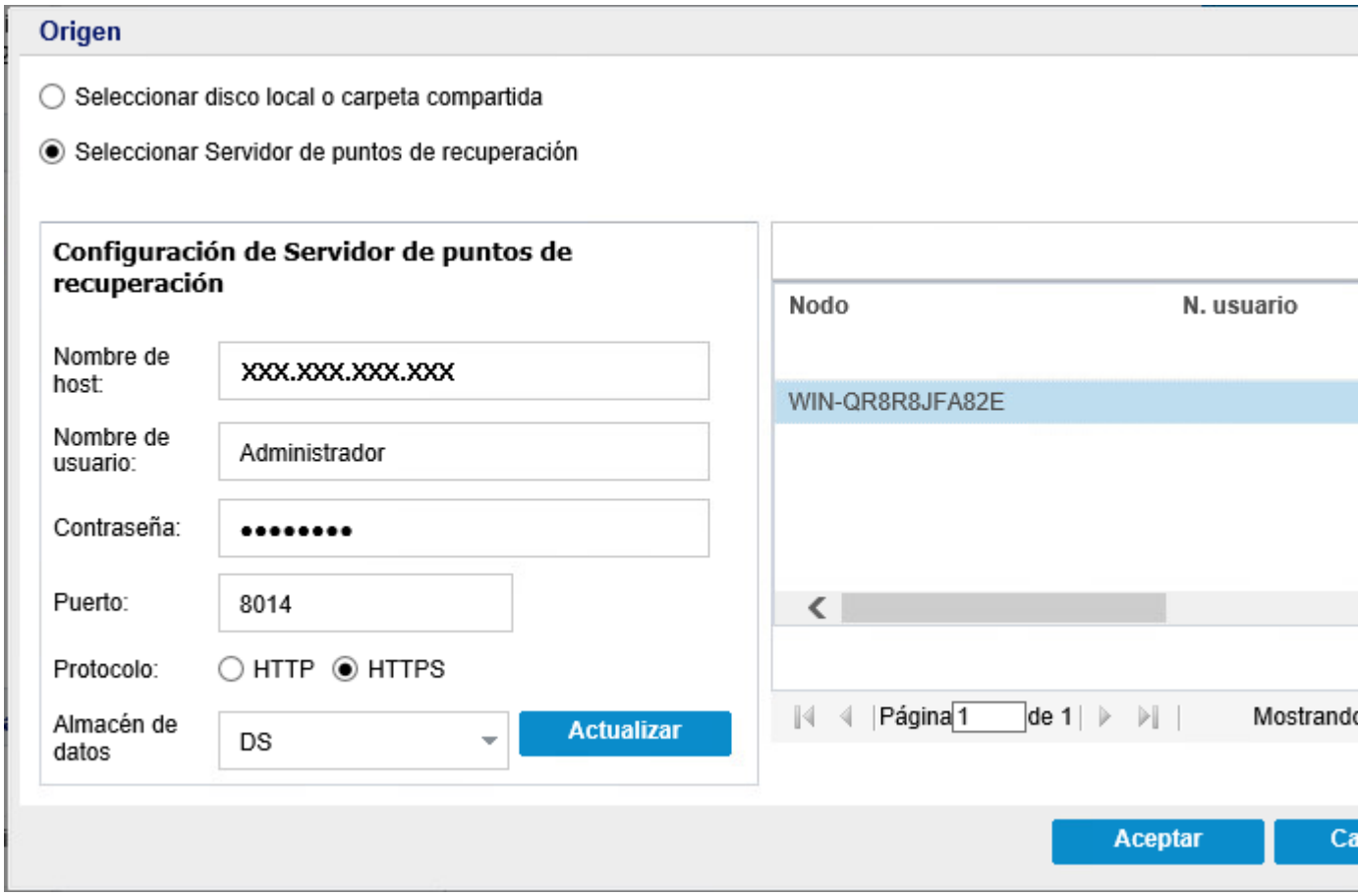
   Nota: Se inicia sesión automáticamente en el nodo del agente y se abre el cuadro de diálogo Restaurar elemento de Exchange.

   Se pueden ver los detalles del Servidor de puntos de recuperación en la Ubicación de la copia de seguridad.



6. (Opcional) Haga clic en **Cambiar** si se desea cambiar la ubicación de la copia de seguridad.

   Se abrirá el cuadro de diálogo Origen. Se puede seleccionar la ubicación de la copia de seguridad en este cuadro de diálogo.



Nota: Cuando se agrega una tarea de copia en cinta al plan y ahora se desea restaurar el punto de recuperación de la copia de seguridad de la copia en cinta, seleccione el punto de recuperación en la copia de seguridad de la copia en cinta. Para obtener más información, consulte Exploración del punto de recuperación de la copia en cinta para la restauración.

7. Para especificar el origen, seleccione una de las siguientes opciones y, a continuación, haga clic en **Aceptar**:

   Seleccionar disco local o carpeta compartida

   Nota: En Arcserve UDP, no se recomienda seleccionar la opción **Seleccionar disco local o carpeta compartida**.

   Seleccionar servidor de puntos de recuperación

   a. Especifique los detalles del valor de configuración del servidor de puntos de recuperación y, a continuación, haga clic en **Actualizar**.

      Todos los agentes se muestran en la columna Agente de protección de datos en el cuadro de diálogo Origen.

b. Seleccione el agente en la lista mostrada y, a continuación, haga clic en **Aceptar**.

   Los puntos de recuperación se enumeran en el cuadro de diálogo Restaurar elemento de Exchange.

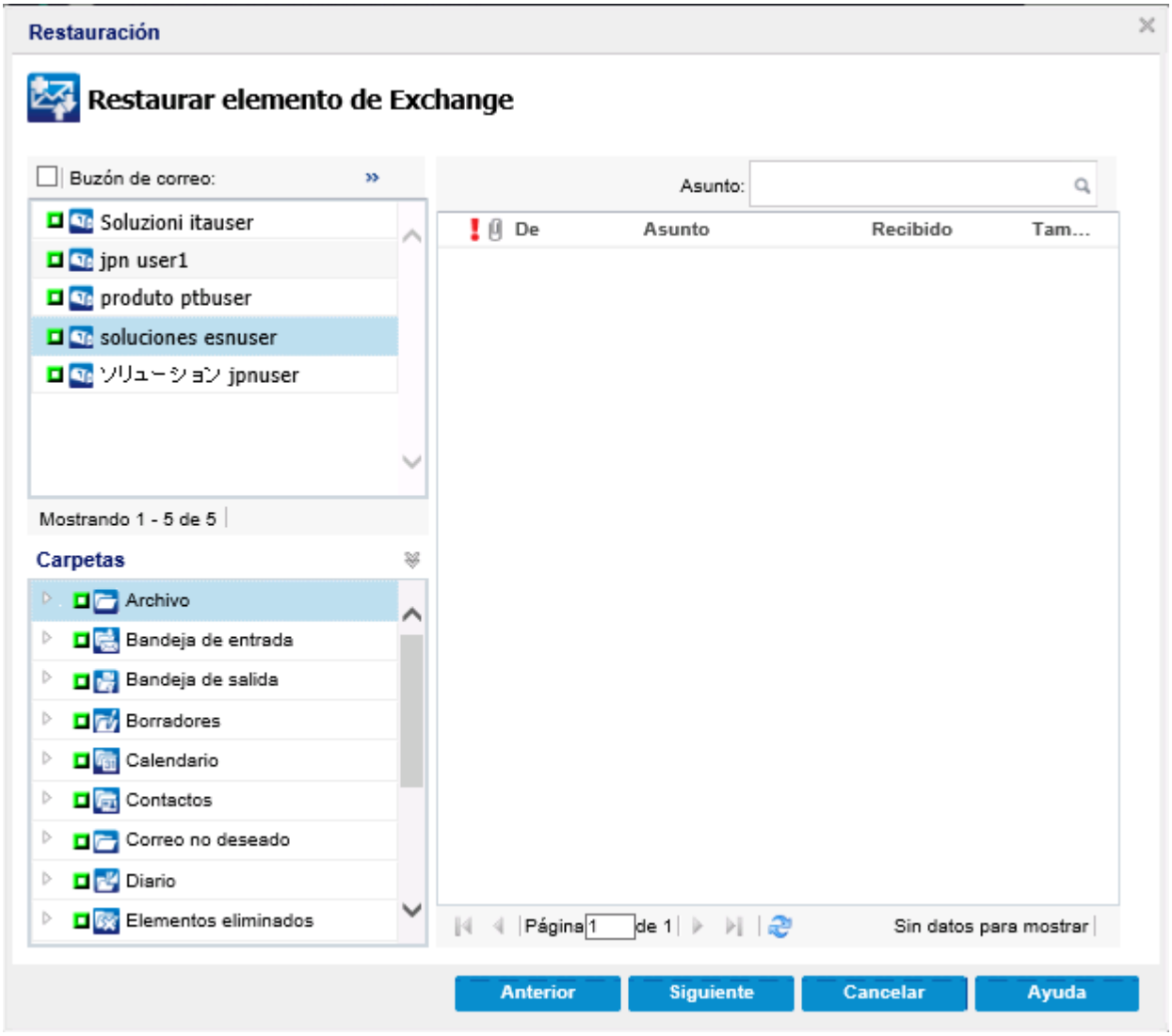
   Nota: Desde el punto de recuperación Carpeta, se pueden ver muchas carpetas con el mismo nombre junto con los nodos de Exchange Online. Esto sucede debido a que el GUID del nodo cambia y se crea una nueva carpeta del punto de recuperación cuando se suprime un nodo y se vuelve a agregar al plan de prueba.

8. Seleccione la fecha de calendario para restaurar la imagen de la copia de seguridad y, a continuación, haga clic en **Siguiente**.

   Todas las fechas que contienen puntos de recuperación para el origen de la copia de seguridad especificado se resaltan en verde.

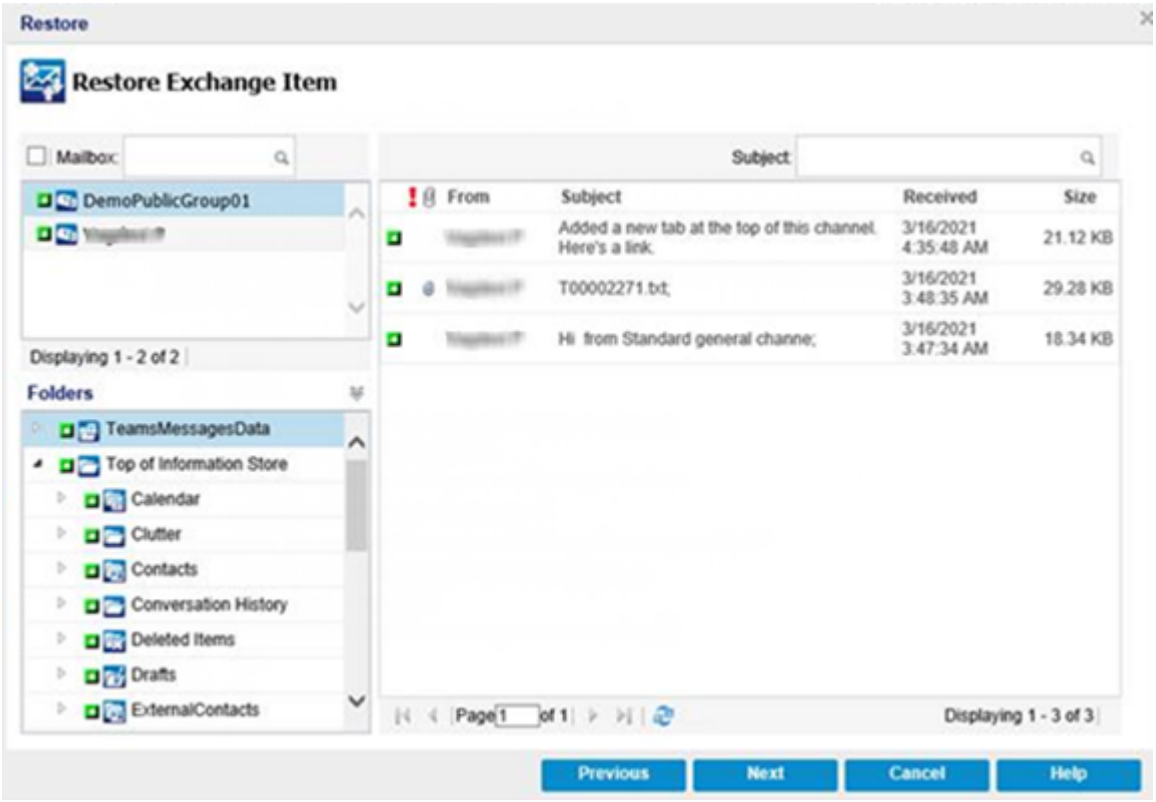
   Aparecerán los puntos de recuperación correspondientes para la fecha, junto con la hora de la copia de seguridad, el tipo de copia de seguridad que se realiza (completa, incremental o de verificación) y el nombre de la copia de seguridad.

9. En el panel Buzón de correo, haga clic en el buzón de correo que se desea restaurar.



Se muestran todos los elementos de correo relacionados con el buzón de correo en el panel Carpetas.

Nota: Para la copia de seguridad de los grupos de Exchange Online de Office 365, la estructura de carpetas para el buzón de correo del grupo es diferente de la del buzón de correo del usuario. Las carpetas del buzón de correo del grupo se muestran en la parte superior de la carpeta Almacén de información. Por ejemplo, cuando el usuario realiza copias de seguridad de buzones de correo o de listas de distribución del grupo de AD, todas las carpetas de las que se realiza la copia de seguridad se muestran en la parte superior de la carpeta Almacén de información.



10. Seleccione los elementos o carpetas relacionados con el correo (incluyendo el buzón de correo completo, los correos electrónicos, los calendarios, los contactos, las notas, las tareas, etc.) que se desean restaurar a partir de Carpetas y, a continuación, haga clic en **Siguiente**.

    Notas:

    - Se puede seleccionar todo el contenido o el contenido parcial del objeto de Exchange para restaurar. Para seleccionar parte del contenido, expanda el objeto y haga clic en la casilla de verificación de dicho contenido.
    - Se pueden seleccionar objetos de Exchange múltiples para restaurar.

    Se abrirá el cuadro de diálogo Opciones de restauración.

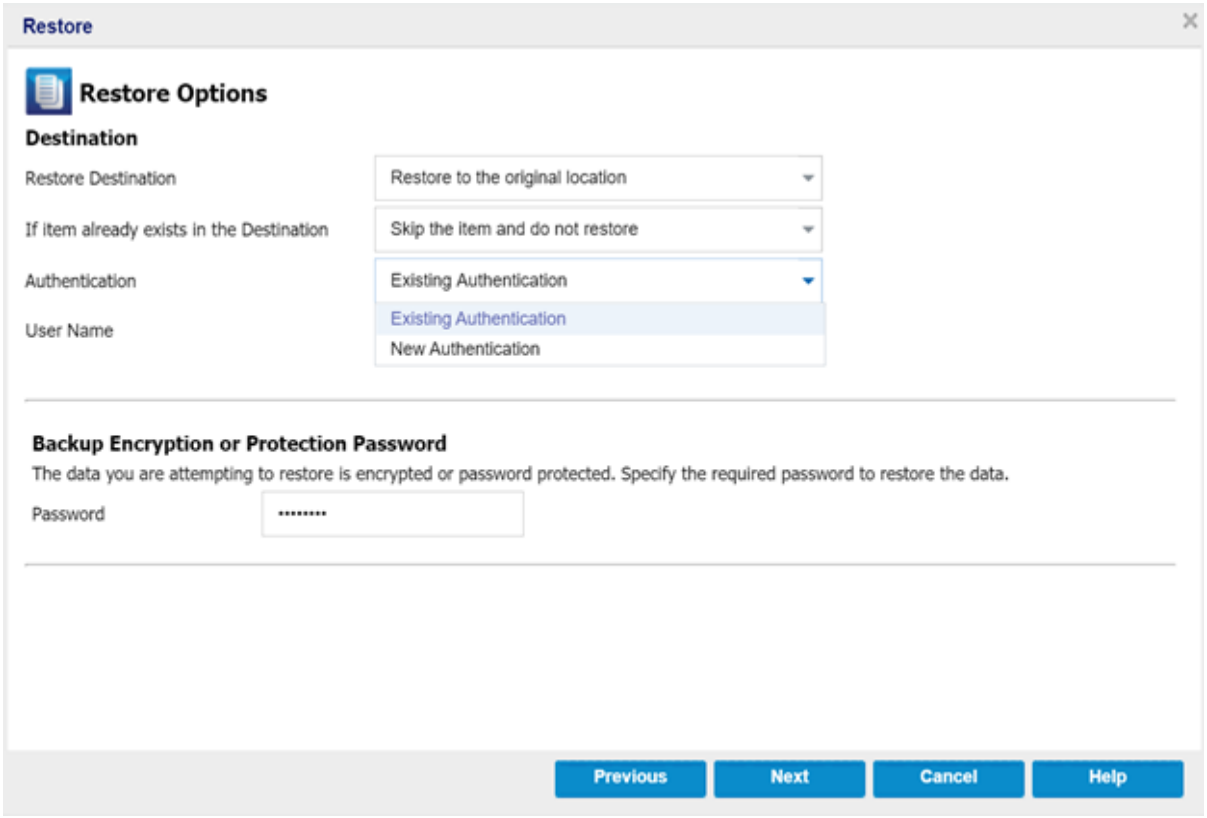
    Se han seleccionado los elementos de correo de Exchange Online que se deben restaurar. Ahora, se pueden definir las opciones de restauración.

Definición de las opciones de restauración

Después de especificar la información de Exchange Online que se debe restaurar, defina las opciones de restauración para el contenido seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, seleccione el destino para la restauración.



A continuación se especifican las opciones de destino disponibles:

Restauración en la ubicación original

Restaura los datos del correo en la misma ubicación desde donde se ha realizado una copia de seguridad.

Notas:

- Si se restaura dos veces un mismo elemento de correo en la ubicación original mediante la opción Sobrescribir, tras la segunda restauración, el primer elemento de correo restaurado no se sobrescribe. De este modo, aparecen dos elementos de correo similares en la ubicación original.

- Si se restaura un elemento de correo en la ubicación original mediante la opción Omitir y en la carpeta original ya existe un elemento similar al elemento restaurado, la tarea de copia de seguridad muestra un resultado incompleto.

Restaurar en una ubicación alternativa

Restaura los datos del correo a otro buzón de correo o a otra carpeta del buzón de correo original. Cuando se selecciona esta opción, se puede examinar y seleccionar el destino.

2. Especifique una de las siguientes opciones del menú desplegable **Si el elemento ya existe en el destino**:

Omitir el elemento y no restaurar

Se omiten los elementos y no se restaurará.

Valor predeterminado: La opción Omitir el elemento y no restaurar.

Sobrescribir el elemento en el destino

Sobrescribe el elemento en el destino.

Nota: La lista desplegable **Si el elemento ya existe en el destino** está disponible si se selecciona la opción **Restaurar en la ubicación original** en la lista desplegable **Destino de la restauración**.

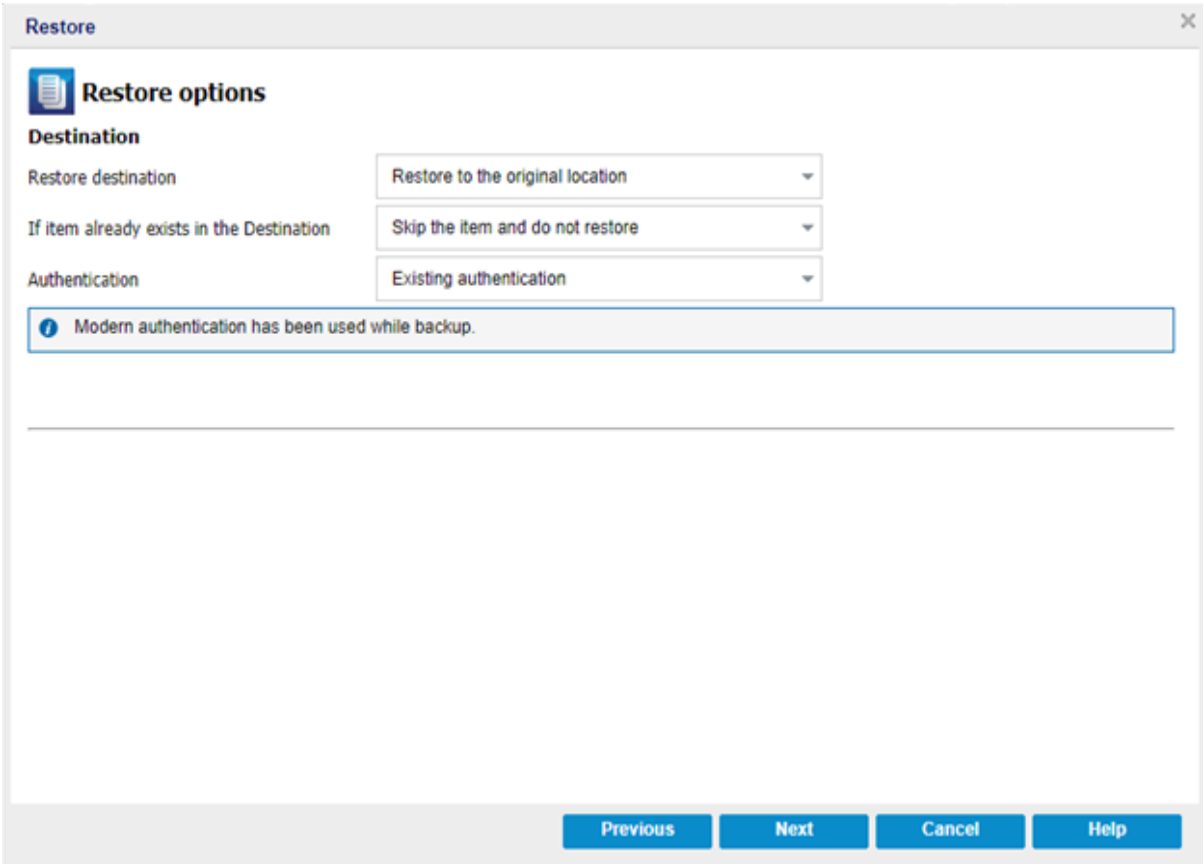
Autentificación

Valida e identifica la cuenta de usuario. Seleccione una de las opciones siguientes:

- **Autenticación existente**

  Cuando se selecciona Autenticación existente, se utiliza el tipo de autenticación que se ha seleccionado durante la creación del nodo.

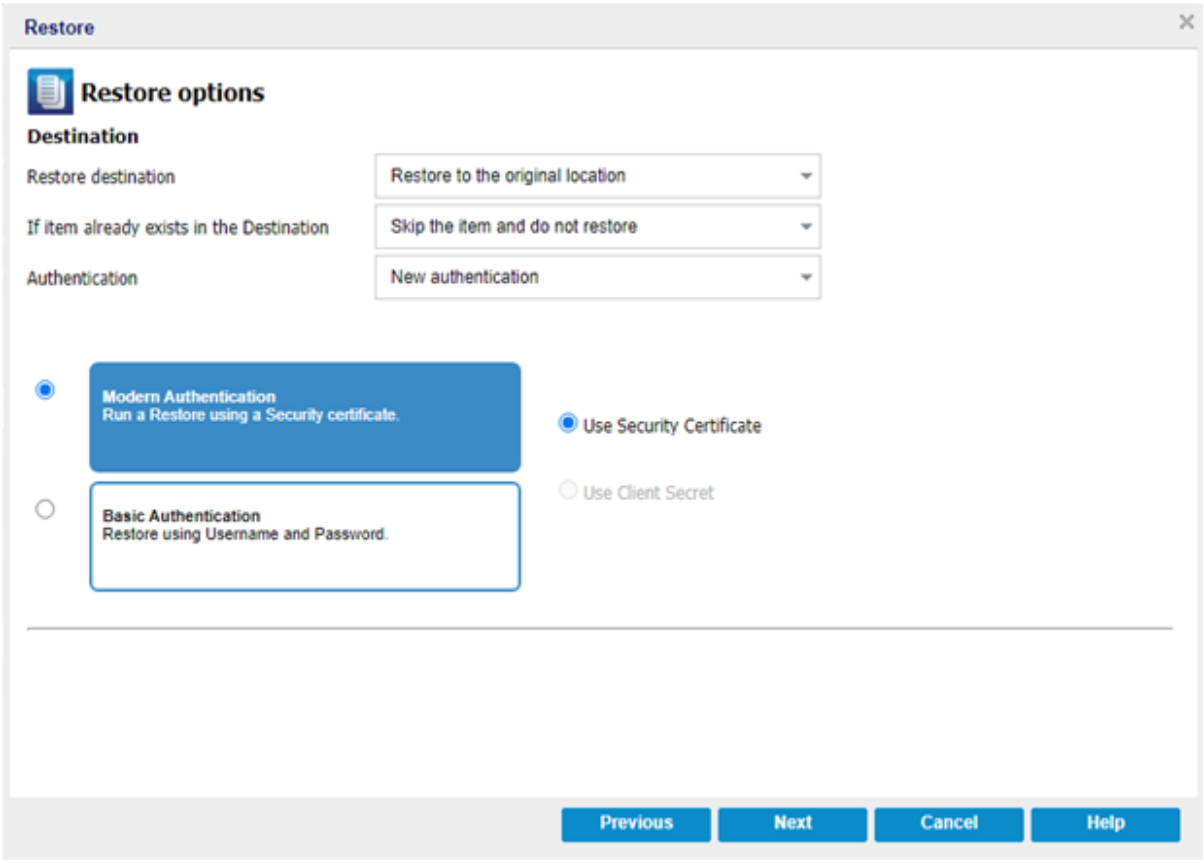
  - Si la autenticación del nodo es básica, se cargan automáticamente parámetros como Nombre de usuario, Contraseña y Cifrado de la copia de seguridad o Contraseña de protección [Si está cifrada] para continuar con la restauración.
  - Si la autenticación del nodo es moderna, se cargan automáticamente parámetros como Nombre de usuario y Cifrado de la copia de seguridad o Contraseña de protección [Si está cifrada] para continuar con la restauración.



- **Nueva autenticación**

  Durante la restauración, se puede seleccionar una de las siguientes opciones para cambiar el tipo de autenticación:

  - Autenticación moderna
  - Autenticación básica



3. Para aplicar la autenticación, realice una de las siguientes acciones:

   Autenticación moderna

   Para la autenticación moderna, se puede ejecutar una restauración utilizando un certificado de seguridad.

   Utilizar certificado de seguridad

   Nota: De forma predeterminada, el plan de copia de seguridad selecciona **Utilizar certificado de seguridad** para la autenticación moderna.

   Siga estos pasos:

   a. Para autenticarse mediante un certificado autofirmado, consulte Descarga del certificado desde UDP y carga del certificado en Azure.

   b. Introduzca el ID de la aplicación y el Nombre de usuario.

   c. Para aplicar los roles y permisos necesarios, seleccione la casilla de verificación **Permitir a Arcserve UDP establecer los roles y permisos de Azure necesarios para esta aplicación** y, a continuación, haga clic en **Siguiente**.

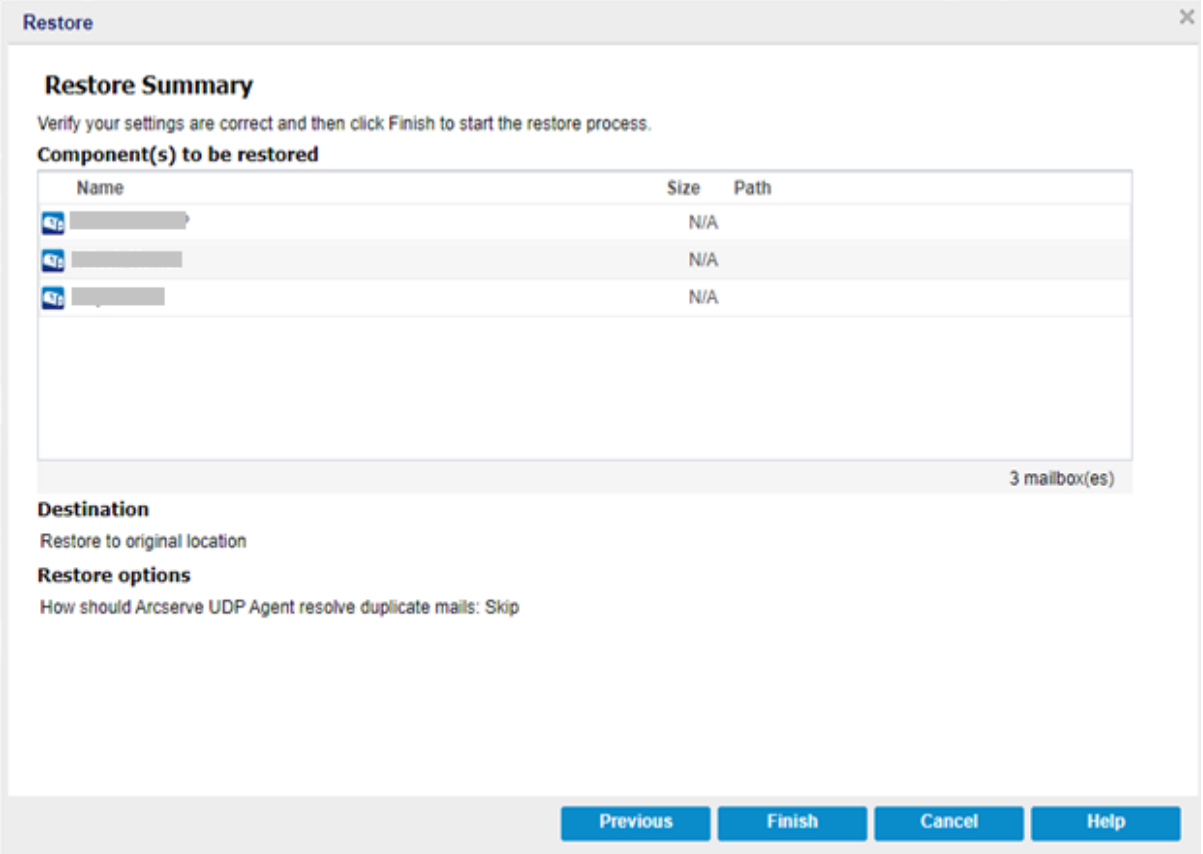
Autenticación básica

Para la Autenticación básica, introduzca el Nombre de usuario y la Contraseña para continuar con la restauración.

Nota: Esta opción produce un error si tiene activada la autenticación moderna en el inquilino o en la cuenta.

4. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Resumen de la restauración**.



5. En la ventana Resumen de la restauración, verifique la configuración y, a continuación, haga clic en **Finalizar**.

Las opciones de restauración se han definido para restaurar la información de Exchange Online.

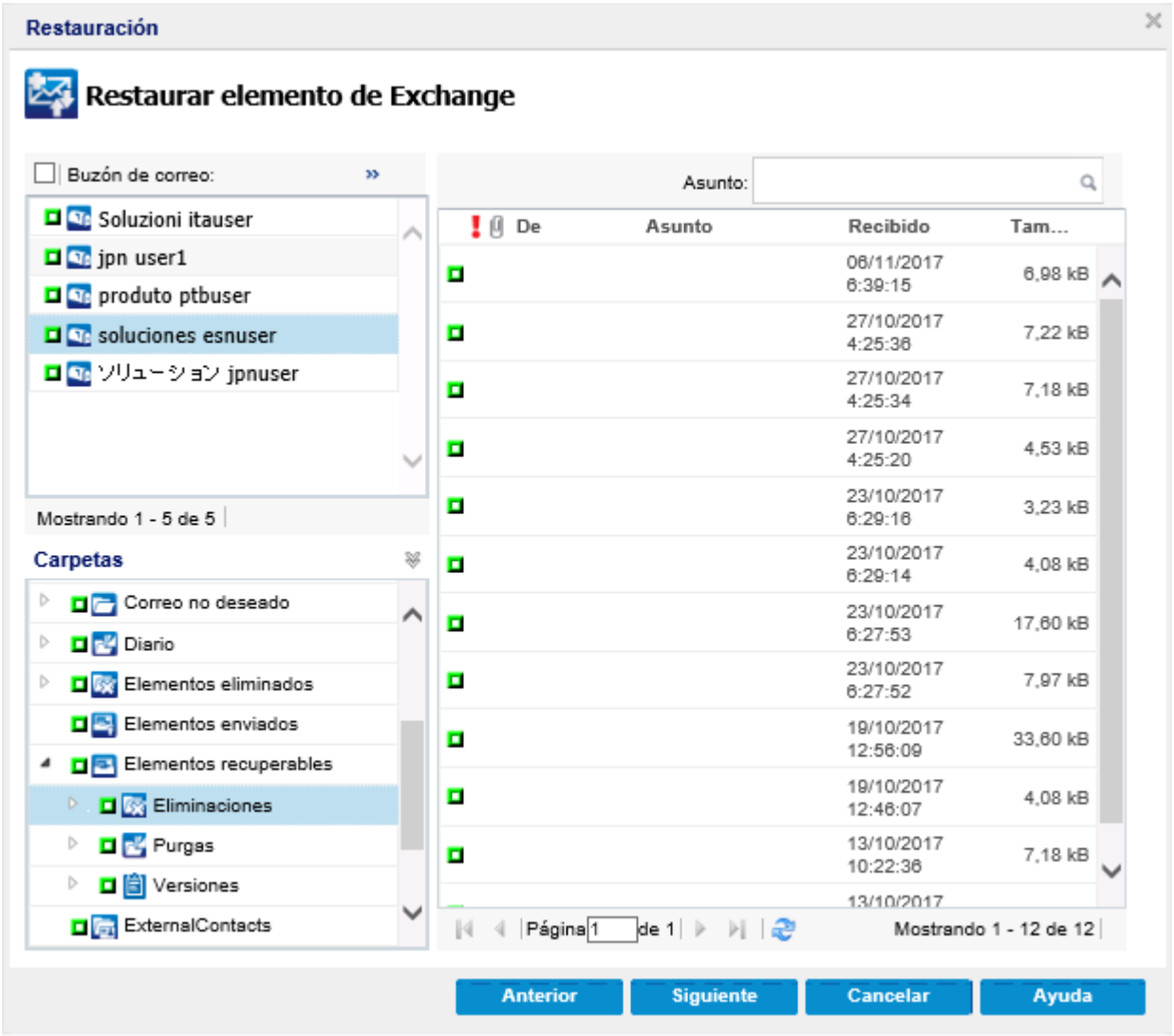
Restauración de los elementos recuperables

Se pueden restaurar los elementos recuperables del buzón que permite la característica In-Place Hold or Litigation Hold desde la interfaz de usuario del nodo de Exchange Online para examinar la sesión de copia de seguridad. Para activar esta característica, consulte Especificación del origen.

Después de activar la característica, se podrán restaurar los elementos recuperables utilizando el asistente de la restauración.

Siga estos pasos:

1. En el cuadro de diálogo **Restaurar elemento de Exchange**, seleccione las carpetas necesarias bajo **Elementos recuperables** y haga clic en **Siguiente**.



Aparecerá el cuadro de diálogo Opción de restauración.

2. Desde la pantalla Opción de restauración, realice los siguientes detalles y haga clic en **Siguiente**:
   - Seleccione el destino de la restauración.
   - Omita o sobrescriba si el elemento ya existe en el destino.

     Se puede realizar la restauración original o alternativa.

     Restauración original

     Los elementos que se encuentran bajo Elementos recuperables se restauran en la carpeta *UDP_RecoverableItems_aaaaMMdd_HHmmssfff* creada en el buzón de correo de destino. Las opciones Omitir y Sobrescribir para la restauración no se aplican a estos elementos.

     Restauración alternativa

     De la misma manera que con el buzón del usuario, restaura los elementos seleccionados en la ruta de destino en una carpeta con la marca de tiempo única como, por ejemplo, *titulado/restore_aaaaMMdd-mmssff*.
   - Proporcione el ID de usuario y la contraseña del destino donde se desea restaurar.

   Se restauran los elementos recuperables seleccionados.

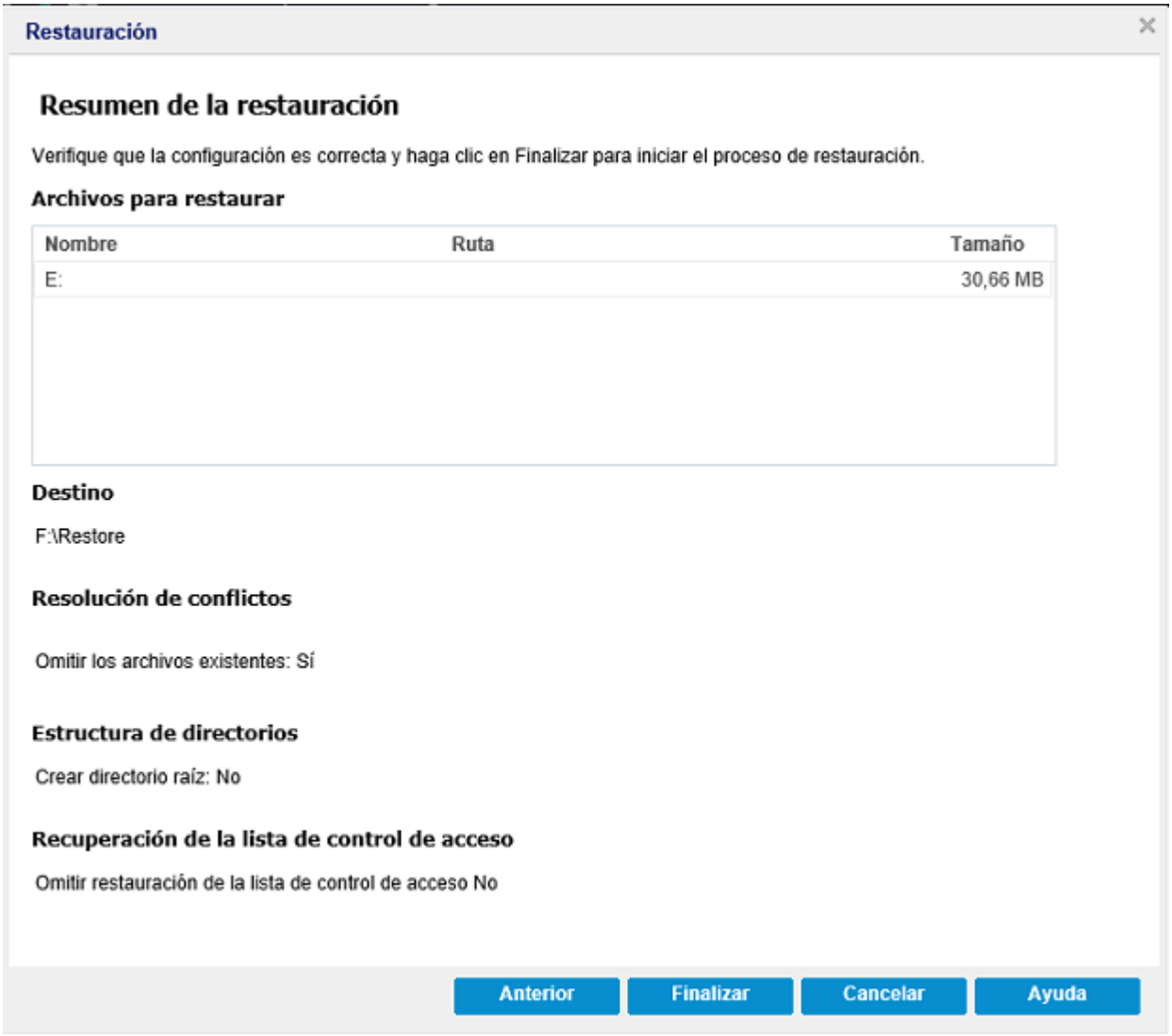
   El contenido del punto de recuperación se restaura.

Restauración del contenido del punto de recuperación

Después de definir las opciones de restauración, verifique que los valores de configuración sean correctos y confirme el proceso de restauración. El **Resumen de la restauración** le ayuda a revisar todas las opciones de la restauración definidas y a modificarlas si es necesario.

Siga estos pasos:

1. En el cuadro de diálogo **Resumen de la restauración**, revise la información que aparece en pantalla para verificar que todas las opciones de restauración y los valores de configuración sean correctos.



- Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo anterior correspondiente para cambiar la configuración incorrecta.

- Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar la tarea de restauración.

El contenido del punto de recuperación se restaura.

Verificación de que se ha restaurado el contenido

Después de la terminación del proceso de restauración, verifique que el contenido se ha restaurado en el destino especificado.

Siga estos pasos:

1. Inicie sesión en el buzón de correo de destino.
2. Compruebe que existe el elemento del buzón de correo que se ha restaurado.
3. Verifique el contenido restaurado.

   El contenido restaurado se ha verificado correctamente.

Cómo restaurar los datos de recopilación de sitios de SharePoint Online

Se puede restaurar la lista o la biblioteca de SharePoint Online, así como los elementos de lista en el sitio o el sitio principal de SharePoint. Se pueden restaurar los datos al sitio original con un nombre nuevo, restaurarlos a la ubicación original y exportarlos al disco desde los puntos de recuperación.

Realice las tareas siguientes para restaurar el elemento de lista de SharePoint Online:

1. Selección de los elementos de lista del sitio de SharePoint Online que se van a restaurar
2. Definición de las opciones de restauración
3. Verificación de que se ha restaurado el contenido

Selección de los elementos de lista del sitio de SharePoint Online que se van a restaurar

Se pueden restaurar los datos de los elementos de lista de SharePoint Online desde un punto de recuperación. Cuando se selecciona una fecha de recuperación y, a continuación, se especifica el tiempo, se muestran todos los puntos de recuperación asociados para esa duración. Tiene la opción de explorar y seleccionar el contenido de la copia de seguridad (incluyendo las aplicaciones) que se debe restaurar.

Siga estos pasos:

1. Iniciar sesión en Arcserve UDP.
2. Haga clic en la ficha **recursos**.
3. Seleccione **Todos los nodos** en el panel izquierdo.

   Se muestran todos los nodos de agregados en el panel central.

   O

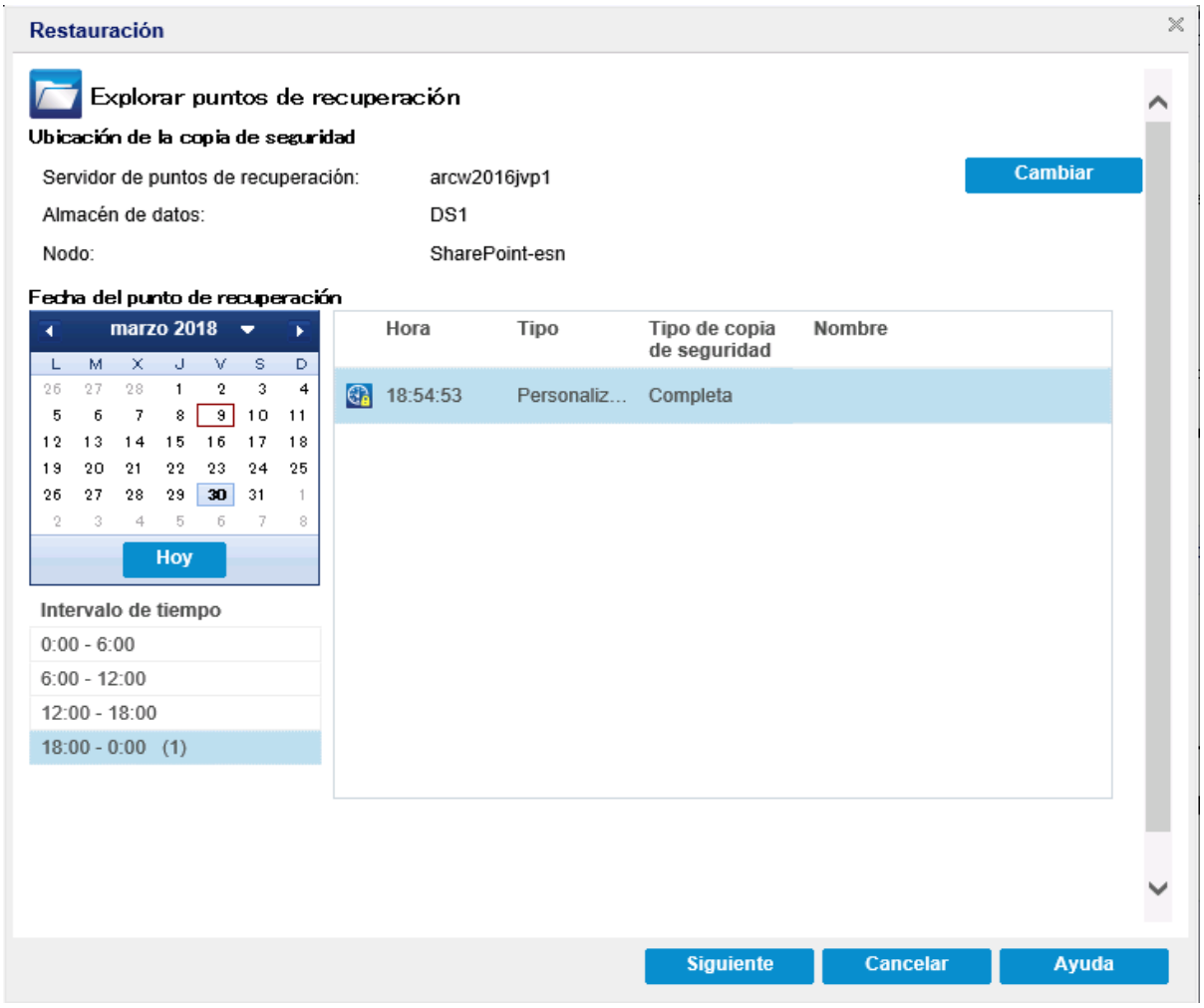
   Seleccione el grupo **Nodos de SharePoint Online**.

   Se muestran todos los nodos de SharePoint agregados en el panel central.
4. En el panel central, seleccione el nodo de SharePoint Online y haga clic en **Acciones**.
5. Haga clic en **Restaurar** del menú desplegable **Acción**.

   Se abre el cuadro de diálogo **Restaurar elemento de SharePoint**.

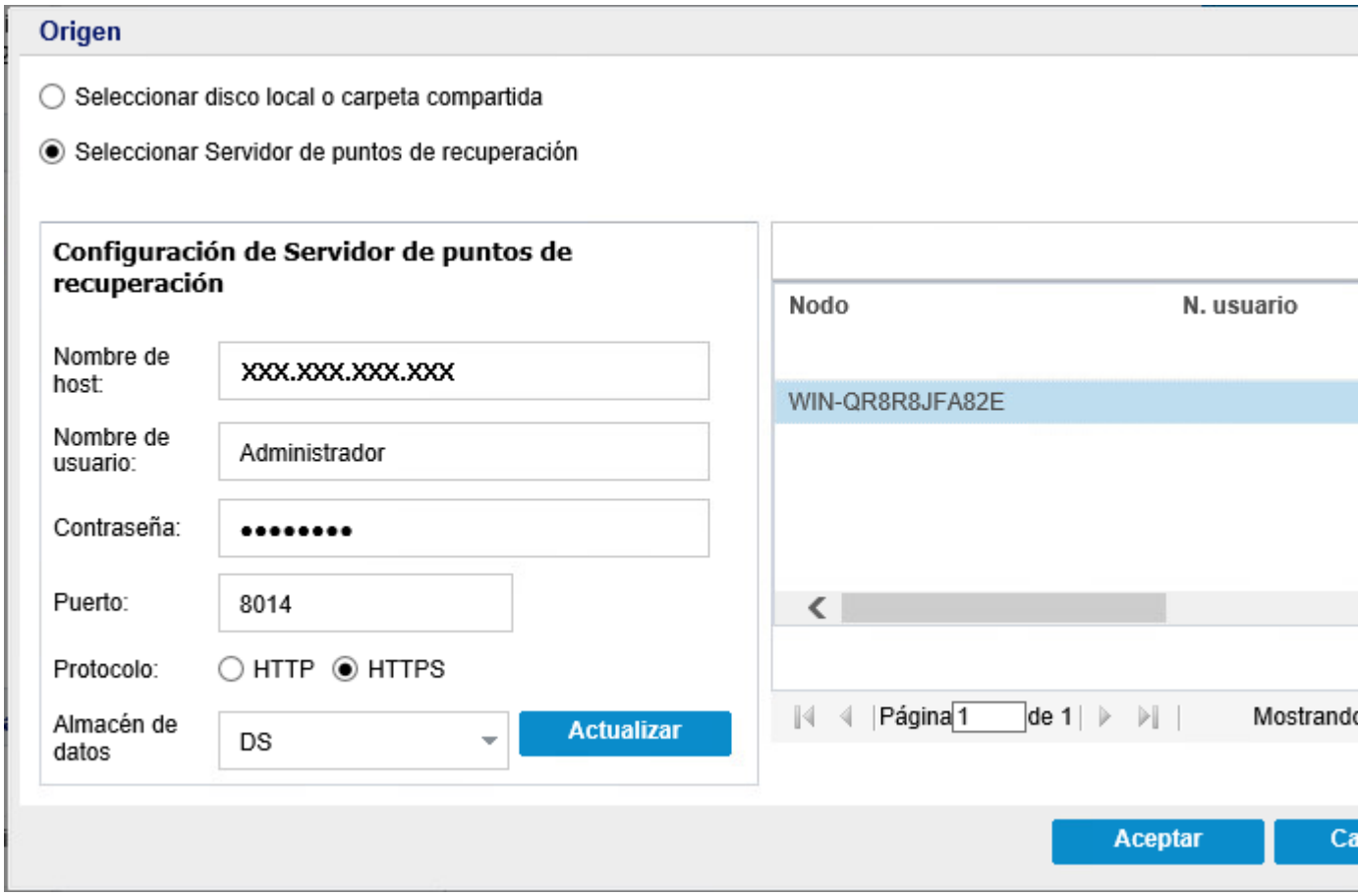
   Nota: Se inicia sesión automáticamente en el nodo del agente y se abre el cuadro de diálogo **Restaurar elemento de SharePoint**.

   La opción **Ubicación de la copia de seguridad** muestra los detalles del **Servidor de puntos de recuperación**.



6. (Opcional) Haga clic en **Cambiar** para modificar la ubicación de la copia de seguridad.

   Se abrirá el cuadro de diálogo **Origen.** Se puede seleccionar la ubicación de la copia de seguridad en este cuadro de diálogo.



Nota: Cuando se agrega una tarea de copia en cinta al plan y ahora se desea restaurar el punto de recuperación de la copia de seguridad de la copia en cinta, seleccione el punto de recuperación en la copia de seguridad de la copia en cinta. Para obtener más información, consulte Exploración del punto de recuperación de la copia en cinta para la restauración.

7. Para especificar el origen, seleccione una de las siguientes opciones y haga clic en **Aceptar**:

   Seleccionar disco local o carpeta compartida

   Nota: En Arcserve UDP, no se recomienda seleccionar la opción **Seleccionar disco local o carpeta compartida**.

   Seleccionar servidor de puntos de recuperación

   a. Especifique los detalles del valor de configuración del Servidor de puntos de recuperación y haga clic en **Actualizar**.

      Todos los agentes se muestran en la columna Agente de protección de datos en el cuadro de diálogo **Origen**.

   b. Seleccione el agente en la lista o biblioteca mostrada y haga clic en **Aceptar**.

Los puntos de recuperación se enumeran en el cuadro de diálogo **Restaurar elemento de SharePoint**.

8. Seleccione la fecha de calendario para restaurar la imagen de la copia de seguridad y haga clic en **Siguiente**.

   Todas las fechas que contienen puntos de recuperación para el origen de la copia de seguridad especificado se resaltan en verde.

   Aparecerán los puntos de recuperación correspondientes para la fecha, junto con la hora de la copia de seguridad, el tipo de copia de seguridad que se realiza (completa o incremental) y el nombre de la copia de seguridad.

9. En el cuadro de diálogo **Restaurar los elementos de SharePoint Online**, expanda la recopilación de sitios.

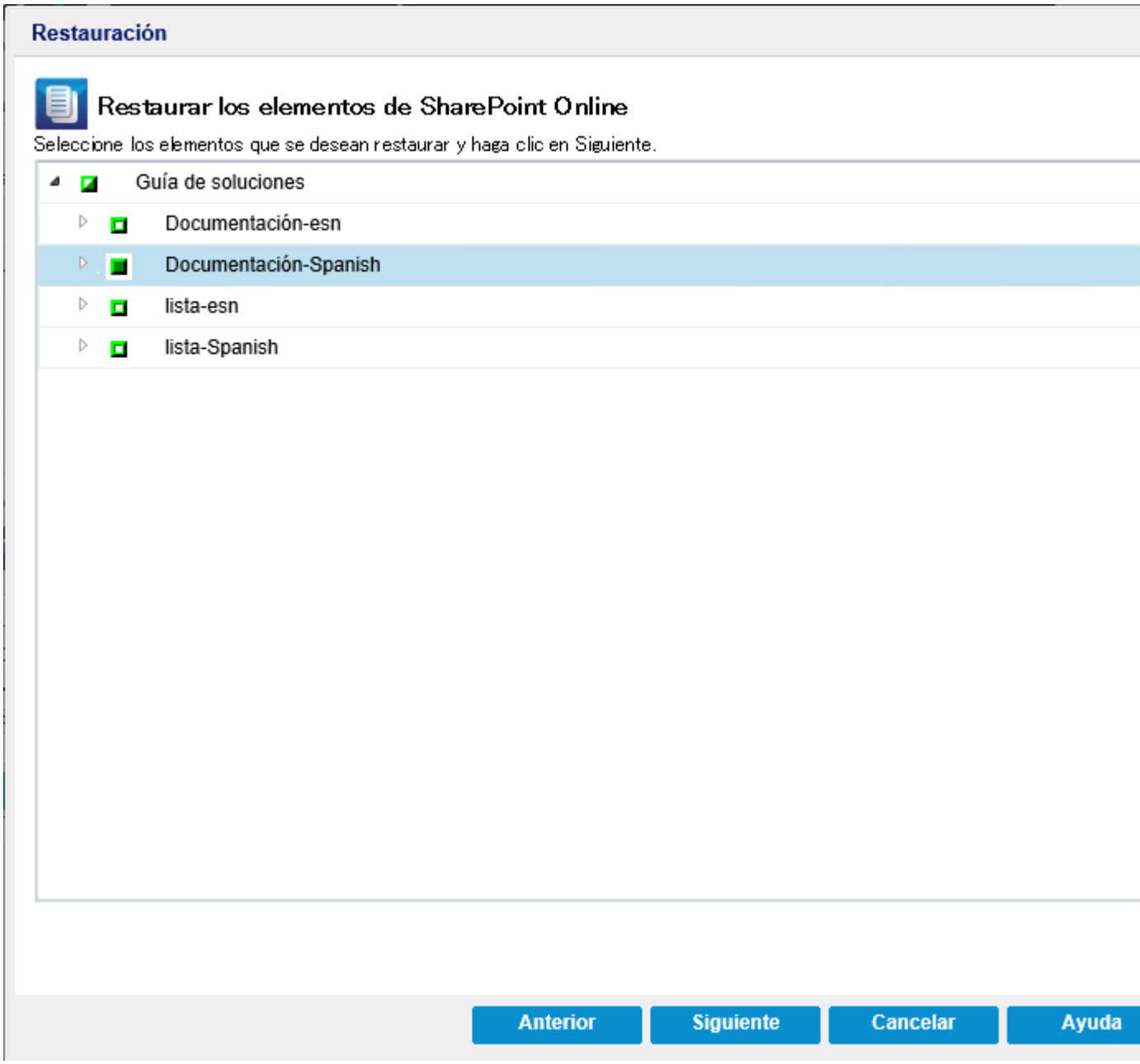
   Se muestran todas las listas o bibliotecas, así como los elementos de lista.

10. Seleccione la lista, la biblioteca o el elemento de lista disponible en la recopilación de sitios que desea restaurar desde la recopilación de sitios de SharePoint y haga clic en **Siguiente**.

    Notas:

    - Se puede seleccionar todo el contenido o el contenido parcial del objeto de SharePoint que se va a restaurar. Para seleccionar parte del contenido, expanda el objeto y haga clic en la casilla de verificación de dicho contenido.
    - Puede seleccionar varias listas o bibliotecas de SharePoint, o los elementos de lista que desea restaurar.

    Se abrirá el cuadro de diálogo **Opciones de restauración**.



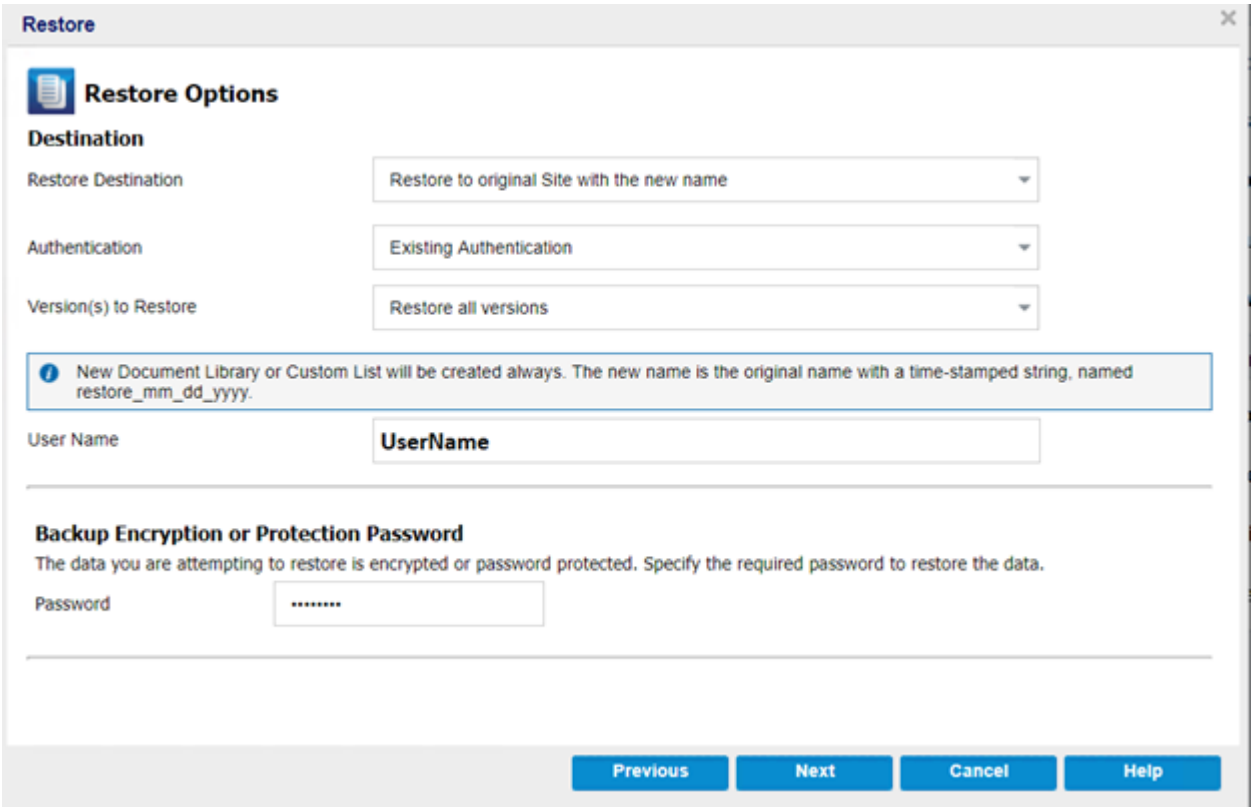
Las listas o bibliotecas de SharePoint Online, así como los elementos de lista que se van a restaurar, están seleccionados. Ahora, se pueden definir las opciones de restauración.

Definición de las opciones de restauración

Después de especificar la información de SharePoint Online que se debe restaurar, defina las opciones de restauración para el contenido seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, seleccione el destino para la restauración.



A continuación se especifican las opciones de destino disponibles:

Restaurar al sitio original con el nombre nuevo

Restaura los datos de la lista o de la biblioteca, así como de los elementos de lista, en el mismo sitio con un nuevo nombre de lista desde donde se ha realizado una copia de seguridad.

Restaurar en la ubicación original

Restaura los datos de la lista o de la biblioteca, así como de los elementos de lista, en la misma ubicación desde donde se ha realizado una copia de seguridad.

2. Especifique una de las siguientes opciones del menú desplegable **Si el elemento ya existe en la lista desplegable Destino**:

Añadir como nueva versión si está activado el control de versiones

Esta opción funciona cuando está activada la configuración de la versión en la configuración de la biblioteca en el sitio de SharePoint. Una vez que se selecciona esta opción, la nueva versión se agrega a las versiones actuales de los elementos de lista si existen elementos de lista.

Omitir el elemento y no restaurar

Se omiten los elementos y no se restaurará.

Sobrescribir el elemento en el destino

Sobrescribe el elemento en el destino.

Exportar a disco

Restaura las listas y las bibliotecas, así como los elementos de lista de la recopilación de sitios, a la carpeta o a la carpeta del recurso compartido del disco.

Nota: Para la restauración de las listas cuando se selecciona la opción de restauración de la opción Exportar a disco, solo se exportan los datos adjuntos de la lista al disco.

Autentificación

Valida e identifica la cuenta de usuario. Seleccione una de las opciones siguientes:

- **Autenticación existente**

  Cuando se selecciona Autenticación existente, se utiliza el tipo de autenticación que se ha seleccionado durante la creación del nodo.

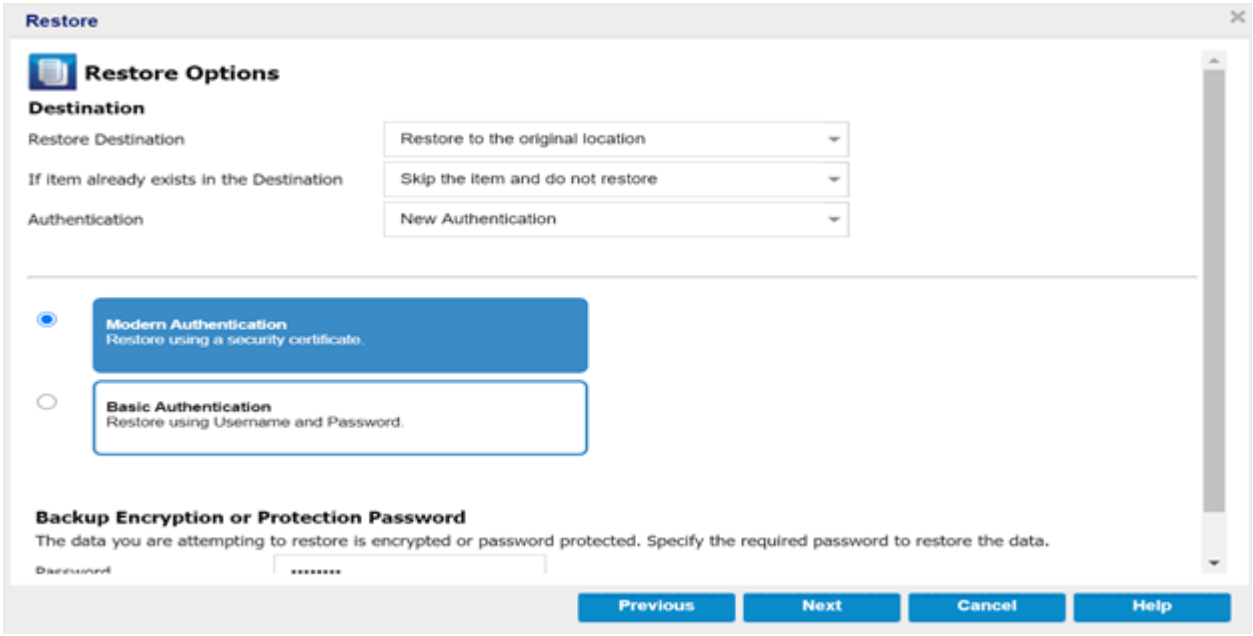
  - Si la autenticación del nodo es básica, se cargan automáticamente parámetros como Nombre de usuario, Contraseña y Cifrado de la copia de seguridad o Contraseña de protección [Si está cifrada] para continuar con la restauración.
  - Si la autenticación del nodo es moderna, se cargan automáticamente parámetros como Nombre de usuario y Cifrado de la copia de seguridad o Contraseña de protección [Si está cifrada] para continuar con la restauración.

- **Nueva autenticación**

  Durante la restauración, se puede seleccionar una de las siguientes opciones para cambiar el tipo de autenticación:

  - Autenticación moderna

- Autenticación básica



3. Para aplicar la autenticación, realice una de las siguientes acciones:

Autenticación moderna

Para la autenticación moderna, se puede ejecutar una restauración utilizando un certificado de seguridad.

Utilizar certificado de seguridad

Nota: De forma predeterminada, el plan de copia de seguridad selecciona **Utilizar certificado de seguridad** para la autenticación moderna.

Siga estos pasos:

a. Para autenticarse mediante un certificado autofirmado, consulte Descarga del certificado desde UDP y carga del certificado en Azure.

b. Introduzca el ID de la aplicación y el Nombre de usuario.

c. Para aplicar los roles y permisos necesarios, seleccione la casilla de verificación **Permitir a Arcserve UDP establecer los roles y permisos de Azure necesarios para esta aplicación** y, a continuación, haga clic en **Siguiente**.

Autenticación básica

Para la Autenticación básica, introduzca el nombre de usuario y la contraseña para continuar con la restauración.

Nota: Esta opción produce un error si tiene activada la autenticación moderna en el inquilino o en la cuenta.

4. Especifique las versiones del elemento de lista que se van a restaurar cuando se active la configuración de la versión desde la configuración de la biblioteca en el sitio de SharePoint.

   Restaurar todas las versiones

   Restaura todas las versiones durante la copia de seguridad.

   Restaurar solo la versión más reciente

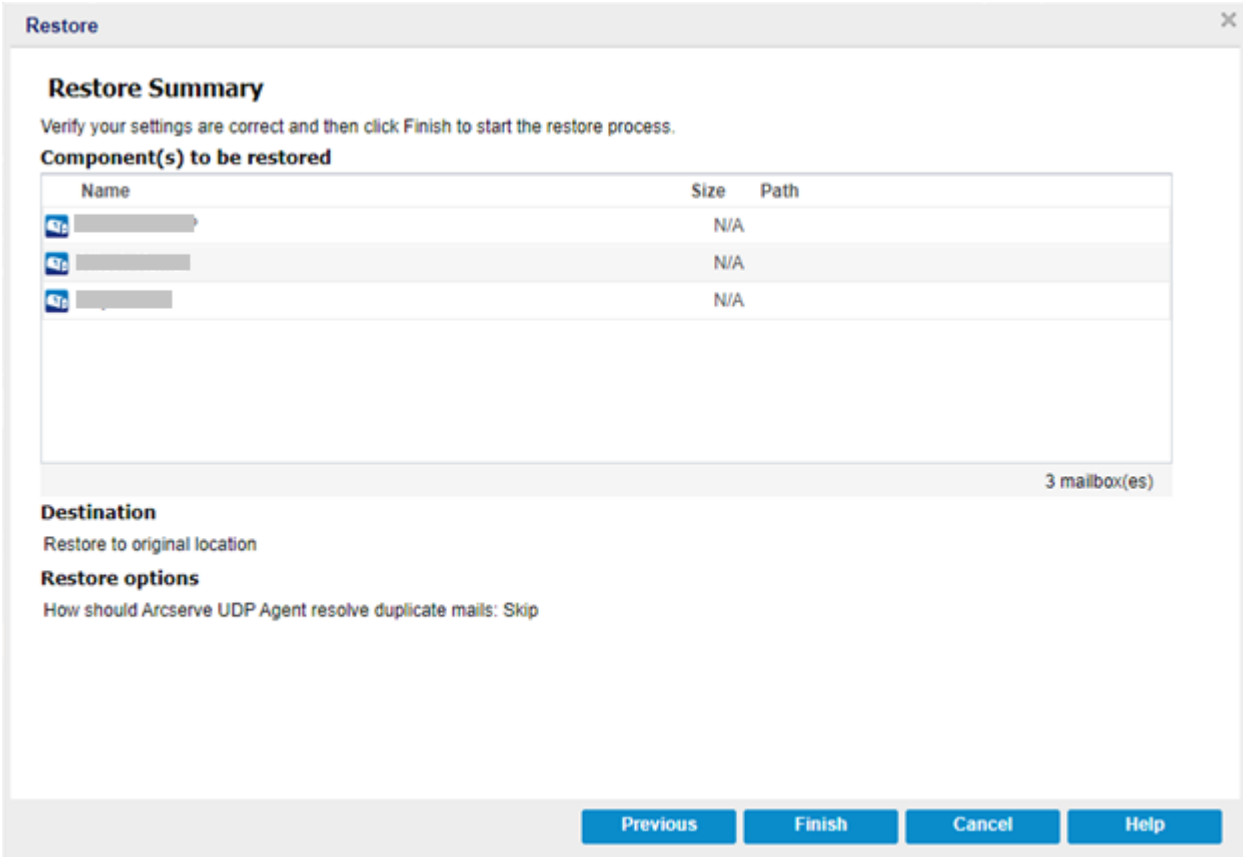
   Restaura solo la versión más reciente durante la copia de seguridad.

   Restaurar solo la última versión principal

   Restaura solo la última versión principal durante la copia de seguridad.

5. Especifique la contraseña de la sesión si la tiene.
6. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Resumen de la restauración**.



   Se puede verificar la información sobre la restauración en el cuadro de diálogo Resumen de la restauración.

7. Haga clic en **Finalizar** para enviar la tarea de restauración.

   Las opciones de restauración se han definido para restaurar la información de SharePoint Online.

Verificación de que se ha restaurado el contenido

Después de la terminación del proceso de restauración, verifique que el contenido se ha restaurado en el destino especificado.

Siga estos pasos:

1. Inicie sesión en la Colección de sitios de SharePoint.
2. Verifique la lista y la biblioteca, así como los elementos de lista.
3. Verifique el contenido restaurado.

   El contenido restaurado se ha verificado correctamente.

Cómo restaurar los datos de OneDrive

Puede restaurar los datos de OneDrive (archivos, carpetas, etc.) utilizando cualquier equipo. Puede restaurar los datos con la opción de restauración o utilizando la opción de montaje de volúmenes de la interfaz de usuario del agente.

Realice las tareas siguientes para restaurar los datos de OneDrive con la opción de restauración:

1. Selección de elementos de OneDrive para restaurarlos
2. Definición de las opciones de restauración
3. Visualización del resumen de la restauración

O, de lo contrario,

Restauración de datos de OneDrive utilizando la opción de montaje de volúmenes

Selección de elementos de OneDrive para restaurarlos

Se pueden restaurar datos de OneDrive desde un punto de recuperación. Cuando se selecciona una fecha de recuperación y, a continuación, se especifica el tiempo, se muestran todos los puntos de recuperación asociados para esa duración. Tiene la opción de explorar y seleccionar el contenido de la copia de seguridad (incluyendo las aplicaciones) que se debe restaurar.

Siga estos pasos:

1. Iniciar sesión en Arcserve UDP.
2. Haga clic en la ficha **recursos**.
3. Seleccione **Todos los nodos** en el panel izquierdo.

   Se muestran todos los nodos de agregados en el panel central.
4. En el panel central, seleccione el nodo de OneDrive y haga clic en **Acciones**.
5. Haga clic en **Restaurar** del menú desplegable **Acción**.

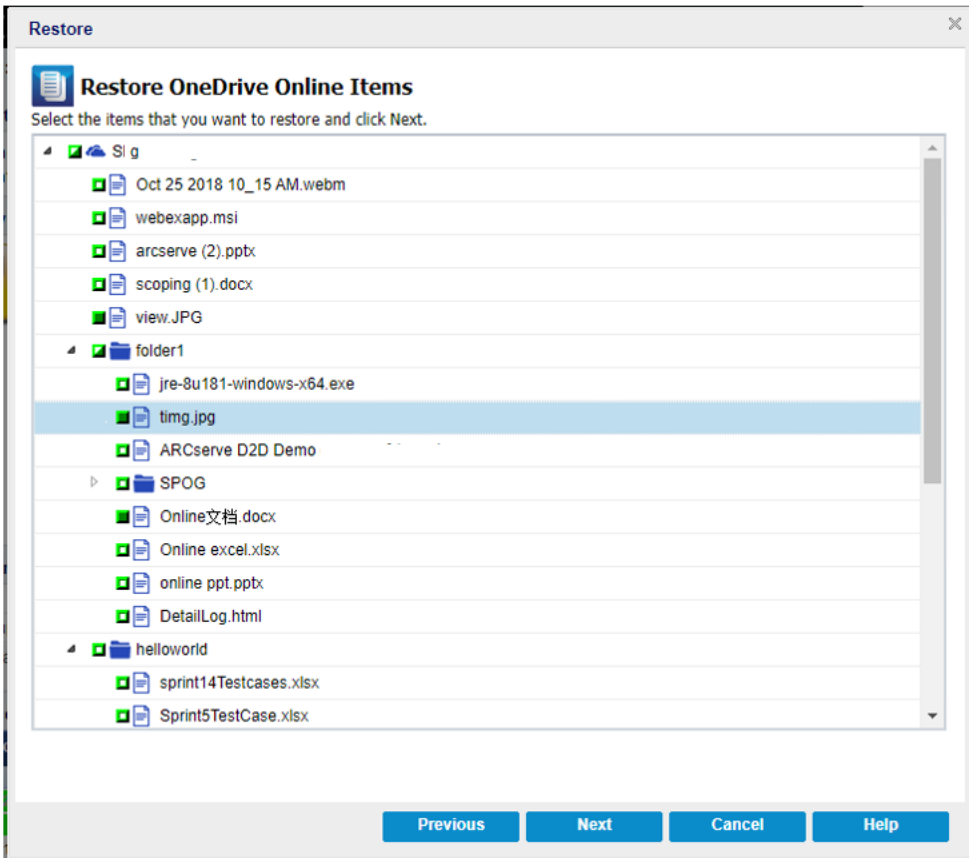
   Nota: Se inicia sesión automáticamente en el nodo del agente y se abre el cuadro de diálogo **Nodo**.

   Se pueden ver los detalles de **Explorar puntos de recuperación** en la ubicación de la copia de seguridad. Se muestra el nombre del *Servidor de puntos de recuperación* seleccionado. Si lo desea, haga clic en **Cambiar** y modifique **los valores de configuración del servidor de puntos de recuperación** en el menú emergente **Origen**.

   Nota: Cuando se agrega una tarea de copia en cinta al plan y ahora se desea restaurar el punto de recuperación de la copia de seguridad de la copia en cinta, seleccione el punto de recuperación en la copia de seguridad de la copia en cinta. Para obtener más información, consulte Exploración del punto de recuperación de la copia en cinta para la restauración.
6. Seleccione la fecha de calendario para restaurar la imagen de la copia de seguridad y haga clic en **Siguiente**.

   Todas las fechas que contienen puntos de recuperación para el origen de la copia de seguridad especificado se resaltan en verde.

   Aparecerán los puntos de recuperación correspondientes para la fecha, junto con la hora de la copia de seguridad, el tipo de copia de seguridad que se realiza (completa o incremental) y el nombre de la copia de seguridad.
7. En el panel **Restauración de los elementos del nodo de OneDrive**, seleccione las casillas de verificación de los elementos o carpetas relacionados que desea restaurar de las carpetas y haga clic en **Siguiente**.



Notas:

- Se puede seleccionar todo el contenido o el contenido parcial del objeto de OneDrive que se va a restaurar. Para seleccionar parte del contenido, expanda el objeto y haga clic en la casilla de verificación de dicho contenido.
- Se pueden seleccionar varios objetos de OneDrive para restaurar.

Se abrirá el cuadro de diálogo **Opciones de restauración**.

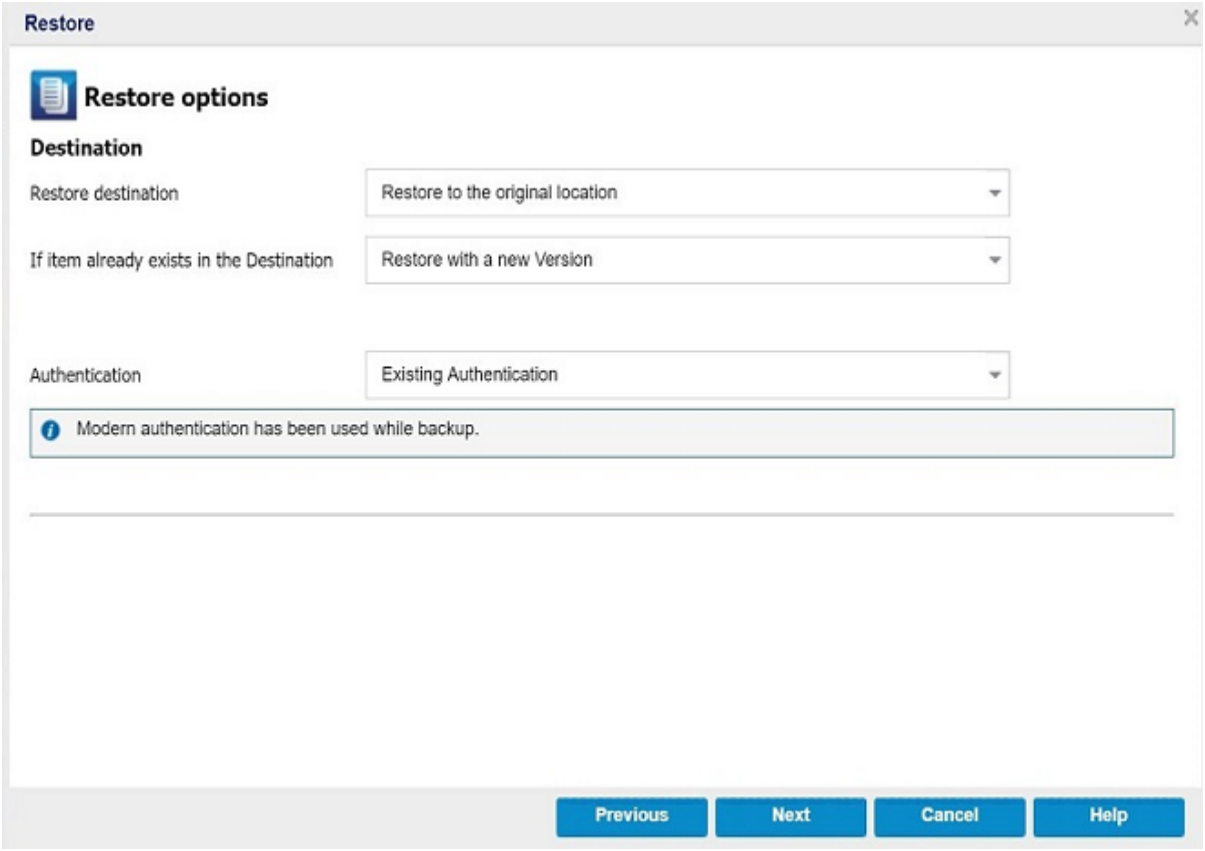
Se seleccionarán los elementos del nodo de OneDrive que se van a restaurar. Ahora, se pueden definir las opciones de restauración.

Definición de las opciones de restauración

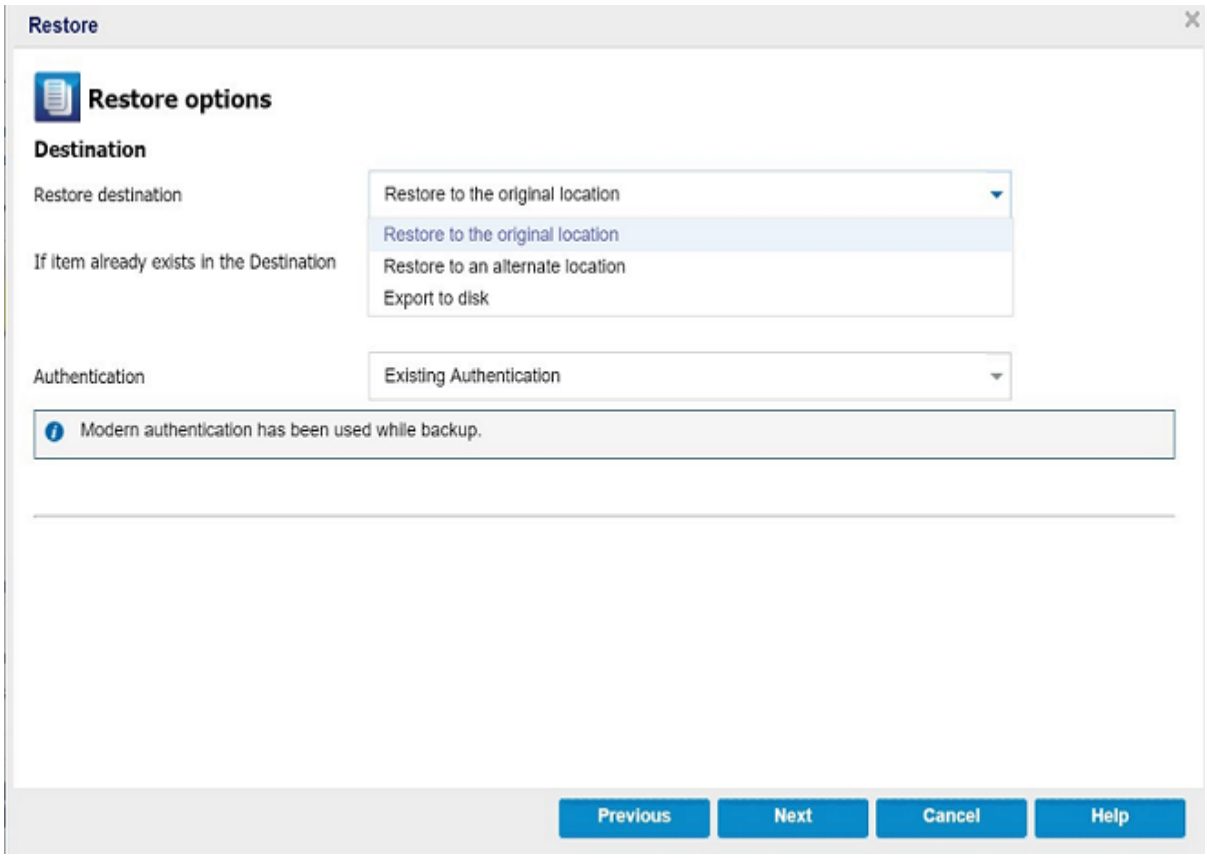
Después de especificar la información de OneDrive que se debe restaurar, defina las opciones de restauración para el contenido seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, seleccione el destino para la restauración.



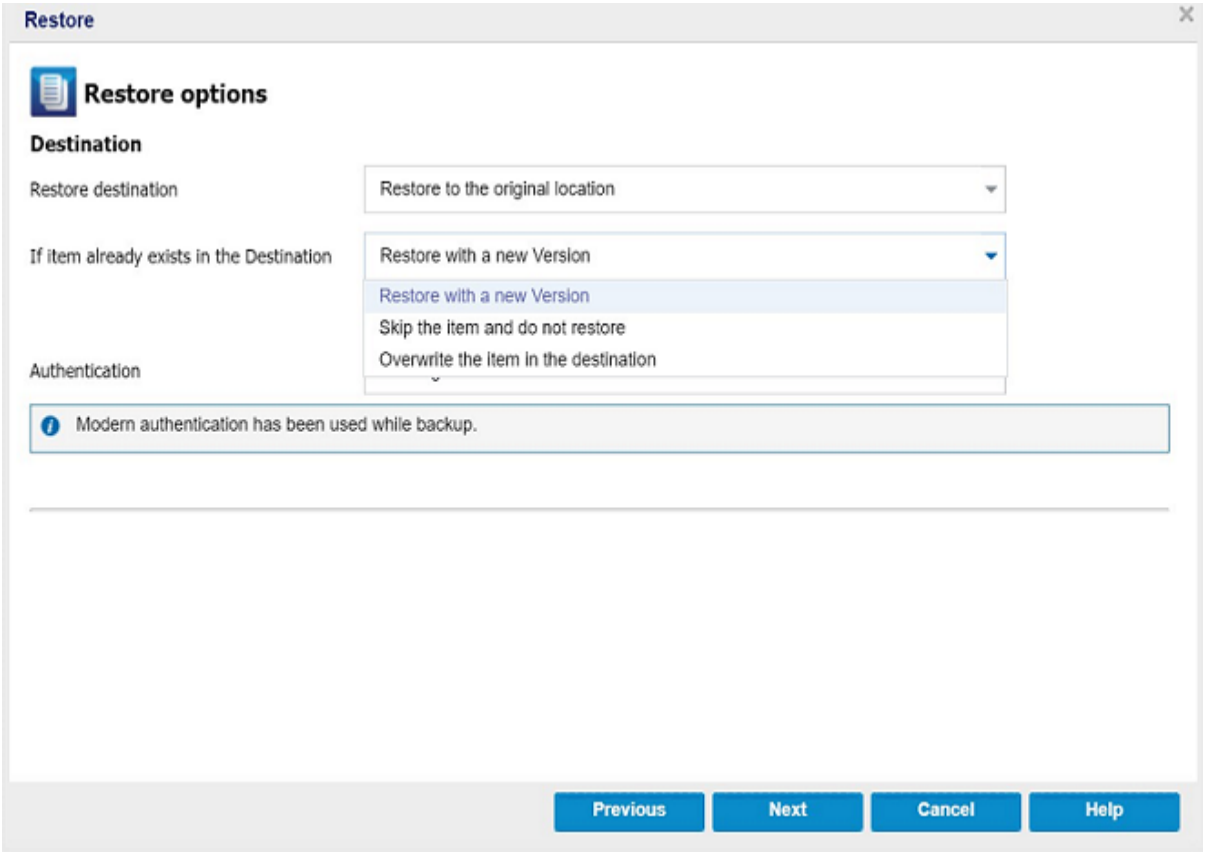
A continuación se especifican las opciones de destino disponibles:



Restaurar en la ubicación original

Restaura los archivos o carpetas del correo en la misma ubicación desde donde se ha realizado una copia de seguridad.

Si selecciona la opción **Restaurar en la ubicación original**, en la lista desplegable **Si el elemento ya existe en el destino**, seleccione una de las siguientes opciones:



Restaurar con una nueva versión

Agrega una nueva versión a los archivos existentes.

Esta opción está seleccionada de forma predeterminada.

Omitir el elemento y no restaurar

Se omiten los elementos y no se restaurará.

Sobrescribir el elemento en el destino

Sobrescribe el elemento en el destino.

Restaurar en una ubicación alternativa

Restaura los archivos, las carpetas o las cuentas en una cuenta de la ubicación alternativa. Cuando se selecciona esta opción, se puede examinar y seleccionar el destino.

Jerarquía del origen

Conserva el árbol de jerarquía tal y como se especifica en el origen al crear planes de copia de seguridad.

Nota: Esta opción solo se muestra cuando se selecciona Restaurar en una ubicación alternativa.

Exportar a disco

Restaura en una carpeta o en una carpeta del recurso compartido que se encuentra en el disco.

2. Para validar e identificar la cuenta de usuario, en el menú desplegable **Autenticación**, seleccione una de las siguientes opciones:

Autenticación existente

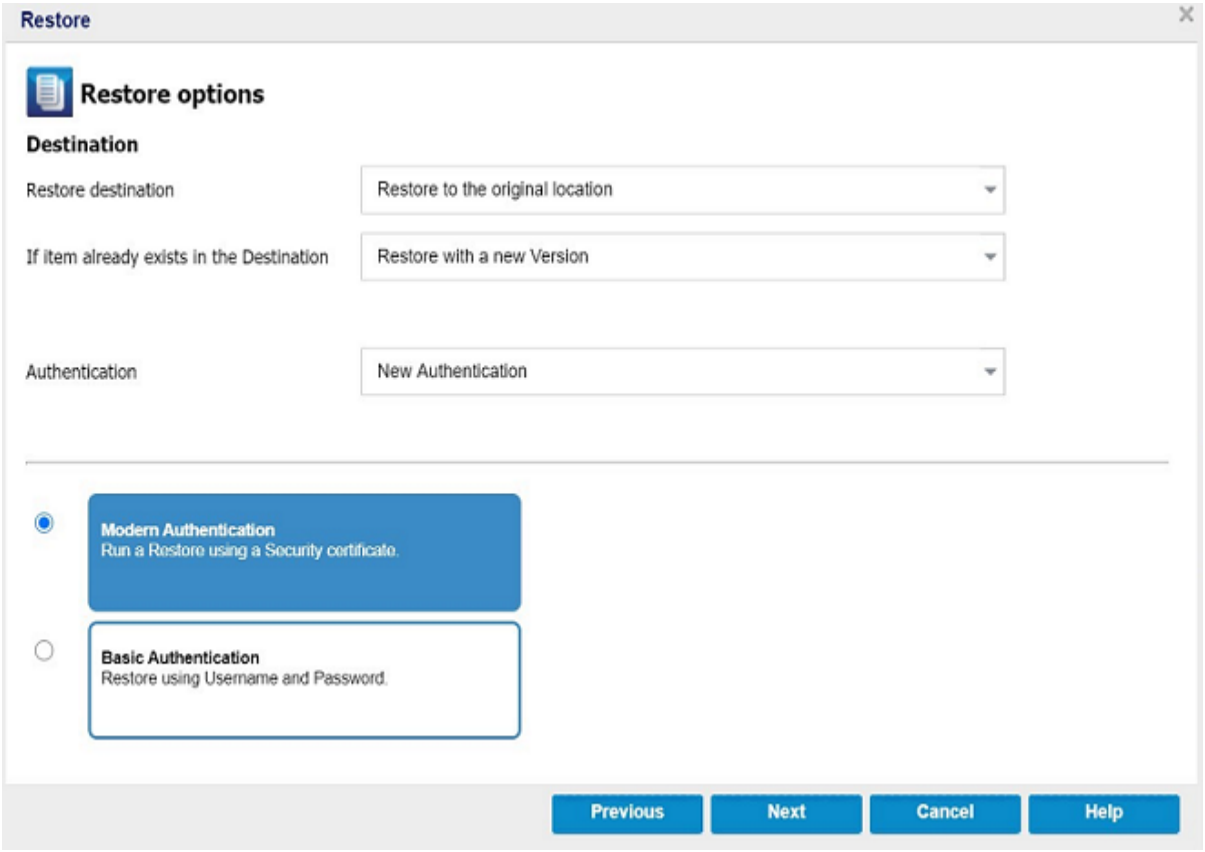
Cuando se selecciona Autenticación existente, se utiliza el tipo de autenticación que se ha seleccionado durante la creación del nodo.

- Si la autenticación del nodo es básica, se cargan automáticamente parámetros como Nombre de usuario, Contraseña y Cifrado de la copia de seguridad o Contraseña de protección [Si está cifrada] para continuar con la restauración.
- Si la autenticación del nodo es moderna, se cargan automáticamente parámetros como Nombre de usuario y Cifrado de la copia de seguridad o Contraseña de protección [Si está cifrada] para continuar con la restauración.

Nueva autenticación

Durante la restauración, se puede seleccionar una de las siguientes opciones para cambiar el tipo de autenticación:

- Autenticación moderna
- Autenticación básica



3. Para aplicar la nueva autenticación, realice una de las siguientes acciones:

Autenticación moderna

Para la autenticación moderna, se puede ejecutar una restauración utilizando un certificado de seguridad.

Siga estos pasos:

a. Para autenticarse mediante el certificado autofirmado, consulte Descarga del certificado desde UDP y carga del certificado en Azure.

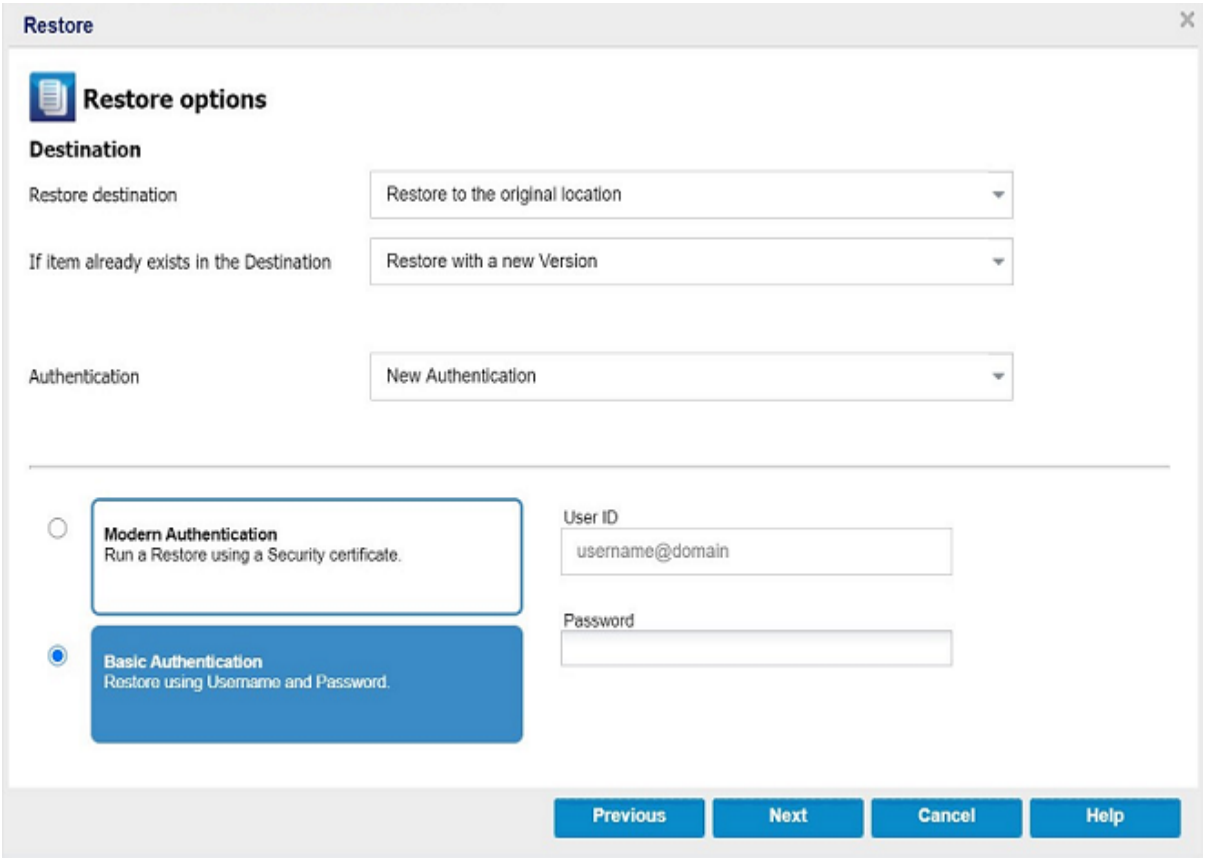
b. Introduzca el ID de la aplicación y el Nombre de usuario.

c. Para aplicar los roles y permisos necesarios, seleccione la casilla de verificación **Permitir a Arcserve UDP establecer los roles y permisos de Azure necesarios para esta aplicación** y, a continuación, haga clic en **Siguiente**.

Autenticación básica

Para la Autenticación básica, introduzca el ID de usuario y la contraseña para con-

tinuar con la restauración.



4. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Resumen de la restauración**.

5. En el cuadro de diálogo Resumen de la restauración, verifique la configuración y, a continuación, haga clic en **Finalizar**.

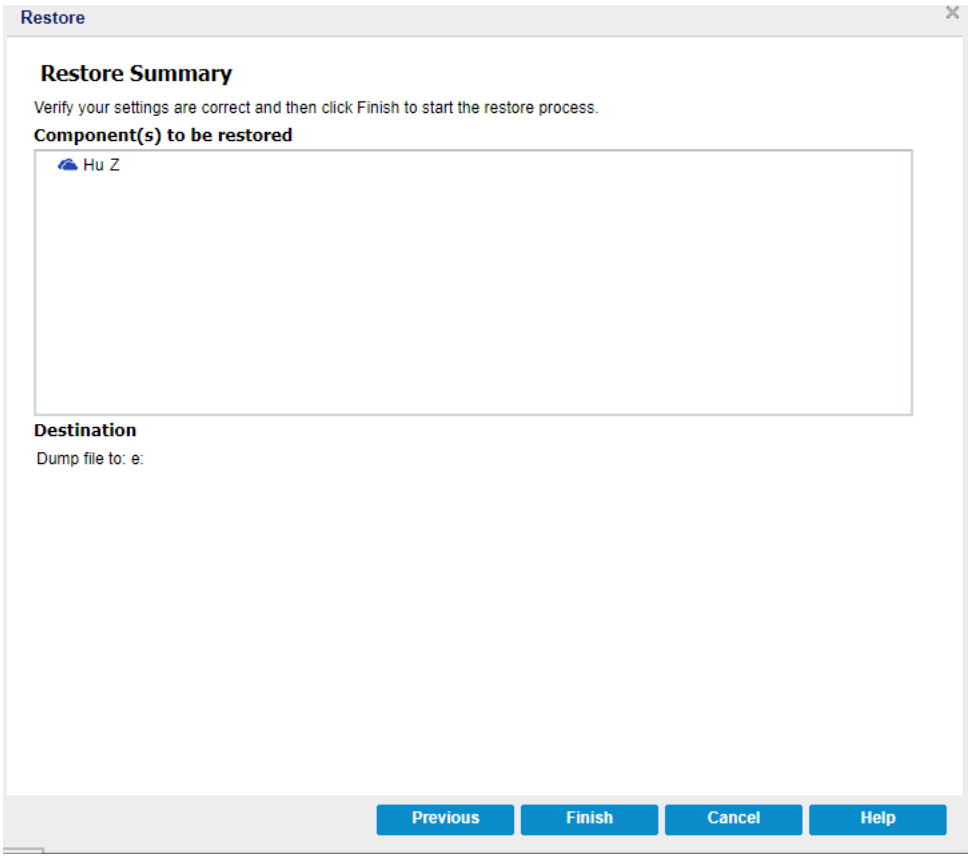
   Las opciones de restauración se han definido para restaurar la información de OneDrive. Ahora se puede ver el resumen de la restauración.

Visualización del resumen de la restauración

Después de definir las opciones de restauración, verifique que los valores de configuración sean correctos y confirme el proceso de restauración. **Resumen de la restauración** le ayuda a revisar todas la opciones de la restauración y la ruta de destino que se han definido. Si necesita realizar alguna modificación, haga clic en **Anterior**.

Siga estos pasos:

1. En el cuadro de diálogo **Resumen de la restauración**, revise la información que aparece en pantalla para verificar que todas las opciones de restauración y los valores de configuración sean correctos.



   - Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para modificar los valores de configuración.
   - Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar la tarea de restauración.

El contenido del punto de recuperación se restaura.

Restauración de datos de OneDrive utilizando la opción de montaje de volúmenes

OneDrive Protection utiliza el formato universal de la sesión de la copia de seguridad. Se puede montar la sesión de la copia de seguridad como una letra de unidad y, a continuación, copiar el archivo o carpeta desde el volumen montado.

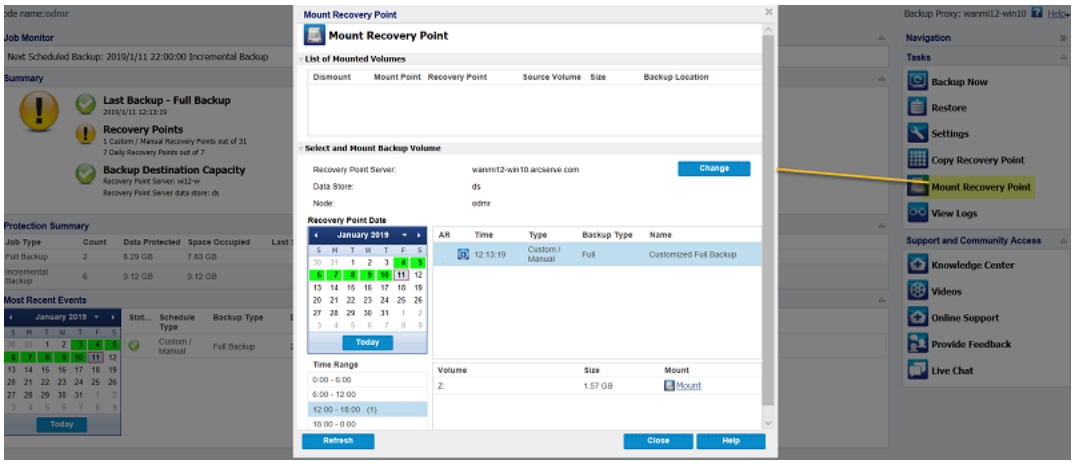
Siga estos pasos:

1. Inicie sesión en Arcserve UDP.
2. Haga clic en la ficha **recursos**.
3. Seleccione **Todos los nodos** en el panel izquierdo.

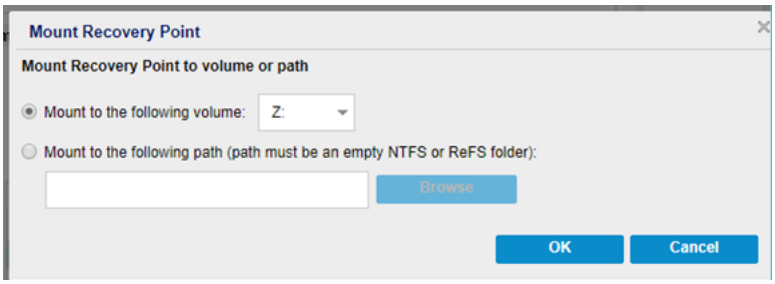
   Se muestran todos los nodos de agregados en el panel central.
4. En el panel central, seleccione el nodo de OneDrive y haga clic en **Acciones**.
5. Haga clic en **Iniciar sesión en el Agente** en el menú desplegable **Acciones**.

   Nota: Se inicia sesión automáticamente en el nodo del agente. Se pueden ver todos los detalles del nodo, incluso en el panel derecho también se puede ver la lista de tareas que se pueden realizar.
6. En el panel derecho que se encuentra bajo **Tareas**, haga clic en **Montar punto de recuperación**.

   Aparecerá el cuadro de diálogo **Montar punto de recuperación.** Se puede seleccionar la sesión de la copia de seguridad en este cuadro de diálogo.



7. Seleccione el destino y monte la sesión como una letra de unidad o móntela en una carpeta NTFS vacía.



Se puede explorar el volumen. En el volumen, Arcserve UDP ha guardado todos los metadatos de OneDrive. Cada cuenta tendrá una carpeta relacionada en el volumen raíz. La carpeta se llama según el nombre de cuenta.

Se puede abrir la carpeta creada por dicho nombre de cuenta y verificar si se ha realizado la copia de seguridad de los datos de OneDrive.

Exploración del punto de recuperación de copia en cinta para la restauración

Esta sección proporciona información sobre cómo seleccionar un punto de recuperación de las copias de seguridad de copia en cinta.

Siga estos pasos:

1. Descargue los puntos de recuperación utilizando el Gestor de Arcserve Backup y, a continuación, cópielos en un disco local.
2. En el cuadro de diálogo Restaurar, haga clic en el botón **Cambiar**.
3. Seleccione la opción **Seleccionar disco local o carpeta compartida**.
4. Haga clic en **Examinar** para ir a la ubicación de la carpeta donde se copian los puntos de recuperación en el paso 1.
5. En la lista de puntos de recuperación, seleccione un punto de recuperación y haga clic en **Aceptar**.

   El punto de recuperación seleccionado aparece en el cuadro de diálogo Restaurar.

Cómo realizar la restauración a un momento determinado

La restauración a un momento determinado admite la restauración de la base de datos SQL en un período de tiempo específico entre los puntos de recuperación N y N+1. La restauración a un momento determinado ayuda a los administradores a restaurar las transacciones que se han producido en la base de datos SQL entre dos puntos de recuperación. Por ejemplo, considere que dispone de un punto de

recuperación el 16/03/2019 a las 12:14:04:177 y un punto de recuperación posterior el 29/03/2019 a las 22:03:14:177. Con la restauración a un momento determinado, se pueden restaurar las transacciones que se han producido entre los dos puntos de recuperación. Esto ayuda a los administradores a restaurar solamente las transacciones necesarias de un gran tamaño de datos de la copia de seguridad.

¿Qué hacer a continuación?

1. Revisión de los requisitos previos
2. Revisión de las consideraciones
3. Realización de la restauración a un momento determinado

Requisitos previos

Revise los siguientes requisitos previos antes de realizar la restauración a un momento determinado:

- La base de datos de MS SQL Server debe estar instalada en el equipo del Agente de Windows.
- Deben existir al menos dos puntos de recuperación para realizar la restauración a un momento determinado.
- Se debe activar manualmente la restauración a un momento determinado cada vez que se realiza la restauración.

Consideraciones

Revise las consideraciones siguientes antes de realizar la restauración a un momento determinado:

- Solo se puede realizar la restauración a un momento determinado utilizando la utilidad de la línea de comandos PIT.EXE.
- Deben existir dos puntos de recuperación trabajando juntos para realizar la restauración a un momento determinado.
- La restauración a un momento determinado solo admite la copia de seguridad basada en el agente. No se admite la copia de seguridad basada en el host.
- La restauración a un momento determinado solo es compatible con la restauración a la ubicación original. No se admite la restauración a una ubicación alternativa, así como tampoco se admite el vaciado en disco.

- La copia de seguridad del registro de transacciones de la base de datos de SQL se guarda en el mismo directorio del archivo de registro de SQL antes de tomar la instantánea.
- El primer punto de recuperación proporciona la restauración a nivel de la base de datos de SQL. Después de la restauración a un momento determinado, la base de datos de SQL se establece en el estado de recuperación. Se puede realizar la copia de seguridad del punto de recuperación en el modo desactivado de la restauración a un momento determinado.
- Para realizar la restauración a un momento determinado, se debe seleccionar el punto de tiempo entre los puntos de recuperación N y N+1. No se permite cualquier punto de tiempo anterior al punto de recuperación N y posterior al punto de recuperación N+1. Si se establece el punto de tiempo en un punto de recuperación que no está entre el punto de recuperación N y el N+1, se produce un error en la tarea de restauración y se daña la base de datos.
- La opción para truncar el registro está desactivada de forma predeterminada en los planes de restauración y copia de seguridad a un momento determinado. Si se activa después de que se trunquen los registros de transacciones de la copia de seguridad y a la siguiente copia de seguridad a un momento determinado le faltan algunas transacciones.

Realización de la restauración a un momento determinado

1. Ejecute el archivo **PIT. EXE**.

   La utilidad de la línea de comandos de la restauración a un momento determinado se abre y muestra el símbolo del sistema PIT$.

   Para obtener más información, consulte Funcionamiento de la utilidad de la línea de comandos de la restauración a un momento determinado.

2. En la línea de comandos, ejecute **set pitbackup=1**.

   Se activa la copia de seguridad a un momento determinado.

3. En la Consola de **Arcserve UDP**, realice una copia de seguridad de la base de datos de SQL.

   Se crea el punto de recuperación N.

4. Verifique que se hayan generado los archivos siguientes en la carpeta **Catalog**:

- Si el nombre de instancia de SQL Server es MSSQLSERVER (nombre de instancia predeterminado):
  - ***_<NombreBaseDatos>.idx.pit***

    Contiene el tamaño fijo del resumen del punto de tiempo.
  - ***_<NombreBaseDatos>.cat.pit***

    Contiene el tamaño variable de los detalles del punto de tiempo.
  - ***_<NombreBaseDatos>.map.pit***

    Contiene la asignación entre la cadena interna y la identidad de la cadena interna.
- Si el nombre de instancia de SQL Server no es MSSQLSERVER (no es el nombre de instancia predeterminado):
  - ***<NombreInstanciaSQL>_<NombreBaseDatos>.idx.pit***

    Contiene el tamaño fijo del resumen del punto de tiempo.
  - ***<NombreInstanciaSQL>_<NombreBaseDatos>.cat.pit***

    Contiene el tamaño variable de los detalles del punto de tiempo.
  - ***<NombreInstanciaSQL>_<NombreBaseDatos>.map.pit***

    Contiene la asignación entre la cadena interna y la identidad de la cadena interna.

5. En la Consola de **Arcserve UDP**, realice otra copia de seguridad de la base de datos de SQL.

   Se crea el punto de recuperación N+1.
6. En la línea de comandos, ejecute ***set pitrestore=1***.

   Se activa la restauración a un momento determinado.
7. En la línea de comandos, ejecute las siguientes consultas de SQL para ver la información del punto de tiempo de la sesión de copia de seguridad de N+1:
   - *Query <NombreInstanciaSQL>\<NombreBaseDatos> <DestinoCopiaSeguridad>\Catalog\<Nombre carpeta de la sesión de copia de seguridad de N+1>*

     Muestra el resumen de todos los puntos de tiempo en la copia de seguridad.
8. En la línea de comandos, ejecute ***set pittime="<MM/DD/AAAA HH:MM:SS:ss>"***

9. En la Consola de **Arcserve UDP**, realice la restauración de nivel de base de datos en la ubicación original utilizando el punto de recuperación N.

   Se ha completado correctamente la restauración a un momento determinado. Verifique que los datos esperados se han restaurado en la base de datos.

Funcionamiento de la utilidad de la línea de comandos de la restauración a un momento determinado

La utilidad de la línea de comandos de la restauración a un momento determinado está disponible en la ruta *<Ruta de instalación de Arcserve UDP>\BIN* con el nombre de archivo *PIT.exe*.

El símbolo del sistema en la utilidad de la línea de comandos aparece como **PIT$**.

A continuación se muestran las opciones disponibles que se pueden ejecutar en la utilidad de la línea de comandos:

HELP

Muestra todas las opciones disponibles en PIT.exe.

COMMAND /?

Muestra el uso del comando.

CONFIG

Utiliza la configuración en el registro.

OPTION

Especifica la opción global. VALUE siempre es un número hexadecimal.

SEQ

Especifica el número de secuencia de la copia de seguridad de la base de datos o del registro de transacciones.

TIMEOUT

Especifica el tiempo de espera de la conexión, en segundos.

DEVICE

Especifica el tipo de dispositivo de la copia de seguridad que siempre es un disco.

DATABASE

Especifica el nombre de la base de datos. Especifique el valor con el formato *[servidor]\[instancia]\<Base de datos>*.

LOGBACKUP

Especifica la ruta de la copia de seguridad del registro de transacciones.

LOGRESTORE

Especifica la ruta de la restauración del registro de transacciones.

DBBACKUP

Especifica la ruta de la copia de seguridad del registro de transacciones.

DBRESTORE

Especifica la ruta de la restauración del registro de transacciones.

CATALOG

Especifica la ruta del catálogo.

STOPAT

Especifica el punto de tiempo para restaurar.

NORECOVERY

Especifica desactivar (1) o activar (0) la recuperación automática después de restaurar la base de datos de UDP.

PITBACKUP

Especifica activar (1) o desactivar (0) la copia de seguridad a un momento determinado para UDP.

Ejemplo: set pitbackup=1

PITRESTORE

Especifica activar (1) o desactivar (0) la restauración a un momento determinado para UDP.

Ejemplo: *set pitrestore=1*

PITTEMP

Carpeta temporal para la restauración a un momento determinado.

PITTIME

Especifica el punto de tiempo para la restauración a un momento determinado.

Ejemplo: set pittime="<MM/DD/AAAA HH:MM:SS:ss>

PITNOSTAGE

Especifica el uso del registro en el volumen montado en lugar de restaurar a la carpeta temporal.

BACKUPOPT

Especifica la opción de copia de seguridad para controlar VSS.

RESTOREOPT

Especifica la opción de restauración para controlar VSS.

A continuación se muestran las consultas SQL que se pueden ejecutar en la utilidad de la línea de comandos:

- *Query <NombreInstanciaSQL>\<NombreBaseDatos> <DestinoCopiaSeguridad>\Catalog\<Nombre carpeta de la sesión de copia de seguridad de N+1>*

  Muestra el resumen de todos los puntos de tiempo en la copia de seguridad.

- *Query /d <NombreInstanciaSQL>\<NombreBaseDatos> <DestinoCopiaSeguridad>\Catalog\<Nombre carpeta de la sesión de copia de seguridad de N+1>*

  Muestra todos los detalles del punto de tiempo en la copia de seguridad.

- *Query /i N <NombreInstanciaSQL>\<NombreBaseDatos> <DestinoCopiaSeguridad>\Catalog\<Nombre carpeta de la sesión de copia de seguridad de N+1>*

  Muestra el resumen del punto de tiempo de N en la copia de seguridad.

- *Query /d /i N <NombreInstanciaSQL>\<NombreBaseDatos> <DestinoCopiaSeguridad>\Catalog\<Nombre carpeta de la sesión de copia de seguridad de N+1>*

  Muestra los detalles del punto de tiempo de N en la copia de seguridad.

Cómo restaurar el volumen compartido de clúster

Cada vez que Arcserve UDP realiza una copia de seguridad correcta, se crea una imagen de instantánea en un momento determinado de la copia de seguridad (punto de recuperación). La recopilación de puntos de recuperación permite ubicar y especificar exactamente la imagen de copia de seguridad que desea restaurar. Si más tarde sospecha que falta información sobre la copia de seguridad realizada, o bien que se ha corrompido o que no es fiable, podrá buscar y restaurar desde una versión correcta anterior ya conocida.

¿Qué hacer a continuación?

1. Revisión de las consideraciones y requisitos previos
2. Especificación de la información de CSV para la restauración
   a. Especificación del CSV y del contenido para la restauración
   b. Definición de las opciones de restauración
3. Restauración del contenido de CSV

Revisión de las consideraciones y requisitos previos

Verifique que los requisitos previos siguientes existen antes de realizar una restauración:

- Como mínimo, existe un punto de recuperación disponible para restaurar.
- Tiene un destino del punto de recuperación válido y accesible desde el que poder restaurar el contenido del punto de recuperación.
- Tiene una ubicación de destino válida y accesible a la que poder restaurar el contenido del punto de recuperación.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones sobre la restauración:

- Si la restauración se debe realizar en un destino remoto y si todas las letras de unidad de disco (de la A a la Z) están ocupadas, la restauración a una ruta remota no se realizará correctamente. Arcserve UDPEl Agente de (Windows) debe utilizar una letra de unidad de disco para montar la ruta de destino remota.
- (Opcional) Debe entender cómo funciona el proceso de restauración. Para obtener más información, consulte Cómo funciona la restauración de nivel de archivo.
- (Opcional) Revise los archivos que se han omitido durante la restauración. Para obtener más información, consulte Archivos omitidos durante la restauración.
- Cuando se intenta restaurar una sesión de copia de seguridad optimizada en un volumen no vacío (restauración no optimizada), la tarea de restauración puede tardar más tiempo que la hora estimada que aparece en el controlador de tareas. La cantidad de datos que se procesa y el tiempo transcurrido puede aumentar en función de los datos que se optimizan en el volumen.

Ejemplo:

El tamaño del volumen de la copia de seguridad es de 100 GB y después de la optimización el tamaño del volumen se reduce a 50 GB.

Cuando se realiza una restauración no optimizada de este volumen, el controlador de tareas de restauración muestra 100% después de haber restaurado 50 GB, pero llevará más tiempo restaurar los 100 GB.

- El mensaje de registro de actividades siguiente se mostrará al restaurar los archivos del sistema:

Se han omitido los archivos del sistema. En caso necesario, se puede utilizar la opción Reconstrucción completa (BMR) para restaurarlos.

Cómo funciona la restauración de nivel de archivo

Durante una copia de seguridad de nivel de bloque, cada archivo con copia de seguridad está compuesto por una recopilación de bloques que definen el archivo en particular. Además, un archivo de catálogo también se crea de forma que contiene una lista de los archivos con copia de seguridad, junto con los bloques individuales que se han utilizado para cada archivo y los puntos de recuperación disponibles para los archivos. Si necesita restaurar un archivo en particular, puede buscar la copia de seguridad y seleccionar el archivo que desea restaurar y el punto de recuperación desde el cual desea empezar a restaurar. A continuación, Arcserve UDP recopilará la versión de los bloques que se han utilizado para el punto de recuperación del archivo especificado, volverá a unir el archivo y lo restaurará.

Nota: Se puede realizar también una restauración sin un archivo de catálogo desde un punto de recuperación de copia de seguridad sin catálogo.

El diagrama de flujo siguiente muestra el proceso de cómo Arcserve UDP restaura un archivo específico:

Archivos omitidos durante la restauración

Mientras el Agente de Arcserve UDP (Windows) realiza una restauración, algunos archivos se pueden omitir intencionadamente.

Se omiten los archivos y las carpetas en la tabla siguiente durante una restauración si se dan las dos condiciones siguientes:

- Se omiten archivos cuando existen tales archivos antes de la restauración y la opción de conflicto es Omitir archivos existentes.
- Se omiten archivos y carpetas que aparecen en la tabla siguiente porque no son un componente importante para Windows o para el Agente de Arcserve UDP (Windows).

SO	Carpeta o ubicación	Nombre del archivo o de la carpeta	Observaciones
Todo	Carpeta Root de cada volumen	CAVolTrc.dat	Utilizado por el controlador de seguimiento de Arcserve UDP.
		cavoltrcsnapshot.dat	
		Información acerca del volumen del sistema*	Utilizado para guardar archivos/carpetas por un sistema Windows, por ejemplo, archivos de instantánea de volumen.
		RECYCLER*	Utilizado solamente en particiones de NTFS. Contiene una papelera de reciclaje para todos los usuarios que se conecten al equipo, que se ordenarán en función del identificador de seguridad (SID).
		$Recycle.Bin*	Cuando se suprime un archivo en el explorador de Windows NT o Mi PC, el archivo se almacena en la Papelera de reciclaje hasta que se vacíe la Papelera de reciclaje o se restaure el archivo.
	Cualquier carpeta puede contener archivos de imagen	Thumbs.db	Almacena pequeñas imágenes para la vista en miniatura del Explorador de Windows.
	Carpeta Root del volumen	PageFile.sys	El archivo de intercambio de memoria virtual de Windows.
		Hiberfil.sys	Se trata del archivo de hibernación, que se utiliza para guardar los datos del sistema cuando un equipo se establece en el modo de hibernación.

Se omiten los archivos y las carpetas siguientes solamente cuando se restaura en la ubicación original o en otra ubicación:

SO	Carpeta o ubicación	Nombre del	Observaciones

		archivo o de la carpeta	
Todo	Carpeta especificada en el registro de valor que se encuentra en: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Todos los archivos/carpetas (recursivamente)	La carpeta contiene un archivo dll en memoria caché que se utiliza para el Comprobador de archivos de sistema (SFC) y el contenido del directorio dll en memoria caché del sistema se reconstruye mediante SFC.
	%SystemRoot%\SYSTEM32\dllCache		
	Carpeta Root de quorum_device	MSCS*	Utilizado para Microsoft Cluster Server.
	%SystemRoot%\SYSTEM32\	perf?00?.dat	Los datos de rendimiento utilizados por el contador de rendimiento de Windows.
		perf?00?.bak	
		CATROOT*	Utilizado para las firmas digitales de registros de la protección de archivos de Windows (WFP) del sistema operativo instala archivos como DLL, EXE, SYS, OCX, etc. para evitar y proteger su supresión o sustitución por versiones anteriores.
	%SystemRoot%\inetsrv\	metabase.bin	El archivo binario metabase de las versiones de IIS anteriores a 6.0.
	Archivo o carpeta especificados en el valor excepto almacenamiento común de SIS en	Todos los archivos/carpetas	No se debe realizar copia de

	HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup	(recursivamente)	seguridad ni acciones de restauración para archivos y/o carpetas. Para obtener más información, consulte este vínculo.
XP W2003	Volumen del sistema	NTLDR	El cargador de arranque principal.
		BOOT.INI	Contiene la configuración de arranque (si esta falta, NTLDR establecerá \Windows como predeterminado en la primera partición de la primera unidad de disco duro).
		NTDETECT.COM	Necesario para iniciar un sistema operativo de NT. Detecta información de hardware básica que es necesaria para un arranque correcto.
Vista y posteriores	Carpeta Root del volumen del sistema	boot*	Carpeta Boot para Windows.
		bootmgr	Archivo del gestor de arranque de Windows.
		EFI\Microsoft\Boot*	Utilizado para el arranque de EFI.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Almacena los archivos de seguimiento de ETW (extensión .etl) para las sesiones de seguimiento

			de eventos en tiempo real.
		con-fig\RegBack*	Copia de seguridad de la tabla de registro actual.
Win8 y posterio-res	Volumen del sistema	swapfile.sys	El archivo de controlador del sistema, normalmente alrededor de 256 MB. Utilizado por las aplicaciones de estilo Metro que no se ajustan a las características de paginación tradicionales (como patrón de uso, crecimiento, reserva de espacio) de pagefile.sys.
		BOOTNXT	Utilizado para iniciar el sistema operativo, distinto de Windows 8. Creado para activar las opciones de inicio y actualizado por Windows.

El registro de actividad proporciona la siguiente información:

- Información sobre la hora y la fecha: se omiten los archivos del sistema jobxxxx. Se puede utilizar la opción de recuperación completa (BMR) para restaurarlos.
- Información sobre la hora y la fecha: se omiten los archivos o directorios jobxxxx. Los archivos y directorios omitidos están disponibles en C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\Logs\Restore-<AAAAMMDD>-<hhmmss>-<ID del proceso>-<ID de la tarea>.log.

Especificación de la información de CSV para la restauración

Arcserve UDP proporciona una opción para restaurar datos desde un punto de recuperación. El objetivo de ejecutar una tarea de restauración correcta es de identificar los datos necesarios de forma rápida y de recuperarlos desde la ubicación de copia de seguridad correspondiente. Cada tarea de restauración necesita un origen y un destino.

¿Qué hacer a continuación?

1. Especificación del CSV y del contenido para la restauración
2. Definición de las opciones de restauración

Especificación del CSV y del contenido para la restauración

Utilice la opción **Explorar puntos de recuperación** para restaurar desde un punto de recuperación. Cuando se selecciona una fecha de recuperación y, a continuación, se especifica el tiempo, se muestran todos los puntos de recuperación asociados para esa duración. Tiene la opción de explorar y seleccionar el contenido de copia de seguridad (incluyendo las aplicaciones) para restaurar.

Siga estos pasos:

1. Acceda al cuadro de diálogo Selección del método de recuperación de una de las formas siguientes:

   En la Consola de Arcserve UDP:

   a. Inicie sesión en **Arcserve UDP**.

   b. Haga clic en la ficha **Recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos de agregados en el panel central.

   d. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   e. Haga clic en **Restaurar** del menú desplegable **Acción**.

      El cuadro de diálogo Selección del método de restauración se abre.

      Nota: Se inicia sesión automáticamente en el nodo del Agente y el cuadro de diálogo Selección del método de restauración se abre desde el nodo del Agente.

   Desde el Agente de Arcserve UDP (Windows):

a. Inicie sesión en el Agente de Arcserve UDP (Windows).

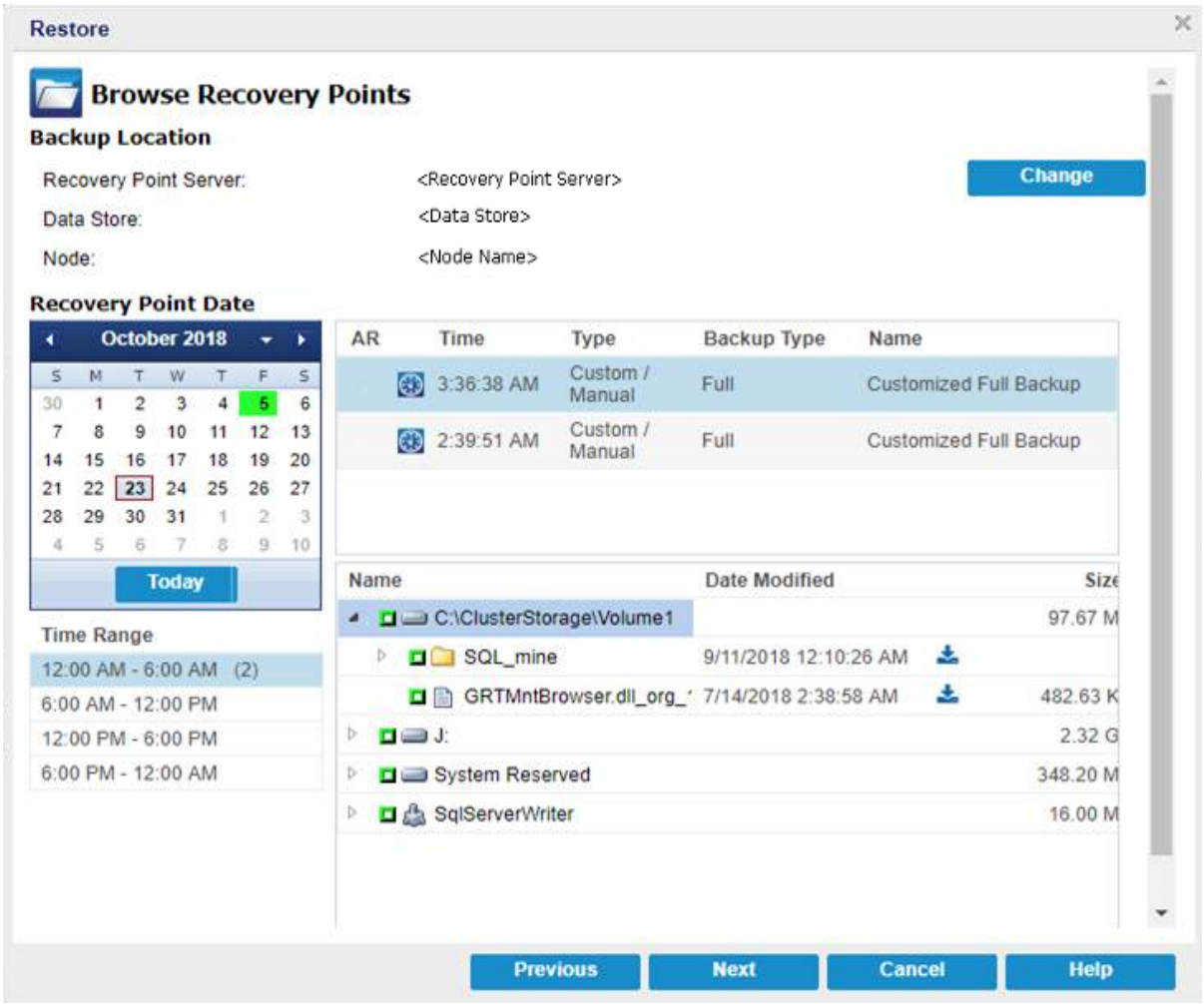
b. En la página principal, seleccione **Restaurar**.

El cuadro de diálogo Selección del método de restauración se abre.

2. Haga clic en la opción **Explorar puntos de recuperación**.

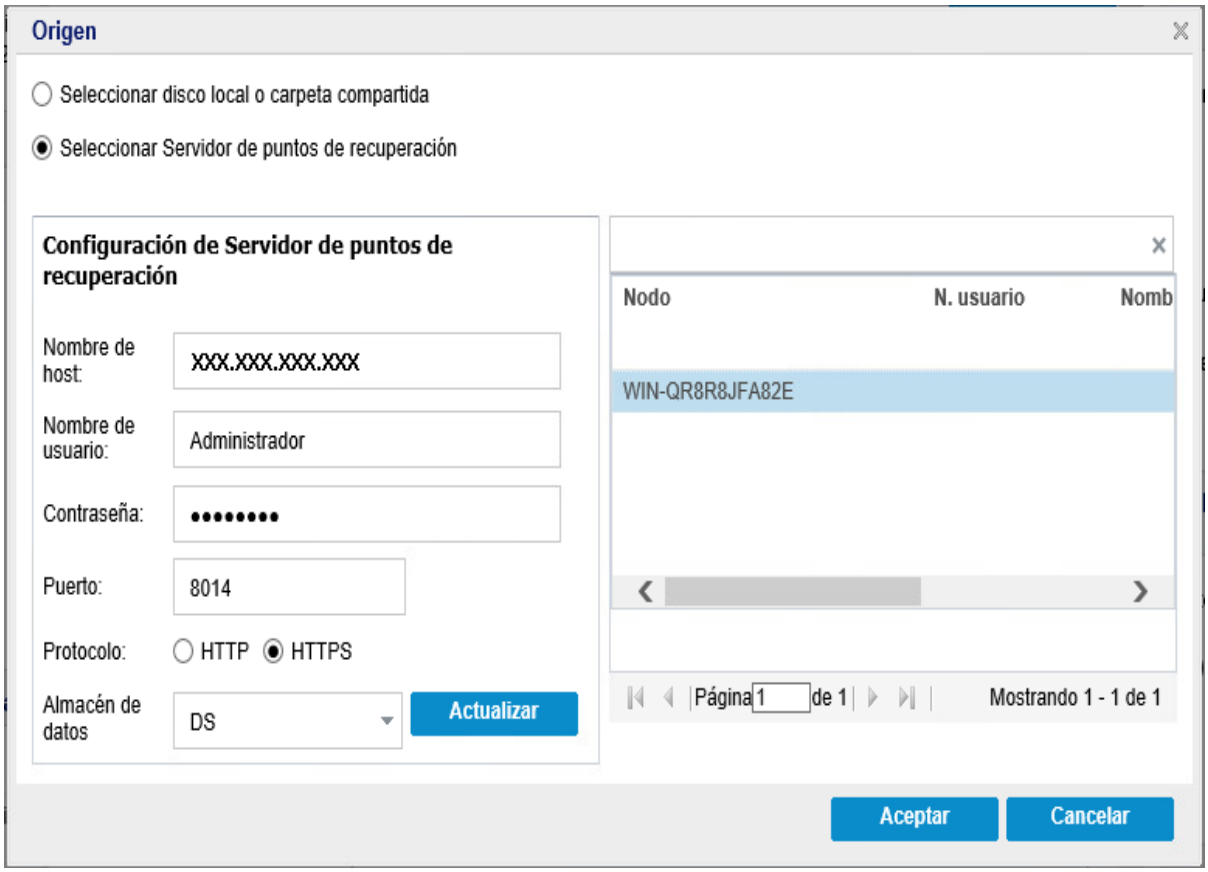
   Aparecerá el cuadro de diálogo **Explorar puntos de recuperación.** Se pueden ver los detalles del **Servidor de puntos de recuperación** en la **Ubicación de la copia de seguridad**.

   Recuperación asegurada indica el resultado de la ejecución si se ha ejecutado la recuperación asegurada para la sesión.



3. Haga clic en **Cambiar** para actualizar la ubicación de la copia de seguridad.

   El cuadro de diálogo **Origen** se abre donde se puede seleccionar la ubicación de la copia de seguridad.



4. Seleccione uno de los orígenes siguientes:

   Seleccionar disco local o carpeta compartida

   a. Especifique o vaya a la ubicación donde se almacenan las imágenes de copia de seguridad y seleccione el origen de la copia de seguridad adecuado.

      Se puede hacer clic en el botón de la flecha verde para comprobar la conexión con la ubicación especificada. Si es necesario, también puede escribir las credenciales de **Nombre de usuario** y **Contraseña** para obtener acceso a dicha ubicación de origen.

      El cuadro de diálogo **Selección de la ubicación de la copia de seguridad** se abre.

   b. Seleccione la carpeta en la cual se almacenan los puntos de recuperación y haga clic en **Aceptar**.

      El cuadro de diálogo **Selección de la ubicación de la copia de seguridad** se cierra y se puede ver la ubicación de la copia de seguridad en el cuadro de diálogo **Origen**.

   c. Haga clic en **Aceptar**.

Los puntos de recuperación se clasifican en el cuadro de diálogo **Examinar puntos de recuperación**.

Seleccionar servidor de puntos de recuperación

d. Especifique los detalles del valor de configuración del Servidor de puntos de recuperación y haga clic en **Actualizar**.

Todos los agentes se muestran en la columna Agente de protección de datos en el cuadro de diálogo Origen.

e. Seleccione el agente de la lista mostrada y haga clic en **Aceptar**.

Los puntos de recuperación se clasifican en el cuadro de diálogo **Examinar puntos de recuperación**.

5. Seleccione la fecha de calendario para la imagen de copia de seguridad que se desea restaurar.

Todas las fechas que contienen puntos de recuperación para el origen de la copia de seguridad especificado se resaltan en verde.

Aparecerán los puntos de recuperación correspondientes para la fecha, junto con la hora de la copia de seguridad, el tipo de copia de seguridad que se realiza (completa, incremental o de verificación) y el nombre de la copia de seguridad.

6. Seleccione un punto de recuperación para restaurar.

Se muestra el contenido de la copia de seguridad (incluyendo cualquier aplicación) del punto de recuperación seleccionado.

Nota: Si un icono de reloj aparece con el símbolo de candado, significa que el punto de recuperación contiene información cifrada y que puede requerir una contraseña para realizar la restauración.

7. Seleccione el volumen CSV que se va a restaurar.

- Para la restauración de nivel de volumen, es posible especificar la restauración del volumen entero o de los archivos o carpetas seleccionados integrados en el volumen.
- Para la restauración de nivel de aplicaciones, tiene la opción de especificar la restauración de la aplicación entera o de los componentes seleccionados, las bases de datos, las instancias, etcétera, integrados en la aplicación.

8. Haga clic en **Siguiente**.

Se abrirá el cuadro de diálogo **Opciones de restauración**.

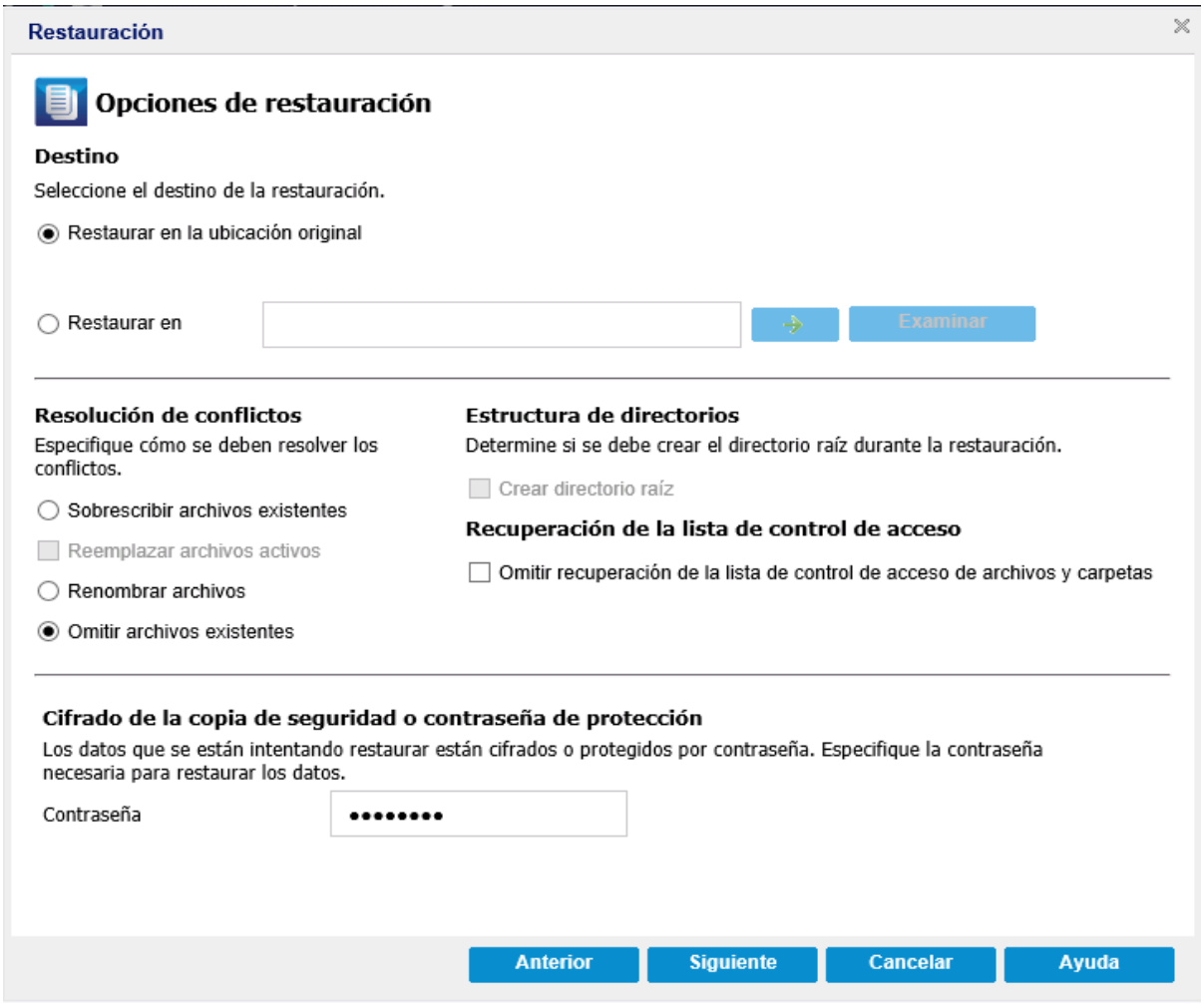
Se especifica el punto de recuperación y el contenido que se debe restaurar.

Definición de las opciones de restauración

Después de especificar un punto de recuperación y el contenido que se deben restaurar, defina las opciones de copia para el punto de recuperación seleccionado.

Siga estos pasos:

1. En el cuadro de diálogo **Opciones de restauración**, seleccione el destino para la restauración.



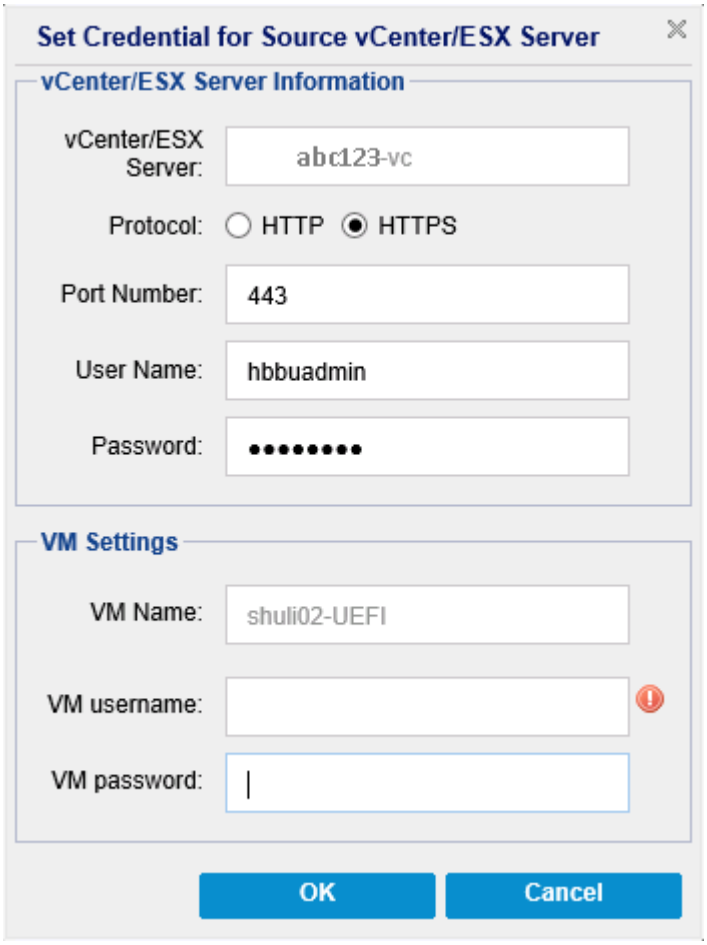
A continuación se especifican las opciones de destino disponibles:

Restaurar en la ubicación original

Restaura en la ubicación original desde la que se ha capturado la imagen de copia de seguridad.

Nota: Si se ha realizado la copia de seguridad del punto de recuperación utilizando la copia de seguridad sin agente basada en el host, la restauración en la ubicación original es volver a llevar a cabo la restauración del archivo en la máquina virtual. En este caso, se abre un cuadro de diálogo. Se pueden introducir las credenciales del hipervisor y el sistema operativo de la máquina virtual.

Para la máquina virtual de VMware:



Nota: Para poder crear o escribir archivos en la máquina virtual, tenga en cuenta los siguientes requisitos para la configuración y los permisos de la cuenta de la máquina virtual:

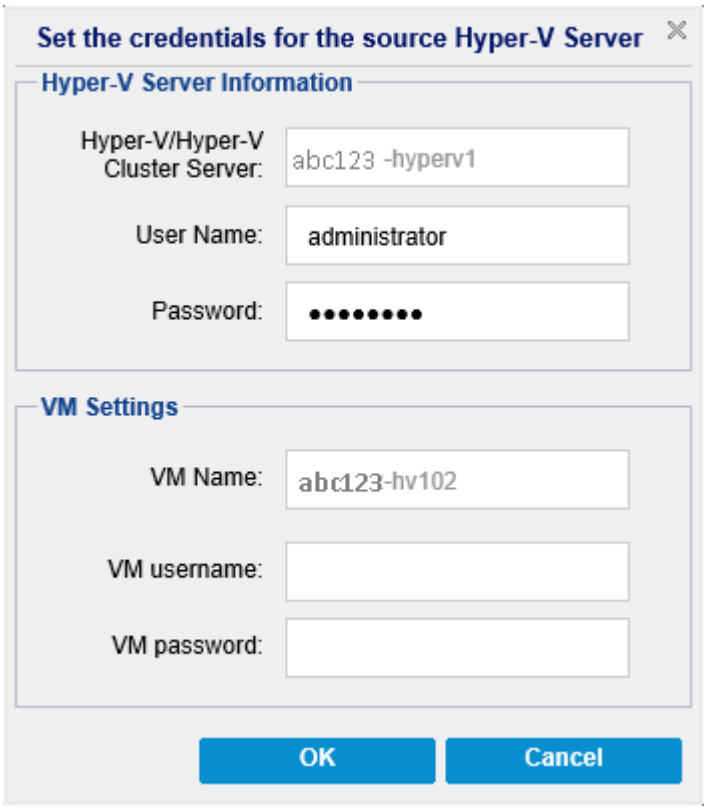
- VMware Tools está instalado y en ejecución.
- Firewall debe permitir compartir archivos e impresoras.
- La cuenta es el administrador local integrado, el administrador del dominio integrado o la cuenta del dominio que es miembro del

grupo de administradores locales. Si se utilizan otras cuentas, deberá realizar lo siguiente:

- Desactive el acceso remoto del Control de cuentas de usuario. Para desactivar el acceso remoto del UAC, consulte Importación de la máquina virtual utilizando una cuenta administrativa adicional.
- Desactive el Control de cuentas de usuario en la Política de seguridad local desactivando el valor de configuración Ejecutar todos los administradores en Modo de aprobación de administrador en secpol.msc-> Políticas locales-> Opciones de seguridad. (Secpol.msc es el editor de políticas de seguridad de Microsoft).

  Importante: No intente desactivar el Control de cuentas de usuario en el cuadro de diálogo Configuración del Control de cuentas de usuario que se abre desde el Panel de control.

Para la máquina virtual de Hyper-V:



Nota: Para poder crear o escribir archivos en la máquina virtual, tenga en cuenta los siguientes requisitos para la configuración y los permisos de la cuenta de la máquina virtual:

- Los servicios de integración de Hyper-V están instalados y en ejecución.
- Firewall debe permitir compartir archivos e impresoras.
- La cuenta es el administrador local integrado, el administrador del dominio integrado o la cuenta del dominio que es miembro del grupo de administradores locales. Si se utilizan otras cuentas:

  Desactive el acceso remoto del Control de cuentas de usuario. Para desactivar el acceso remoto del UAC, consulte Importación de la máquina virtual utilizando una cuenta administrativa adicional.
- Si el sistema operativo invitado de la máquina virtual es la versión de cliente de Windows (por ejemplo, Windows 10), se deberá configurar manualmente el cortafuegos para permitir el servicio Windows Management Instrumentation (WMI).

Restaurar en

Restaura en la ubicación especificada. Se puede hacer clic en el botón de la flecha verde para comprobar la conexión con la ubicación especificada. Si es necesario, también puede escribir las credenciales de nombre de usuario y de contraseña para obtener acceso a dicha ubicación.

2. En **Resolución de conflictos**, especifique la opción correspondiente a la acción que deberá realizar si se encuentran conflictos durante el proceso de restauración.Arcserve UDP

   A continuación se especifican las opciones disponibles:

   Sobrescribir archivos existentes

   Sobrescribe (reemplaza) todos los archivos existentes que se encuentran en el destino de restauración. Todos los objetos se restaurarán desde los archivos de copia de seguridad, independientemente de si actualmente se encuentran en el equipo.

   Reemplazar los archivos activos

   Reemplaza todos los archivos activos después del reinicio. Si durante el intento de restauración, el Agente de Arcserve UDP (Windows) detecta que el archivo existente está actualmente en uso o que algún usuario está accediendo al archivo, no sustituye ese archivo de forma inmediata, sino que retrasa la sustitución de los archivos activos hasta que se reinicie de nuevo el equipo con el fin de evitar problemas. La restauración ocurrirá de forma inmediata pero los archivos activos se sustituirán a partir del reinicio siguiente.

Esta opción solamente está disponible si selecciona la opción **Sobrescribir archivos existentes**.

Nota: Si no se selecciona esta opción, se omite de la restauración cualquier archivo activo.

Cambiar el nombre de los archivos

Si el nombre de archivo ya existe, crea un archivo nuevo. Al seleccionar esta opción se copiará el archivo de origen en el destino con el mismo nombre de archivo pero con una extensión diferente. A continuación, los datos se restaurarán en un archivo nuevo.

Omitir archivos existentes

Omite y no sobrescribe (reemplaza) ningún archivo existente que se encuentre en el destino de restauración. Solo se restaurarán desde los archivos de copia de seguridad los objetos que no estén en el equipo actualmente.

Valor por omisión: Omitir archivos existentes

3. Especifique la **Estructura de directorios** para crear un directorio raíz durante la restauración.

Crear directorio raíz

Especifica que si una estructura de directorio raíz existe en la imagen de copia de seguridad capturada, Arcserve UDP recreará la misma estructura de directorio raíz en la ruta de destino de la restauración.

Si no se selecciona esta opción, el archivo o carpeta se restaurará directamente en la carpeta de destino.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt" y "C:\Folder1\SubFolder2\B.txt" y durante la restauración ha especificado como destino de la restauración "D:\Restore".

- Si ha seleccionado la restauración de los archivos "A.txt" y "B.txt" de manera individual, el destino de los archivos restaurados será "D:\Restore\A.txt" y "D:\Restore\B.txt" (no se recreará el directorio raíz anterior en el nivel de archivo especificado).
- Si se selecciona la restauración desde el nivel "Subcarpeta2", el destino para los archivos restaurados será "D:\Restore\SubFolder2\A.txt" y "D:\Restore\SubFolder2\B.txt" (el directorio raíz superior al nivel de carpeta especificada no se recreará).

Con esta opción seleccionada, la ruta completa de directorio raíz para los archivos/carpetas (incluyendo el nombre de volumen) se recrea en la carpeta de destino. Si los archivos o carpetas que deben restaurarse provienen del mismo

nombre de volumen, la ruta del directorio raíz de destino no incluirá el nombre del volumen. Sin embargo, si los archivos o carpetas que deben restaurarse provienen de diferentes nombres de volúmenes, la ruta del directorio raíz de destino incluirá el nombre de volumen.

Por ejemplo, si durante la copia de seguridad ha capturado los archivos "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", y también E:\Folder3\SubFolder4\C.txt", y durante la restauración ha especificado el destino de restauración como "D:\Restore".

- Si ha seleccionado la restauración únicamente del archivo "A.txt", el destino para el archivo restaurado será "D:\Restore\Folder1\SubFolder2\A.txt" (se recreará todo el directorio raíz sin el nombre de volumen).
- Si ha seleccionado la restauración tanto del archivo "A.txt" como del archivo "C.txt", el destino para los archivos restaurados será "D:\Restore\C\ Folder1\SubFolder2\A.txt" y "D:\Restore\ E\Folder3\SubFolder4\C.txt" (se recreará todo el directorio raíz con el nombre de volumen).

4. En **Recuperación de la lista de control de acceso**, seleccione la opción **Omitir recuperación de la lista de control de acceso de archivos y carpetas** para omitir el permiso original para los archivos y carpetas restaurados. Al seleccionar esta opción se permite heredar los permisos de la carpeta de destino. Si no se selecciona esta opción, se mantienen los permisos originales.
5. Si es necesario, especifique la **Contraseña de cifrado de la copia de seguridad**, cuando los datos que se están intentando restaurar están cifrados.

   Si se intenta realizar una restauración desde el mismo equipo del Agente de Arcserve UDP para Windows desde el que se ha realizado la copia de seguridad cifrada, no es necesario proporcionar ninguna contraseña. Sin embargo, sí será necesaria una contraseña si se intenta realizar la restauración desde otro equipo del Agente de Arcserve UDP para Windows.

   Nota: Si un icono de reloj aparece con el símbolo de candado, significa que el punto de recuperación contiene información cifrada y que puede requerir una contraseña para realizar la restauración.
6. Haga clic en **Siguiente**.

   Se abrirá el cuadro de diálogo **Resumen de la restauración**.

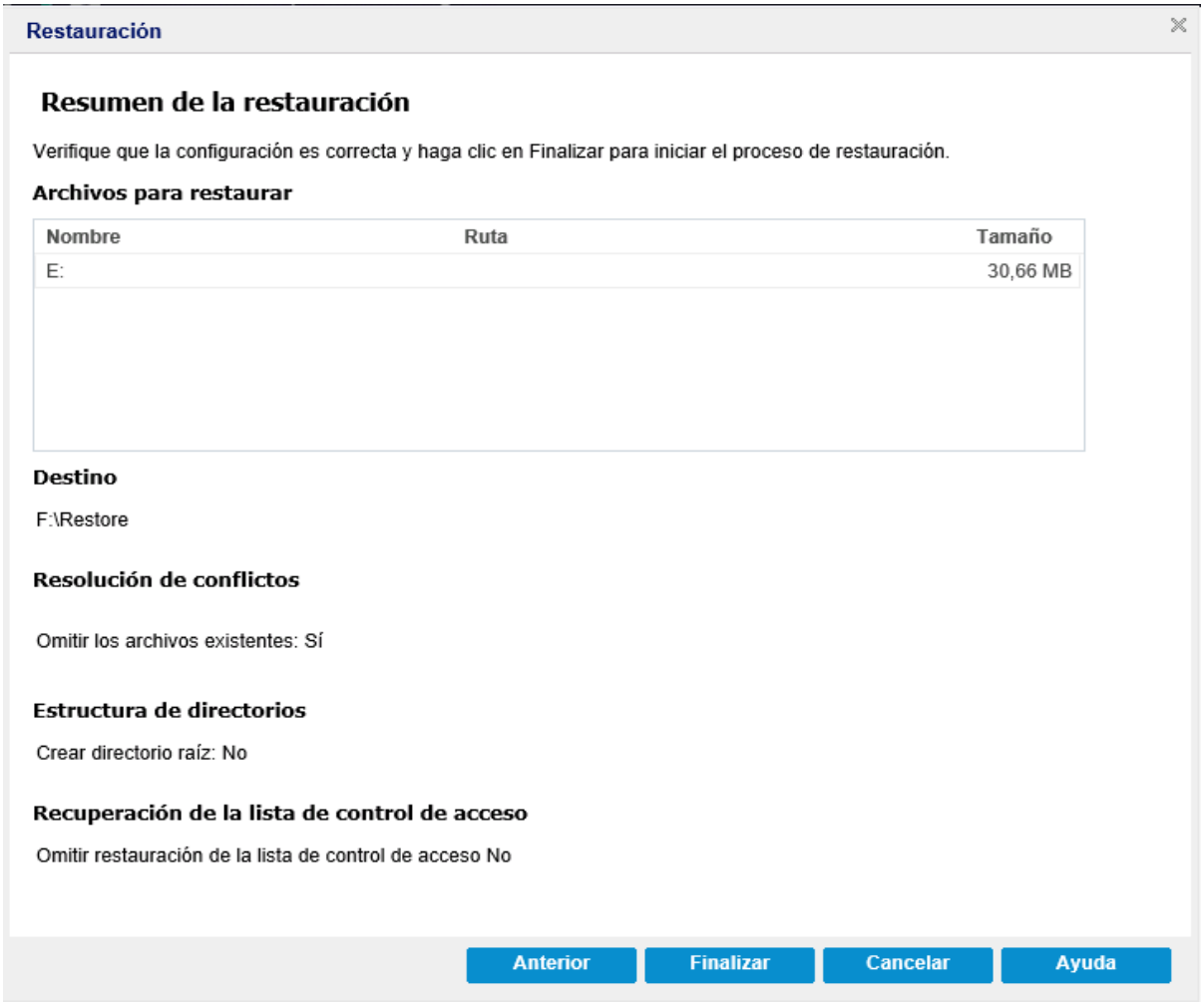
   Las opciones de restauración se han definido para restaurar desde un punto de recuperación.

Restauración del contenido de CSV

Después de definir las opciones de restauración, verifique que los valores de configuración sean correctos y confirme el proceso de restauración. El **Resumen de la restauración** le ayuda a revisar todas las opciones de la restauración definidas y a modificarlas si es necesario.

Siga estos pasos:

1. En el cuadro de diálogo **Resumen de la restauración**, revise la información que aparece en pantalla para verificar que todas las opciones de restauración y los valores de configuración sean correctos.



- Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para cambiar el valor de configuración incorrecto.

- Si la información de resumen es correcta, haga clic en **Finalizar** para iniciar el proceso de restauración.

El contenido del punto de recuperación se restaura.

Capítulo 2: Gestión de restauración y copia de seguridad de cintas

Arcserve UDP permite realizar copias de seguridad de los datos en una cinta y restaurar la copia de seguridad de los datos de la cinta a un nodo.

Esta sección incluye los siguientes temas:

Cómo realizar la copia de seguridad de un almacén de datos de deduplicación en una cinta

Para realizar la copia de seguridad de un almacén de datos de deduplicación en una cinta, utilice los métodos siguientes:

- Copia de seguridad de los nodos de UDP en cinta. Para obtener más información, consulte la sección Método 1: Copia de seguridad de la última sesión de copia de seguridad de UDP en cinta que se encuentra en la Guía de administración de Arcserve Backup.
- Copia de seguridad de los datos de Arcserve UDP desde almacenes de datos. Para obtener más información, consulte la sección Método 2: Copia de seguridad de los datos de Arcserve UDP desde almacenes de datos que se encuentra en la Guía de administración de Arcserve Backup.

Cómo restaurar un almacén de datos de deduplicación desde una cinta

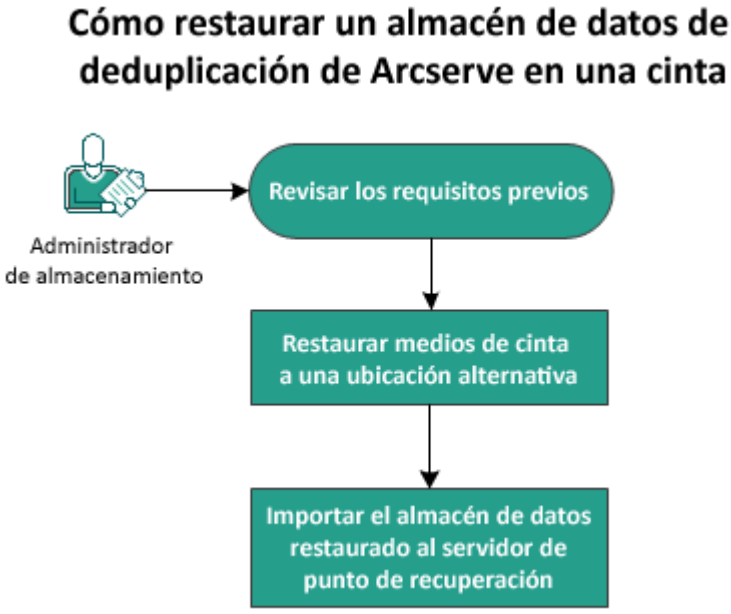
Si se ha realizado una copia de seguridad de un almacén de datos de deduplicación desde un servidor de puntos de recuperación (RPS) a un dispositivo de cinta, se podrá restaurar el almacén de datos. Para este procedimiento, Arcserve Backup y Arcserve UDP se utilizan combinados para restaurar un almacén de datos de deduplicación desde una cinta. Arcserve Backup se utiliza para restaurar el almacén desde la cinta a un destino especificado y, a continuación, se utiliza Arcserve UDP para importarlo a un servidor de puntos de recuperación.

Los dos procesos siguientes están implicados en el procedimiento de restauración:

1. El primer proceso utiliza Arcserve Backup para restaurar las sesiones desde los medios de cinta a un volumen. Se recomienda restaurar las sesiones en una ubicación alternativa.
2. El segundo proceso utiliza Arcserve UDP para importar el almacén de datos restaurados al servidor de puntos de recuperación.

   Nota: Se deberá proporcionar la ruta de la **Carpeta de destino de la copia de seguridad** del almacén de datos de deduplicación al examinar la ubicación durante la importación.

El siguiente diagrama resume cómo restaurar un almacén de datos de deduplicación de Arcserve desde una cinta:



¿Qué hacer a continuación?

1. Revisión de los requisitos previos
2. Restaurar desde un medio de cinta a una ubicación alternativa
3. Importar el almacén de datos restaurado al servidor de puntos de recuperación

Revisión de los requisitos previos

Revise los requisitos previos siguientes antes de iniciar la restauración:

- Se debe haber realizado la copia de seguridad de un almacén de datos del servidor de puntos de recuperación en la cinta.
- Si es necesario, se podrá proporcionar la contraseña de sesión.
- Será necesario proporcionar el nombre de usuario y la contraseña para el destino de la restauración.

Restaurar desde un medio de cinta a una ubicación alternativa

Para restaurar la sesión desde el medio de cinta a una ubicación alternativa, se deberá utilizar el Gestor de Arcserve Backup.

Una vez que la restauración se ha realizado correctamente, se puede importar el almacén de datos restaurado al servidor de puntos de recuperación mediante Arcserve UDP.

Siga estos pasos:

1. En Arcserve Backup, inicie sesión en el Gestor de Arcserve Backup.
2. En el panel de navegación **Inicio rápido**, haga clic en **Restaurar** y, a continuación, en el panel central, seleccione la ficha **Origen**.
3. En el menú desplegable, seleccione **Restaurar por sesión** y seleccione la sesión que se va a restaurar.
4. Haga clic en la ficha **Destino**.
5. Deseleccione (desactive) la casilla de verificación **Restaurar archivos a sus ubicaciones originales**.
6. Expanda el objeto **Sistemas Windows** y desplácese hasta la ubicación en donde se desea restaurar.
7. Haga clic en la ficha **Programación** y seleccione **Una vez** para la opción **Método de repetición**.
8. Haga clic en **Enviar**.

   Se abrirá el cuadro de diálogo **Medios de restauración**.
9. Verifique el medio de restauración y haga clic en **Aceptar**.

   Aparecerá el cuadro de diálogo **Nombre de usuario y contraseña de sesión**.
10. Proporcione el nombre de usuario y la contraseña para la ubicación de la restauración y la contraseña de sesión para los puntos de recuperación, si es necesario.
11. Haga clic en **Aceptar**.

    Se abrirá el cuadro de diálogo **Enviar tarea**.
12. Proporcione la información necesaria en el cuadro de diálogo **Enviar tarea** y haga clic en **Aceptar**.

    Se envía la tarea de restauración.

Una vez completada la tarea de restauración, los archivos del almacén de datos de Arcserve UDP se mostrarán en la ubicación especificada.

Importación del almacén de datos restaurado al servidor de puntos de recuperación

Para importar el almacén de datos restaurado al Servidor de puntos de recuperación, se deberá utilizar la Consola de Arcserve UDP. La función **Importar almacén de datos** le permite agregar un almacén de datos al servidor de puntos de recuperación. Se puede importar cualquier almacén de datos existente a un servidor de puntos de recuperación.

Siga estos pasos:

1. En la Consola, haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se muestra la página **Destinos: Servidores de puntos de recuperación**.
3. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en un servidor de puntos de recuperación.
   - Seleccione un servidor de puntos de recuperación y en el menú central haga clic en la lista desplegable **Acciones**.
4. Haga clic en **Importar almacén de datos**.

   Se muestra la página **Importación de un almacén de datos**.
5. Realice las acciones siguientes y haga clic en **Siguiente**:
   a. Haga clic en **Examinar** y seleccione la **Carpeta de destino de la copia de seguridad** desde donde se desea importar el almacén de datos.
   b. Si hace falta, introduzca la **Contraseña de cifrado**.

      Nota: Si no se cifra el almacén de datos, se podrá dejar vacío este campo.

   Después de autenticar la **Carpeta de destino de la copia de seguridad**, la página **Importación de un almacén de datos** muestra los detalles del almacén de datos.

   Nota: No se admite la importación del almacén de datos restaurado si el almacén de datos original está presente en el mismo servidor de puntos de recuperación. Debe suprimir el almacén de datos original antes de importar el almacén de datos restaurado o, alternativamente, importar el almacén de datos a otro servidor de puntos de recuperación.
6. Si es necesario, modifique los detalles del almacén de datos y haga clic en **Guardar**.

Cuando se importa el almacén de datos restaurados, Arcserve UDP continuará leyendo los destinos de datos, índice y hash de los valores de configuración del almacén de datos y mostrará las rutas reales donde se encontraba originalmente el almacén de datos. Después de completar la importación, es necesario cambiar estos destinos de las rutas por las nuevas rutas restauradas.

Nota: No se puede activar o desactivar la opción de cifrado para un almacén de datos existente.

El almacén de datos se agrega al servidor de puntos de recuperación y se muestra en el cuadro de diálogo **Destinos: Servidores de puntos de recuperación**.

Tras la finalización de una importación correcta, aparecerá una marca de verificación verde junto al nombre del almacén de datos correspondiente.

Se ha restaurado correctamente un almacén de datos de deduplicación desde una cinta.

Capítulo 3: mediante la interfaz de PowerShell

Esta sección incluye los siguientes temas:

Cómo utilizar la interfaz de PowerShell

Arcserve UDP proporciona funciones de PowerShell que permiten enviar una tarea de copia de seguridad, realizar una restauración y recuperar la máquina virtual desde la línea de comandos. La interfaz de PowerShell se llama UDPPowerCLI.ps1.

Revisión de los requisitos previos

Revise los requisitos previos siguientes antes de usar la interfaz de PowerShell:

- Debe tener Windows Server 2008 R2 o versiones posteriores.
- Debe tener PowerShell 3 o una versión posterior instalada en el servidor.

Uso de la interfaz de PowerShell para Arcserve UDP

La utilidad PowerShell está incluida en el archivo de instalación de Arcserve UDP.

Cuando se instala Arcserve UDP, por lo general el archivo se instala en la ubicación siguiente:

C:\Archivos de programa\Arcserve\Unified Data Protection

En tales casos, en la Consola, UDPPowerCLI.ps1 se instala en la ubicación siguiente:

C:\Archivos de programa\Arcserve\Unified Data Protection\Management\PowerCLI

En el servidor de puntos de recuperación o en el Agente, UDPPowerCLI.ps1 se instala en la ubicación siguiente:

C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\PowerCLI

Consulte las siguientes opciones para ayudarle a utilizar la interfaz de PowerShell:

- Actualice la política de ejecución de PowerShell para permitir que se ejecuten los scripts. Por ejemplo, actualice la política de ejecución a **Set-ExecutionPolicy RemoteSigned**.

  Nota: Para obtener más información sobre la modificación de la política de ejecución, consulte el sitio web de Microsoft.

- Ejecute el siguiente comando de PowerShell para obtener mensajes de ayuda con información detallada y ejemplos de scripts:

  ```
  En la Consola:
  ```

  Get-Help 'C:\Archivos de programa\Arcserve\Unified Data Protection\Management\PowerCLI\UDPPowerCLI.ps1' -full

  En el servidor de puntos de recuperación o en el Agente:

  Get-Help 'C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\PowerCLI\UDPPowerCLI.ps1' -full

Sintaxis y parámetros de PowerShell

SINTAXIS 1

```
UDPPowerCLI.ps1 -Command <CreatePswFile> -Password
<System.Security.SecureString> -PasswordFile <string>
[<CommonParameters>]
```

SINTAXIS 2

```
UDPPowerCLI.ps1 -Command <Backup> [-UDPCon-
soleServerName <String>] [-UDPConsoleProtocol <{http|h-
ttps}>] [-UDPConsolePort <int>] [-UDPConsoleUserName
[<String>]] [-UDPConsolePassword <Sys-
tem.Security.SecureString>] [-UDPConsolePasswordFile
<String>] [-UDPConsoleDomainName <String>] -planName
<String> -nodeName <String> [-backupJobType <String>]
[-jobDescription <String>] [-waitJobFinish <String
String>] [-timeOut <int>] [-jobType <{ agen-
tbase|agentless|uncpath} String>] [-backupScheduleType
<String>] [<CommonParameters>]
```

SINTAXIS 3

```
UDPPowerCLI.ps1 -Command <Restore> [-UDPCon-
soleServerName <String>] [-UDPConsoleProtocol
<String>] [-UDPConsolePort <int>] [-UDPConsoleUserName
<String>] [-UDPConsolePassword <Sys-
tem.Security.SecureString>] [-UDPConsolePasswordFile
<String>] [-UDPConsoleDomainName <String>] [-UDPA-
gentServerName <String>] [-UDPAgentProtocol <String>]
[-UDPAgentPort <int>] [-UDPAgentUserName <String>] [-
UDPAgentPassword <System.Security.SecureString>] [-
UDPAgentPasswordFile <String>] [-UDPAgentDomainName
<String>] [-RestoreDirectoryPath <String>] [-Res-
toreFilePath <String>] [-BackupSessionNumber <int>] [-
VmName <String>] -RestoreDestination <String> [-Res-
toreDestinationUserName <String>] [-Res-
toreDestinationPassword
<System.Security.SecureString>] [-CreateRootFolder
<String>] [-ChangeFileName <String>] [-Repla-
ceActiveFilesFlag <String>] [-OverwriteExistFiles
<String>] [<CommonParameters>]
```

SINTAXIS 4

```
UDPPowerCLI.ps1 -command <RecoverVM> [-UDPCon-
soleServerName <String>] [-UDPConsoleProtocol
<String>] [-UDPConsolePort <int>] [-UDPConsoleUserName
<String>] [-UDPConsolePassword
```

```
<System.Security.SecureString>] [-UDPCon-
solePasswordFile <String>] [-UDPConsoleDomainName
<String>] [-UDPAgentServerName <String>] [-UDPA-
gentProtocol <String>] [-UDPAgentPort <int>] [-UDPA-
gentUserName <String>] [-UDPAgentPassword
<System.Security.SecureString>] [-UDPAgentDomainName
<String>] [-UDPAgentPasswordFile <String>] [-Backu-
pSessionNumber <int>] -RecoverVmName <String> [-Ove-
rwriteExistingVM <String>] [-PoweronVM <String>]
[<CommonParameters>]
```

DESCRIPCIÓN

Una utilidad para conectarse al servicio de la Consola de Arcserve UDP y enviar tareas de copia de seguridad y restauración.

PARÁMETROS

-Command <String>

Especifica el comando que se utiliza. Actualmente, se admiten las siguientes cadenas:

- CreatePswFile
- Copia de seguridad
- Restauración
- RecoverVM

¿Obligatorio? **true**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-Password <System.Security.SecureString>

Especifica la contraseña que desea utilizar para crear el archivo de contraseñas.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPConsoleServerName <String>

Especifica el nombre DNS del servidor UDP (el servidor en el que ha instalado la Consola) con el que se desea realizar la conexión. Si no se especifica este valor, el cmdlet utiliza el valor predeterminado, el nombre DNS del equipo local.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **$env:COMPUTERNAME**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPConsolePort <int>

Especifica el número de puerto que se desea usar para la conexión. Si no se especifica este valor, el cmdlet utiliza el valor predeterminado, 8015.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **8015**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPConsoleProtocol <String>

Especifica el protocolo del servidor que se desea usar para la conexión. El protocolo puede ser http o https. Si no se especifica este valor, el cmdlet utiliza el valor predeterminado, http.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **http**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPConsoleUserName <String>

Especifica el nombre de usuario que se desea usar para realizar la conexión al servidor UDP. Si no se especifica el nombre de usuario, el cmdlet utilizará el que se usa actualmente para iniciar sesión en el sistema.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **$env:UserName**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPConsolePassword <System.Security.SecureString>

Especifica la contraseña que se desea usar para realizar la conexión al servidor UDP.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-PasswordFile <String>

Especifica la generación del archivo de contraseña.

¿Obligatorio? **true**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPConsolePasswordFile <String>

Especifica el archivo de contraseña de UDP que se desea usar para realizar la conexión al servidor UDP.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPAgentServerName <String>

Especifica el nombre DNS del servidor del Agente de UDP con el que se desea conectar para realizar la restauración.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **$env:COMPUTERNAME**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPAgentProtocol <String>

Especifica el protocolo de Internet que se desea usar para conectarse al servidor del Agente de UDP. Puede ser http o https. Si no se especifica este valor, el cmdlet utiliza el valor predeterminado, http.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **http**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPAgentPort <int>

Especifica el número de puerto que se desea usar para conectarse al servidor del Agente de UDP. Si no se especifica este valor, el cmdlet utiliza el valor predeterminado, 8014.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **8014**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPAgentUserName <String>

Especifica el nombre de usuario que se desea usar para conectarse al servidor del Agente de UDP. Si no se especifica el nombre de usuario, el cmdlet utilizará el que se usa actualmente para iniciar sesión en el sistema.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **$env:UserName**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPAgentPassword <System.Security.SecureString>

Especifica la contraseña que se desea usar para conectarse al servidor del Agente de UDP.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPAgentPasswordFile <String>

Especifica el archivo de contraseña del agente de UDP que se desea usar para conectarse al servidor del Agente de UDP.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPAgentDomainName <String>

Especifica el nombre de dominio donde se encuentra el usuario del Agente de UDP especificado.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-NodeName <String>

Especifica el nombre del nodo del que se desea realizar una copia de seguridad.

¿Obligatorio? **true**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-RestoreFilePath <String>

Especifica el archivo que se desea restaurar.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-RestoreDirectoryPath <String>

Especifica el directorio que se desea restaurar.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-BackupSessionNumber <int>

Especifica el número de sesión que se va a utilizar para la tarea de restauración.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-VmName <String>

Especifica el nombre de host de una máquina virtual para restaurar el archivo o el directorio desde la sesión de copia de seguridad.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-RestoreDestination <String>

Especifica la ruta del directorio en la que se restaurarán los archivos.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-RestoreDestinationUserName <String>

Especifica el nombre de usuario del equipo de destino en el que se desea restaurar los datos. El nombre de usuario pertenece al usuario que puede iniciar sesión en el equipo de destino.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-RestoreDestinationPassword <System.Security.SecureString>

Especifica la contraseña que se utilizará para iniciar sesión en el equipo de destino.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-CreateRootFolder <String>

Especifica que si existe una estructura de directorio raíz en la imagen de copia de seguridad capturada, Arcserve UDP recreará la misma estructura de directorio raíz en la ruta de destino de la restauración. Si no se selecciona esta opción, el archivo o la carpeta se restaurarán directamente en la carpeta de destino. Se puede usar cualquiera de las cadenas siguientes:

- True
- False

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **False**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-ChangeFileName <String>

Si el nombre de archivo ya existe, crea un archivo nuevo. Al seleccionar esta opción se copiará el archivo de origen en el destino con el mismo nombre de archivo pero con una extensión diferente. A continuación, los datos se

restaurarán en un archivo nuevo. Se puede usar cualquiera de las cadenas siguientes:

- True
- False

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **False**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-ReplaceActiveFilesFlag <String>

Reemplaza todos los archivos activos después del reinicio. Si durante el intento de restauración el Agente de Arcserve Unified Data Protection para Windows descubre que el archivo existente está actualmente en uso o que alguien está accediendo a él, no sustituirá el archivo de forma automática, sino que para evitar cualquier problema aplazará la sustitución de los archivos activos hasta la próxima vez que el equipo se reinicie. (La restauración ocurrirá de forma inmediata pero los archivos activos se sustituirán a partir del reinicio siguiente). Esta opción solo está disponible cuando el parámetro **OverwriteExistingFiles** presenta el valor True. Se puede usar cualquiera de las cadenas siguientes:

- True
- False

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **False**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-OverwriteExistingFiles <String>

Sobrescribe (reemplaza) todos los archivos existentes que se encuentran en el destino de restauración. Todos los objetos se restaurarán desde los archivos de copia de seguridad, independientemente de si actualmente se encuentran en el equipo. Se puede usar cualquiera de las cadenas siguientes:

- True
- False

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **False**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-UDPConsoleDomainName <String>

Especifica el nombre de dominio donde se encuentra el usuario especificado. Si no se especifica este valor, el cmdlet utiliza el nombre de dominio del equipo local o el nombre DNS del equipo local si no se encuentra en un dominio.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-PlanName <String>

Especifica el nombre del plan que define la configuración de la tarea de copia de seguridad.

¿Obligatorio? **true**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-BackupJobType <String>

Especifica el tipo de la tarea de copia de seguridad. Se puede utilizar uno de los siguientes valores: Full (indica una copia de seguridad completa), Incr (indica una copia de seguridad incremental) o Rsyn (indica una copia de seguridad de resincronización). Se admiten las siguientes cadenas:

- Completa
- Incr
- Rsyn

¿Obligatorio? **true**

¿Posición? **named**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-JobDescription <String>

Especifica la descripción para la tarea de copia de seguridad.

¿Obligatorio? **true**

¿Posición? **named**

Valor predeterminado **PowerCLIJo**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-RecoverVmName <String>

Especifica el nombre de host de la máquina virtual que se desea recuperar.

¿Obligatorio? **true**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-OverwriteExistingVM <String>

Especifica que, si el valor es true, la tarea de restauración sobrescribe la máquina virtual existente. El valor predeterminado es false. Se puede usar cualquiera de las cadenas siguientes:

- True
- False

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **False**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-PoweronVM <String>

Especifica que, si el valor es true, la máquina virtual se enciende después de la recuperación. El valor predeterminado es false. Se puede usar cualquiera de las cadenas siguientes:

- True
- False

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **False**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-waitJobFinish <{true|false} String>

Especifica que, si el valor es true, el comando espera para obtener instrucciones más detalladas hasta que se complete la tarea de copia de seguridad. El valor predeterminado es false. Se puede usar cualquiera de las cadenas siguientes:

- True
- Falso

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **False**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-timeOut <int>

Especifica el tiempo de espera máximo (en segundos) para que finalice la tarea de copia de seguridad.

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **600**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-jobType <String>

Especifica el tipo de tarea de copia de seguridad para los diferentes tipos de nodo. El valor predeterminado es agentbase. Utilice cualquiera de las cadenas siguientes:

- agentbase
- agentless
- uncpath

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado **agentbase**

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

-backupScheduleType <String>

Especifica la tarea de copia de seguridad de la programación, envía la tarea de copia de seguridad de la programación especificada inmediatamente y se ejecuta solo una vez. Se admiten las siguientes cadenas:

- Diario
- Cada semana
- Cada mes

¿Obligatorio? **false**

¿Posición? **named**

Valor predeterminado

¿Aceptar la entrada de canalización? **false**

¿Aceptar caracteres comodín? **false**

<CommonParameters>

Este cmdlet admite los parámetros comunes, como **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer** y **OutVariable**. Para obtener más información, consulte about_CommonParameters.

ENTRADAS

SALIDAS

- 0 o 1

Si la tarea se ha enviado correctamente, el comando devuelve 0; de lo contrario, devuelve el valor 1.

Ejemplos de PowerShell

Creación del tipo System.Security.SecureString de contraseña

Nota: Si tiene un script de PowerShell configurado en Arcserve UDP 6.5 que utiliza una contraseña de texto sin formato, modifíquelo para que utilice $SecurePassword o el archivo de contraseñas.

Descripción

El comando se utiliza para crear la contraseña con el tipo System.Security.SecureString y también se utiliza con todos los otros comandos. El tipo System.Security.SecureString es el tipo predefinido del sistema. Hay varias formas de generar este tipo. Los dos tipos siguientes se utilizan normalmente para distintos fines:

- Este comando solicita introducir la contraseña en la Consola de PowerShell. Requiere una interacción con los usuarios finales. Por lo general, después de ejecutar este comando se puede ejecutar el comando *CreatePswFile* para escribir la contraseña en un archivo de contraseñas. A continuación, utilice el archivo de contraseñas para ejecutar scripts de PowerShell automáticamente.

  ```
  $SecurePassword = Read-Host -AsSecureString
  ```

- Este comando requiere la contraseña con texto sin formato. Se puede utilizar directamente para ejecutar scripts de PowerShell automáticamente.

  ```
  $SecurePassword = ConvertTo-SecureString "<PlainPassword>" - AsPlainText - Force
  ```

- (Opcional) Después de ejecutar uno de los comandos anteriores para asignar una contraseña, ejecute el comando CreatePswFile para escribir la contraseña en un archivo de contraseñas. A continuación, utilice el archivo de contraseñas para ejecutar scripts de PowerShell automáticamente.

  El comando cifra la contraseña segura y la guarda en el archivo de contraseñas.

  ```
  C:\PS>UDPPowerCLI.ps1 -Command CreatePswFile -Password $SecurePassword -PasswordFile myUDPPasswordFile
  ```

Ejemplo 1

Descripción

El comando cifra la contraseña segura y la guarda en el archivo de contraseñas.

```
C:\PS>UDPPowerCLI.ps1 -Command CreatePswFile -Password
$SecurePassword -PasswordFile myUDPPasswordFile
```

Ejemplo 2

Descripción

En el servidor local, el comando se conecta con el servicio de la Consola de UDP con el protocolo de HTTP a través del puerto 8015 y, a continuación, envía una tarea de copia de seguridad incremental para el plan llamado *myplan*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleUserName myUsr -UDPConsolePassword $SecurePassword
-PlanName myPlan -BackupJobType Incr
```

Ejemplo 3

Descripción

En el servidor local, el comando se conecta con el servicio de la Consola de UDP con el protocolo de HTTP a través del puerto 8015 y, a continuación, envía una tarea de copia de seguridad incremental para el nodo llamado *myNodeName*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleUserName myUsr -UDPConsolePasswordFile myUDPPa-
sswordFile -NodeName myNodeName -BackupJobType Incr
```

Ejemplo 4

Descripción

El comando se conecta con el servicio de la Consola de UDP en el servidor llamado *myServer* con el protocolo HTTPS a través del puerto 8018 y, a continuación, envía una tarea de copia de seguridad completa para el plan llamado *myPlan* y establece la descripción de la tarea como *myJob*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleServerName myServer -UDPConsoleProtocol https -
UDPConsolePort 8018 -UDPConsoleUserName myUsr -UDPCon-
solePassword $SecurePassword -UDPConsoleDomainName
myDomain -PlanName myPlan -BackupJobType Full -JobDes-
cription myJob
```

Ejemplo 5

Descripción

El comando se conecta con el servicio del Agente de UDP en el servidor llamado *yourUDPAgentServer* con el protocolo HTTP a través del puerto 8014 y, a continuación, envía una tarea de copia de seguridad incremental para *yourUDPAgentServer*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPA-
gentServerName yourUDPAgentServer -
```

```
UDPAgentPasswordFile myUDPAgentPasswordFile -Backu-
pJobType Incr
```

Ejemplo 6

Descripción

El comando reduce el nombre del parámetro.

```
C:\PS>UDPPowerCLI.ps1 -Cmd Backup -Svr myServer -Ptc
https -Prt 8018 -Usr myUsr -Psw $SecurePassword -Dmn
myDomain -Pln myPlan -Jbt Full -Jbd myJob
```

Ejemplo 7

Descripción

El comando se conecta con el servidor denominado *yourUDPAgentServer* utilizando el nombre de usuario del entorno, el protocolo HTTP predeterminado y el puerto 8014. Verifica que el número de sesión de copia de seguridad es 1 en la configuración de copia de seguridad *yourUDPAgentServer* y, a continuación, restaura el directorio a la ubicación original, con la opción de restauración Sobrescribir archivos existentes seleccionada.

```
C:\PS>UDPPowerCLI.ps1 -Command restore -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
RestoreDirectoryPath 'c:\Test' -BackupSessionNumber 1
```

Ejemplo 8

Descripción

El comando se conecta con el servidor denominado *yourUDPAgentServer* utilizando el protocolo HTTPS y el puerto 8018. Verifica que el número de sesión de copia de seguridad es 1 en la configuración de copia de seguridad *yourUDPAgentServer* y, a continuación, restaura el archivo 1.txt a una ubicación alternativa, con la opción de restauración Overwrite existing file and create root directory (Sobrescribir archivos existentes y crear directorio raíz) seleccionada.

```
C:\PS>UDPPowerCLI.ps1 -Command restore -UDPA-
gentServerName yourUDPAgentServer -UDPAgentUserName
UDPAgentUsername -UDPAgentPasswordFile myUDPA-
gentPasswordFile -UDPAgentProtocol 'https' -UDPA-
gentPort 8018 -UDPAgentDomainName UDPAgentdomainName -
BackupSessionNumber 1 -RestoreFilePath 'C:\1.txt' -Res-
toreDestination 'C:\restore' -Res-
toreDestinationUserName remoteAccessUser -
RestoreDestinationPassword remoteAccessPsw -Crea-
teBaseFolder 'true'
```

Ejemplo 9

Descripción

El comando se conecta con el servidor denominado *yourUDPAgentServer* utilizando el nombre de usuario del entorno, el protocolo HTTP predeterminado y el puerto 8014. A continuación, se conecta con el servidor de UDP usando el puerto predeterminado 8015 y el protocolo HTTP para comprobar que el número de sesión de copia de seguridad sea 1. Por último, restaura el directorio a una ubicación alternativa, con la opción de restauración Overwrite existing file and create root directory (Sobrescribir archivos existentes y crear directorio raíz) seleccionada.

```
C:\PS>UDPPowerCLI.ps1 -Command restore -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
RestoreDirectoryPath 'c:\Test' -BackupSessionNumber 1
-RestoreDestination 'C:\restore' -Res-
toreDestinationUserName remoteAccessUser -Res-
toreDestinationPassword remoteAccessPsw -
UDPConsoleServerName yourUDPServer -vmname sour-
ceVMName -UDPConsolePasswordFile myUDPPasswordFile -
domainname yourUDPDomainName -OverwriteExistFiles
'true' -CreateRootFolder 'true'
```

Ejemplo 10

Descripción

El comando se conecta con el servidor denominado *yourUDPAgentServer* utilizando el nombre de usuario del entorno, el protocolo HTTP predeterminado y el puerto 8014. A continuación, se conecta con el servidor de UDP usando el puerto predeterminado 8015 y el protocolo HTTP para comprobar que el número de sesión de copia de seguridad sea 1. Por último, recupera la máquina virtual a la ubicación original, con la opción de recuperación de máquina virtual Overwrite existing vm and power on vm after recovered (Sobrescribir máquina virtual existente y encender la máquina virtual tras la recuperación) seleccionada.

```
C:\PS>UDPPowerCLI.ps1 -Command RecoverVM -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
BackupSessionNumber 1 -UDPConsoleServerName you-
rUDPServer -recovervmname sourceVMName -UDPCon-
solePasswordFile myUDPPasswordFile -
UDPConsoleDomainName yourUDPDomainName -Ove-
rwriteExistingVM 'true' -PoweronVM 'true'
```

Ejemplo 11

Descripción

El comando envía la tarea de copia de seguridad semanal del Agente de UDP inmediatamente y ejecuta solamente una vez.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPA-
gentServerName myServer -UDPAgentPassword $Se-
curePassword -UDPAgentDomainName myDomainName -
UDPAgentUserName UDPAgentUsername -BackupJobType Incr
-backupScheduleType 'weekly' -jobDescription 'Powe-
rCLIJob'
```

Ejemplo 12

Descripción

El comando envía la tarea de copia de seguridad y establece el tiempo de espera en segundos durante el que se debe esperar a que finalice la tarea.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleServerName myServer -UDPConsolePasswordFile
myUDPPasswordFile -UDPConsoleDomainName myDomainName -
nodeName myNodeName -UDPConsoleUserName myAdmin -Backu-
pJobType Incr -jobDescription 'PowerCLIJob' wai-
tJobFinish 'true' -timeout 600 -jobType 'agentbase'
```

Archivo de configuración y propiedades de PowerCLI

Se pueden personalizar las propiedades y el archivo de configuración de PowerCLI de UDP:

Nombre del archivo de configuración: *PowerCLIConfiguration.properties*

Ubicación de la instalación del archivo de configuración:

- *C:\Archivos de programa\Arcserve\Unified Data Protection\Management\Configuration*
- *C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\Configuration*

Formato del archivo de configuración:

Enable24HoursSetting=yes

LogPath=D:\PowerCLILogPath

RotationSizeInMB=2

RetentionPeriodInDays=5

RetainNoOfFiles=6

Propiedades de configuración:

Nombre de la propiedad	Descripción	Valor predeterminado	Valor aceptado
Enable24HoursSetting	▪ Si el valor se establece en Yes, la marca de tiempo del archivo de registro se escribe en formato de 24 horas. ▪ Si el valor se establece en No, la marca de tiempo del archivo de registro se escribe en formato de 12 horas.	Sí	Yes o No
LogPath	▪ La ubicación de la carpeta de los archivos de registro de PowerCLI. ▪ Si no se proporciona la ubicación, el archivo de registro se escribe en su ubicación predeterminada. ▪ LogPath acepta rutas relativas y absolutas. ▪ Los símbolos excepto \ /: *? < > | son aceptables para el nombre de archivo o carpeta.	-	-
RotationSizeInMB	▪ Si se alcanza el límite especificado en RotationSizeInMB, el archivo de registro de PowerCLI se renombra (se rota) con una marca de fecha y hora.	0	Mínimo = 1 Máximo = 1024
RetentionPeriodInDays	▪ Si los archivos rotados son anteriores al valor proporcionado en RetentinPeriodInDays, se suprimirán los archivos de registro antiguos.	0	Mínimo = 5 Máximo = 365
RetainNoOfFiles	▪ Si hay más archivos de registro rotados que el	0	Mínimo = 5 Máximo =

	valor proporcionado en RetainNoOfFiles, se suprimirán los archivos adicionales.		1000

Notas:

- Si se proporcionan valores para las propiedades de configuración distintos del valor permitido, PowerCLI muestra un error y se detiene la ejecución.
- Si se proporcionan valores predeterminados para las propiedades de configuración, la ejecución de PowerCLI continúa y se ejecuta con el comportamiento predeterminado.

Capítulo 4: Protección del sistema Oracle utilizando Recovery Manager (RMAN)

Recovery Manager (RMAN) es una utilidad de Oracle que realiza tareas de copia de seguridad, tareas de restauración y recuperación en bases de datos y automatiza la administración de estrategias de copia de seguridad. Con esta función, se pueden realizar copias de seguridad, restaurar y recuperar archivos de la base de datos.

Esta sección incluye los siguientes temas:

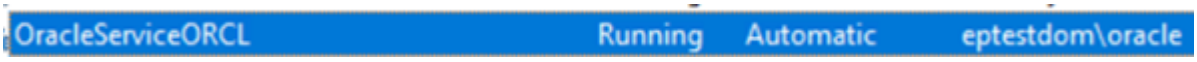
Revisión de los requisitos previos para la base de datos de Oracle con RMAN (Windows y Linux)

Requisitos previos para configurar cuando Oracle está instalado en Windows

Agregar plan

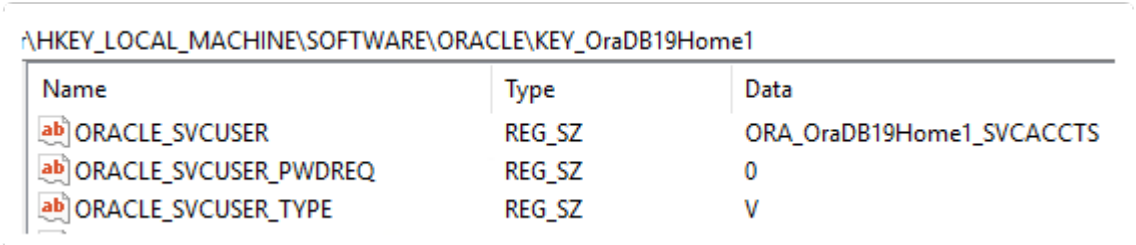
- Los nodos de Windows Oracle, la Consola de UDP y el servidor de puntos de recuperación deben estar en el mismo dominio.
- La Consola de UDP y el servidor de puntos de recuperación deben estar instalados y se deben utilizar con el administrador del dominio (<dominio>\administrador) o cuenta equivalente.
- Cuando inicie sesión en la Consola de UDP, haga lo siguiente:
  1. El usuario "<dominio>\Administrador" se agrega al grupo local ORA_DBA en los nodos de Oracle de Windows.
  2. Agregue el nodo de Oracle a la Consola de UDP mediante el ID de usuario <dominio>\<Usuario del dominio>.

  Nota: Se puede utilizar cualquier usuario en UDP que no sea el administrador, pero se deben proporcionar los permisos adecuados.
- Admite las siguientes cuentas de Oracle utilizadas durante las instalaciones de Oracle (aplicable tanto para Stand-Alone como para RAC).
  - Usuario de dominio: Tome nota del usuario de dominio que posee el servicio de Oracle (cuenta de servicio). Por ejemplo, eptestdom\oracle.

  - Cuenta virtual: Cuando se instala Oracle mediante una cuenta virtual, compruebe los parámetros en el registro del servidor de Oracle antes de agregar la base de datos al plan de UDP.

    Nota: De forma predeterminada, las cuentas virtuales están activadas en Windows.

- Asegúrese de configurar correctamente la escucha, que ayuda a proteger la base de datos de Oracle y que se conecta a sqlplus y RMAN para esa base de datos.

  Ejemplo: "rman target / " debe hacer referencia a la base de datos correcta.

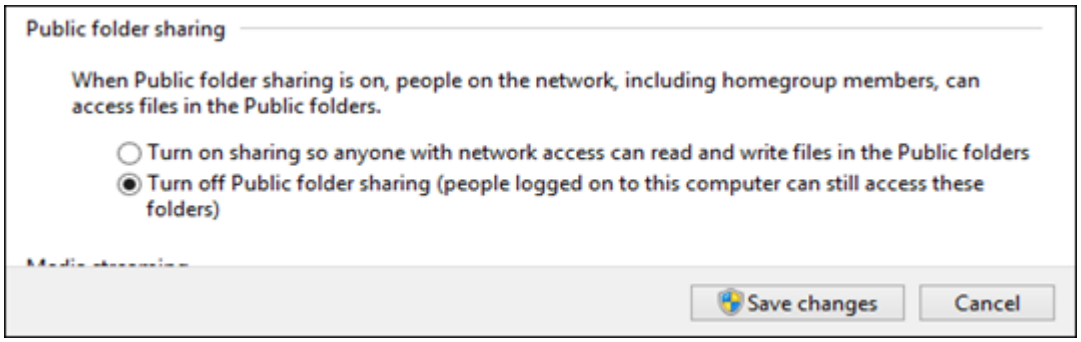
Copia de seguridad

- Cuando realice una copia de seguridad de las bases de datos de Oracle, asegúrese de que estén en estado ABIERTO con el modo ARCHIVELOG activado. Para obtener más información, consulte Cómo activar el modo ARCHIVELOG.
- Para realizar correctamente las copias de seguridad de Oracle RMAN con Arcserve UDP, debe activar la autenticación nativa de Windows. Para confirmar si la autenticación de Windows está activada, asegúrese de agregar la siguiente línea en el archivo sqlnet.ora en la ruta de ORACLE_HOME/network/admin.

  SQLNET.AUTHENTICATION_SERVICES= (NTS)
- El uso compartido de carpetas públicas está desactivado para activar el acceso seguro a las bases de datos.

  Para desactivar el uso de la carpeta pública para el uso compartido de la red, siga estos pasos:

  1. Vaya al Centro de redes y recursos compartidos y, a continuación, haga clic en **Cambiar configuración de uso compartido avanzado**.
  2. En el panel izquierdo, busque la configuración de uso compartido de la carpeta pública para la ubicación de red activa y, a continuación, haga clic en **Desactivar el uso compartido de carpetas públicas (los usuarios que iniciaron sesión en este equipo todavía podrán obtener acceso a esas carpetas)**.
  3. Haga clic en **Guardar cambios**.



Restaurar tablas

Las restauraciones a nivel de tabla y del espacio de tablas utilizan una base de datos auxiliar, que requiere los siguientes permisos:

- **Usuario de dominio para la instalación de Oracle:** Agregue el usuario de Oracle de la cuenta de servicio al grupo Administradores en los nodos de Oracle. Por ejemplo, se agrega eptestdom\oracle al grupo de administradores locales.
- **Cuenta virtual para la instalación de Oracle:** Abra la clave de registro, HKLM\SYSTEM\CurrentControlSet\services\eventlog\Application, y, a continuación, haga clic con el botón secundario del ratón y agregue permisos al grupo como, por ejemplo, ORA_OraDB18Home1_SVCACCTS.

Restaurar en un nodo alternativo

- La misma versión de Oracle con la misma configuración está instalada en el sistema de destino.
- La base de datos está instalada con el mismo SID que el equipo de origen (original).
- La base de datos de Oracle en el nodo de destino debe estar en estado apagado.

Configuración del cortafuegos para permitir el acceso a los nodos de Oracle de Windows

netsh advfirewall firewall add rule name="AS ora" dir=in action=allow program="C:**path\to\oracle\home**\bin\oracle.exe" enable=yes	
netsh advfirewall firewall add rule name="AS tns" dir=in action=allow program="C:**path\to\oracle\home**\tnslsnr.exe" enable=yes	
netsh advfirewall firewall add rule name="AS ora" dir=out action=allow program="C:**path\to\oracle\home**\bin\oracle.exe" enable=yes	
netsh advfirewall firewall add rule name="AS tns" dir=out action=allow program="C:**path\to\oracle\home**\bin\tnslsnr.exe" enable=yes	

netsh advfirewall firewall add rule name-e="ora_1521" dir=in action=allow pro-tocol=TCP localport=**1521**	
netsh advfirewall firewall add rule name-e="ora_1521" dir=out action=allow pro-tocol=TCP localport=**1521**	El número de puerto puede cambiar en función del puerto configurado.

Requisitos previos para configurar cuando Oracle está instalado en Linux

Agregar plan

- El nodo de Oracle /etc/hosts debe tener una entrada para FQDN y “resol-v.conf” con la entrada de DNS adecuada.
- Todas las bases de datos que se deben proteger deben tener una entrada en el archivo /etc/oratab.

  Nota: En el entorno RAC, asegúrese de que el contenido se actualice para ambos nodos.

  La sintaxis en el archivo /etc/oratab es la siguiente:

  <NOMBRE_EXCLUSIVO_BD>:<DIRECTORIO_PRINCIPAL_ ORACLE>:<ACTIVO/INACTIVO>

  Ejemplo: ORCL:/u01/app/oracle/ORCL/:Y

Copia de seguridad

- Cuando realice una copia de seguridad de las bases de datos de Oracle, asegúrese de que estén en estado ABIERTO con el modo ARCHIVELOG activado. Para obtener más información, consulte Cómo activar el modo ARCHIVELOG.
- Instale smbclient utilizando el siguiente comando:

  #yum install smbclient
- Asegúrese de configurar correctamente la escucha, que ayuda a proteger la base de datos de Oracle y que se conecta a sqlplus y RMAN para esa base de datos.

  Ejemplo: Compruebe «lsnrctl status» para las bases de datos disponibles para una escucha en particular.

  El comando "rman target /" debe estar conectado a la base de datos correcta especificada para la copia de seguridad.

Tareas de recuperación asegurada

- Asegúrese de que las bases de datos de Oracle para la copia de seguridad estén en estado MONTAJE o ABIERTO.

Autenticación basada en claves públicas y privadas

Nota: Se ha implementado la autenticación basada en claves públicas y privadas para la ejecución de scripts de RMAN de Linux. Esto evita las contraseñas de texto sin formato mientras se ejecutan scripts remotos en el servidor de Oracle de Linux desde el servidor de puntos de recuperación (RPS).

1. En el nodo del servidor de puntos de recuperación, haga lo siguiente:
   a. Compruebe que el instalador haya creado el directorio *PrivateKey* en la siguiente ruta:

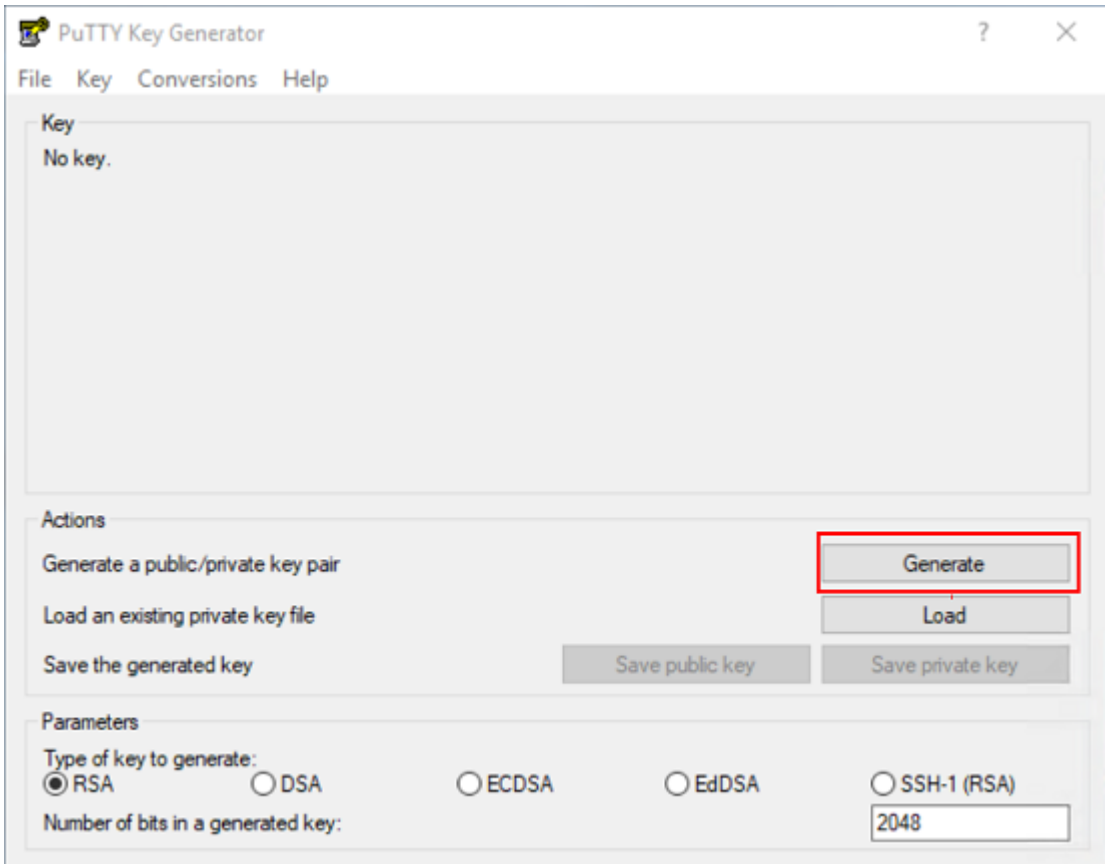
      *Install Path**Arcserve**Unified Data Protection**Engine**BIN**OracleRMAN**PrivateKey*

   b. Instale PuTTY (versión 0.73 o posterior) y, a continuación, para abrir PuTTY Key Generator, realice una de las siguientes acciones:
      - En cmd.exe, ejecute el comando *puttygen*.
      - Vaya a **Todos los programas** > **PuTTY** > **PuTTYgen**.

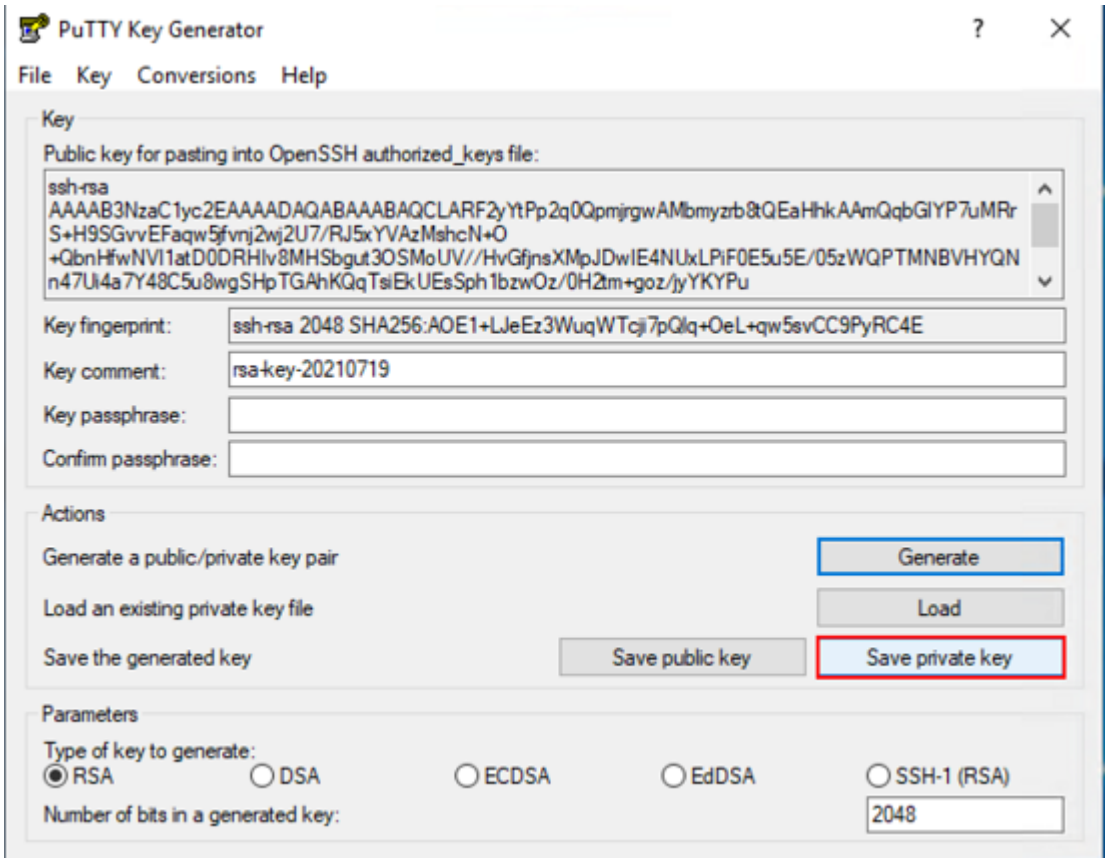
      Aparecerá el cuadro de diálogo PuTTY Key Generator.

   c. En la pantalla PuTTY Key Generator, haga clic en **Generar**.

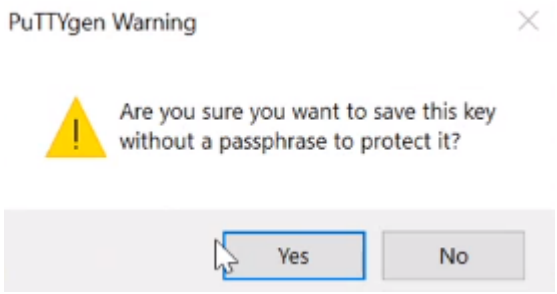
      Se generan las claves públicas y privadas.



d. Haga clic en **Save private key**.



e. En el cuadro de diálogo de advertencia de PuTTYgen, haga clic en **Yes** para guardar la clave privada sin una frase de contraseña.



f. Mientras se guarda la clave privada, vaya a la siguiente ruta, escriba el nombre del archivo y, a continuación, haga clic en **Save**:

Install Path\Arcserve\Unified Data Protection\Engine\BIN\OracleRMAN\PrivateKey

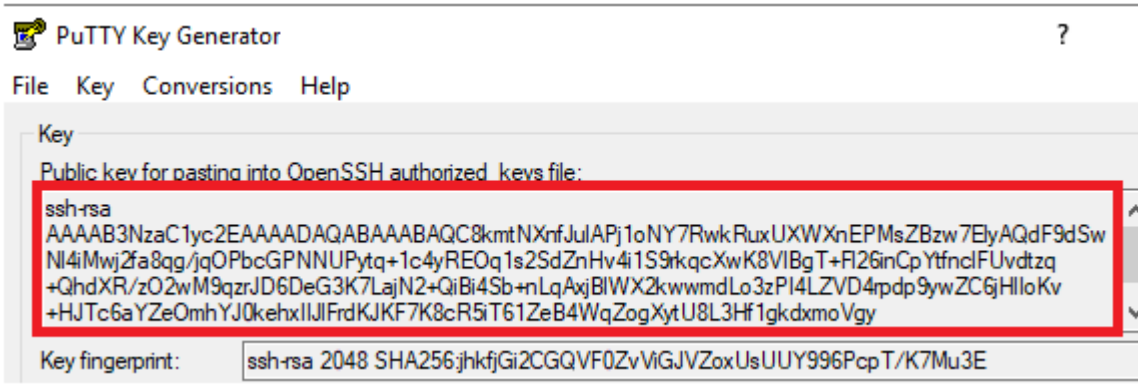
Notas:

- El nombre del archivo debe tener el formato PrivateKeyFile.ppk. Se puede dar cualquier nombre.
- Guarde la clave privada con la extensión .ppk en la siguiente ruta:

Engine\Bin\OracleRMAN\PrivateKey

- Copie la clave pública manualmente desde el cuadro de diálogo PuTTY Key Generator y guárdela en formato de texto en la siguiente carpeta para futuras referencias en caso de que sea necesario agregarla a otros servidores Oracle de Linux:

  Engine\Bin\OracleRMAN\PrivateKey



g. Abra la ruta *Engine\Bin directory* en cmd.exe.

h. Ejecute el siguiente comando para cifrar la clave privada mediante la utilidad de línea de comandos RMANCryptUtil.exe:

   RMANCryptUtil.exe "C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN\<Nombre de la clave privada generada>.ppk"

   El archivo de la clave privada cifrado se genera con la extensión **.enc** en la ubicación siguiente:

   Engine\Bin\OracleRMAN\PrivateKey

   Un ejemplo del nombre de archivo: PrivateKey.ppk.enc

   La clave privada cifrada (.enc), que se genera mediante RMANCryptutil, se guarda en la carpeta PrivateKey.

i. Copie la clave **.enc** en otros nodos del servidor de puntos de recuperación y Consolas de UDP.

j. En el nodo de la Consola de UDP, cree la carpeta PrivateKey como se indica a continuación y, a continuación, copie la clave .enc en la carpeta PrivateKey:

   UDP\Engine\Bin\OracleRMAN\PrivateKey

k. Copie la clave pública de la interfaz de usuario de PuTTYgen y consulte el paso 2 para agregar la clave pública en el nodo de Oracle de Linux según corresponda.

2. En el nodo de Linux en el que está instalado Oracle, realice las siguientes operaciones:

   a. Asegúrese de que la carpeta *.ssh* esté disponible en el directorio raíz (~). Si el directorio *.ssh* no está disponible, cree el directorio utilizando el siguiente comando y los permisos predeterminados:

      mkdir ~.ssh

   b. Compruebe si el servicio *sshd* se está ejecutando en el servidor de Linux mediante el siguiente comando:

      service sshd status

      Nota: Si *sshd* no está instalado, instale *sshd* en función del tipo de sistema operativo Linux.

   c. Abra o edite el archivo *authorized_keys* mediante el siguiente comando:

      vim authorized_keys

   d. Cree o modifique el archivo *.ssh/authorized_keys*.

   e. Agregue la clave pública generada en el servidor de puntos de recuperación al archivo *.ssh/authorized_keys* mediante PuTTY Key Generator.

   f. Establezca los permisos mínimos necesarios para el archivo *.ssh/authorized_keys* mediante el siguiente comando:

      chmod 400 .ssh/authorized_keys

   Notas:

   - Para agregar una clave pública en cualquier otro nodo de Oracle de Linux siempre que el servidor de puntos de recuperación siga siendo el mismo, siga solamente el paso 2 mencionado anteriormente.
   - Al cambiar el nodo del servidor de puntos de recuperación, siga los pasos 1 y 2 mencionados anteriormente.

Cómo crear un plan de copia de seguridad para la base de datos de Oracle (Windows y Linux)

Para proteger los nodos o los nodos agrupados en clúster de Windows y Linux, se debe crear un plan. El plan consiste en una tarea de copia de seguridad. Esta tarea de copia de seguridad le permite especificar los nodos que se desean proteger, el destino de la copia de seguridad y la programación de la copia de seguridad. El destino de la copia de seguridad es un servidor de punto de recuperación donde se desea almacenar sus datos de copia de seguridad. El destino también puede ser un destino local o una carpeta de recurso compartido remota.

Esta sección incluye los siguientes temas:

Creación de un plan de copia de seguridad con una tarea de copia de seguridad

Un plan de copia de seguridad incluye una tarea de copia de seguridad que realiza una copia de seguridad de un nodo y almacena los datos en un destino especificado. Cada tarea está formada por parámetros que definen el origen, destino, programación y otros detalles de la copia de seguridad. Esta sección proporciona información sobre cómo crear un plan de copia de seguridad para la base de datos de Oracle.

Siga estos pasos:

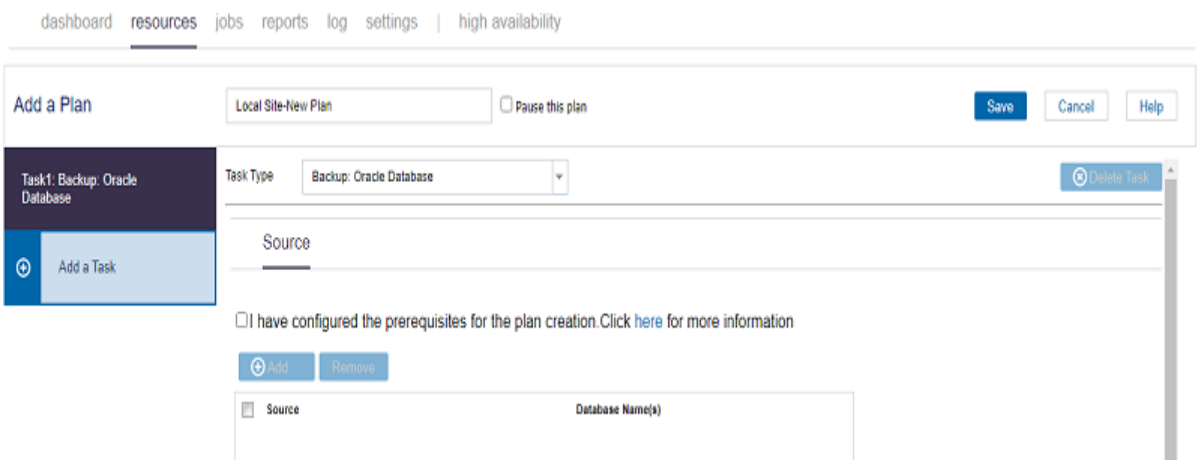
1. Inicie sesión en la Consola de Arcserve UDP.
2. Vaya a **recursos** > **Plan** > **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre la página Agregar un plan.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.
6. En la lista desplegable Tipo de tarea seleccione **Copia de Seguridad: Base de datos de Oracle**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Notas:

- Para comprobar la corrupción de bloques físicos y lógicos en los archivos de datos existentes en el equipo de origen de Oracle, se utiliza el comando Backup Validate RMAN.
- Para agregar la validación a la tarea de copia de seguridad, utilice la siguiente clave de registro:

  \HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\SourceDBValidation

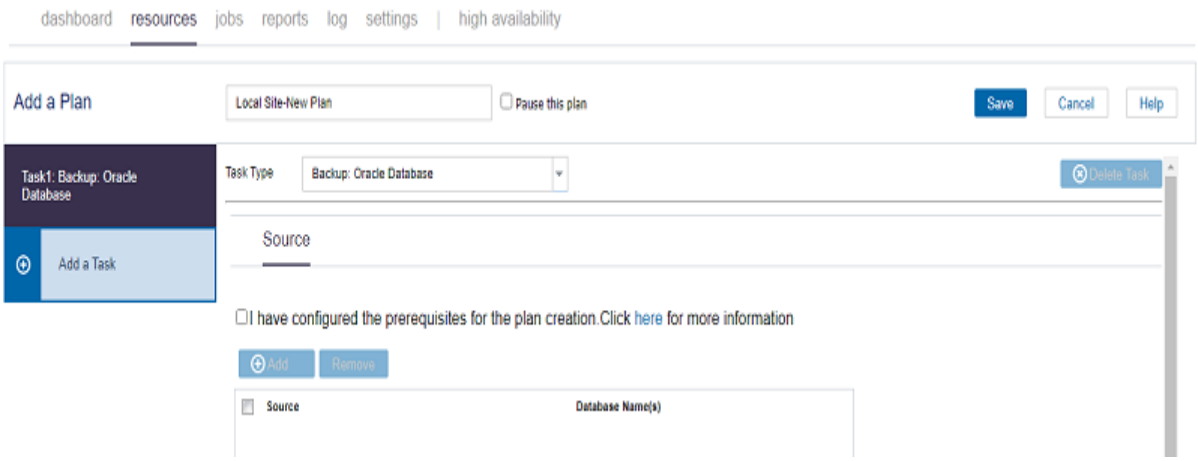
  - Si no se agrega la clave (valor predeterminado): la validación de la copia de seguridad no está activada
  - Si la clave se agrega como 1, la validación de la copia de seguridad está activada
  - Si la clave se agrega con cualquier otro valor: la validación de la copia de seguridad no está activada
- La validación de la copia de seguridad es una tarea que requiere mucho tiempo. La activación de esta configuración aumenta el tiempo de copia de seguridad en función del tamaño de los archivos de datos. La validación se ejecuta en todo el archivo de datos de origen incluso para una copia de seguridad incremental.

Especificación del origen

La página Origen le permite especificar los nodos de origen que se desean proteger. Se pueden seleccionar más de un nodo del plan. Si no se ha agregado ningún nodo a la consola, se podrán agregar nodos al crear o modificar un plan en la página Origen. Se puede guardar un plan sin agregar ningún nodo de origen. El plan se implementa solamente después de agregar nodos de origen.

Siga estos pasos:

1. En la ficha Origen, para confirmar las configuraciones de los requisitos previos, seleccione la casilla de verificación **Se han configurado los requisitos previos para crear este plan**. Para obtener más información, consulte Revisión de los requisitos previos de la base de datos de Oracle para RMAN (Windows y Linux).



2. Haga clic en **+ Agregar**.
3. Seleccione una de las opciones siguientes:

Selección de orígenes para proteger en Arcserve UDP

Se abre el cuadro de diálogo Seleccionar nodos para proteger. Seleccione los nodos de la lista que se muestra. Seleccione esta opción si ya se han agregado los nodos a la consola.

Agregar nodo de Windows

Se abrirá el cuadro de diálogo Agregar nodo de Windows. Seleccione esta opción si no se han agregado los nodos y desea agregarlos manualmente para la protección.

Agregar nodo de Linux

Se abre el cuadro de diálogo Agregar nodo de Linux. Seleccione esta opción si no se han agregado los nodos y desea agregarlos manualmente para la protección.

4. Si se selecciona la opción **Seleccionar orígenes para proteger en Arcserve UDP**, en el cuadro de diálogo Seleccionar nodos para proteger, haga lo siguiente:

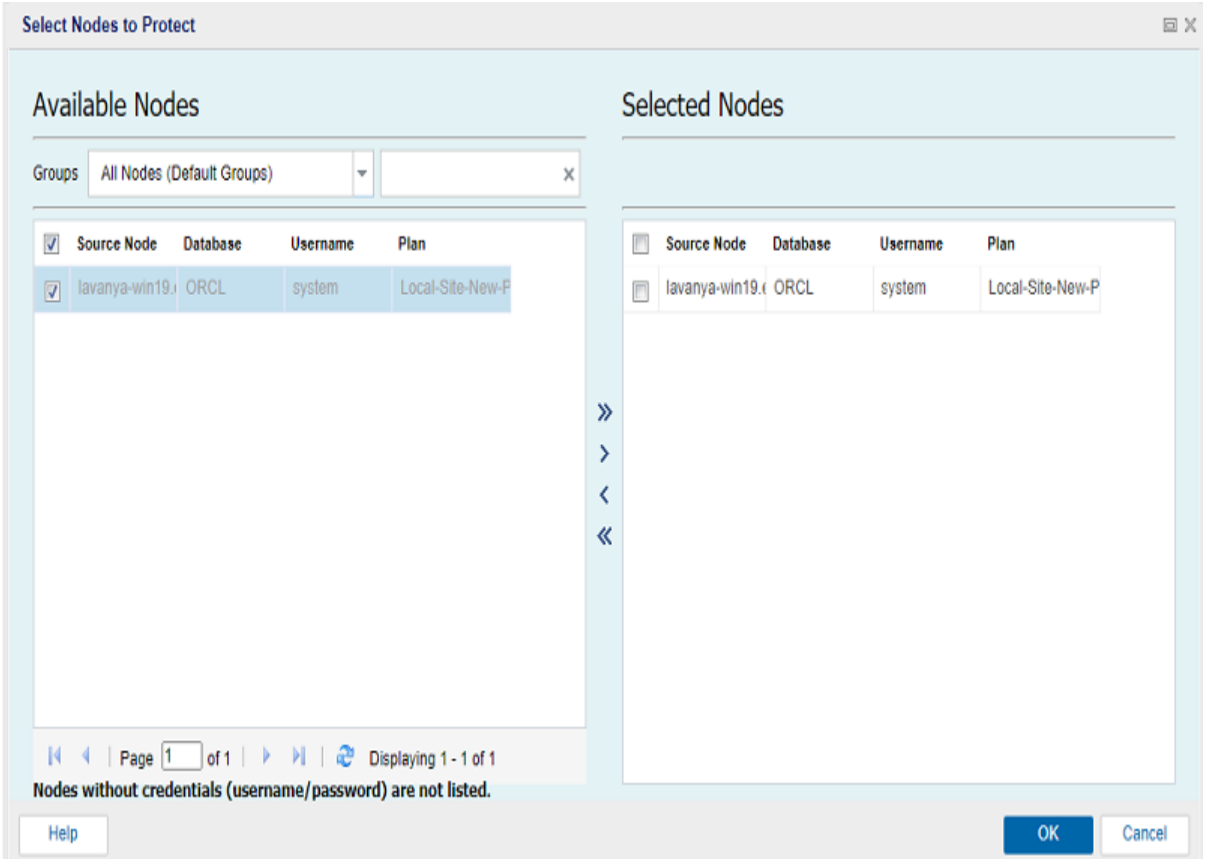
   a. (Opcional) Seleccione un filtro en la lista desplegable Grupos para filtrar nodos. Se pueden especificar palabras clave para filtrar más detalladamente los nodos.

      Los nodos se muestran en la columna Nodos disponibles.

   b. Seleccione los nodos en la columna Nodos disponibles y, a continuación, haga clic en la flecha simple hacia la derecha (>) o en la flecha doble hacia la derecha (>>) para mover los nodos seleccionados o todos los nodos respectivamente a la columna Nodos seleccionados.

      Los nodos se muestran en la columna Nodos seleccionados.

   c. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.



5. Si se selecciona la opción **Agregar nodo de Windows**, haga lo siguiente en el cuadro de diálogo Agregar nodo de Windows de Oracle:

a. Introduzca el nombre de nodo o la dirección IP del nodo de Oracle que se desea agregar.

b. Especifique una descripción para el nodo.

c. Introduzca las credenciales de administrador.

d. Haga clic en **Agregar**.

   Espere hasta que finalice la validación del nombre de usuario y la contraseña.

   El nodo se agrega al panel central.

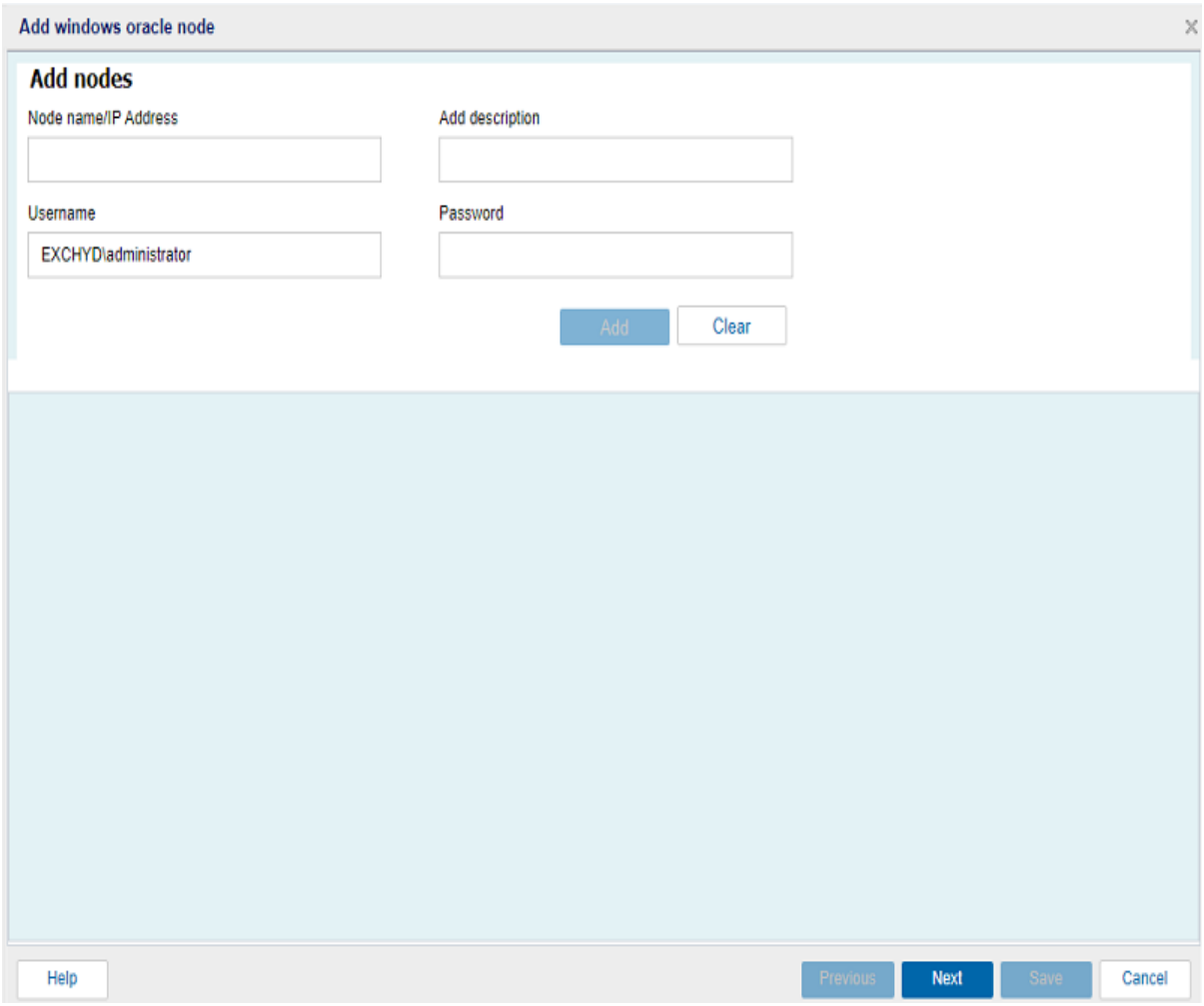
e. Para agregar varios nodos, siga los pasos otra vez. Todos los nodos agregados se muestran en el panel central.

f. Haga clic en el símbolo de expansión situado junto a la dirección IP y, a continuación, verifique los detalles que se agregan.

   Notas:

   - Para editar los nodos agregados de la lista, seleccione el nodo que desea editar y, a continuación, haga clic en **Editar**.
   - Para eliminar los nodos agregados de la lista, seleccione los nodos que desea eliminar y, a continuación, haga clic en **Eliminar**.
   - Para eliminar todos los nodos agregados, haga clic en **Eliminar todo**.

g. Haga clic en **Siguiente**.



6. Si se selecciona la opción **Agregar nodo de Linux**, haga lo siguiente en el cuadro de diálogo Agregar nodo de Linux de Oracle:
    a. Introduzca el nombre de nodo o la dirección IP del nodo de Oracle que se desea agregar.
    b. Especifique una descripción para el nodo.
    c. Especifique el nombre de usuario.
    d. Para el propietario de Oracle, especifique el nombre de usuario que se utiliza para la instalación de Oracle.
    e. Para el puerto SSH, especifique el valor del puerto. El valor predeterminado del puerto es 22.
    f. Haga clic en **Agregar**.

       Espere hasta que finalice la validación del nombre de usuario y la contraseña.

       El nodo se agrega al panel central.

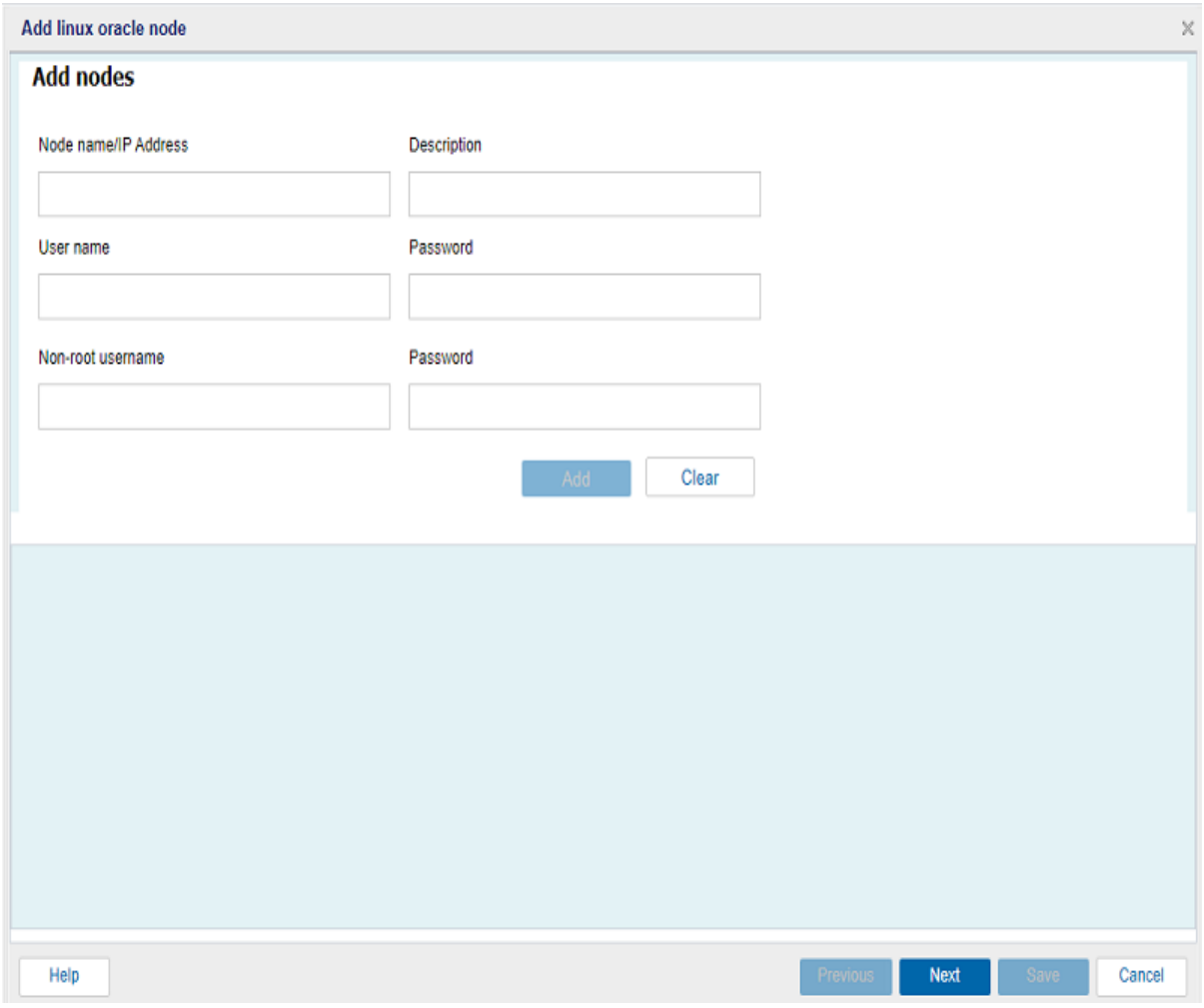
g. Para agregar varios nodos, siga los pasos otra vez. Todos los nodos agregados se muestran en el panel central.

h. Haga clic en el símbolo de expansión situado junto a la dirección IP y, a continuación, verifique los detalles que se agregan.

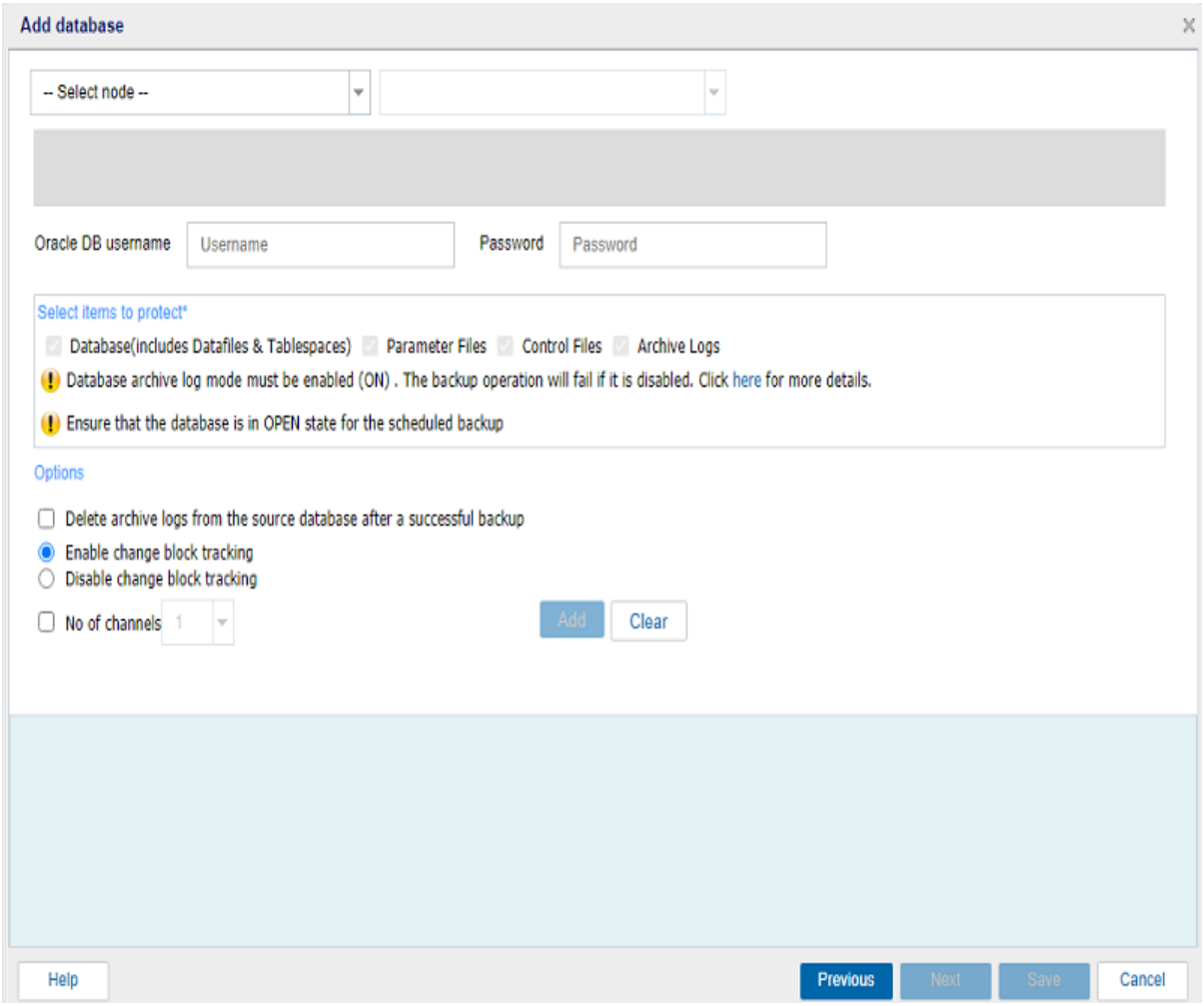
Notas:

- Para editar los nodos agregados de la lista, seleccione el nodo que desea editar y, a continuación, haga clic en **Editar**.
- Para eliminar los nodos agregados de la lista, seleccione los nodos que desea eliminar y, a continuación, haga clic en **Eliminar**.
- Para eliminar todos los nodos agregados, haga clic en **Eliminar todo**.

i. Haga clic en **Siguiente**.



7. En el cuadro de diálogo Agregar base de datos, haga lo siguiente:



a. Seleccione el nodo en la lista desplegable.

   Espere hasta que aparezca la lista de bases de datos disponibles en el host seleccionado y se active la lista desplegable.

b. En la lista desplegable, realice una de las siguientes opciones:

   Agregar nueva base de datos

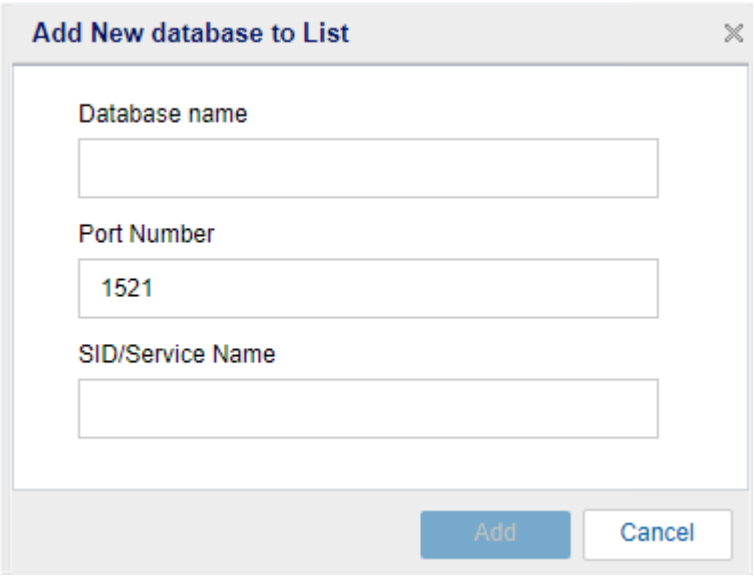
   Para agregar una nueva base de datos, siga estos pasos:

   1. Seleccione la opción **Agregar nueva base de datos**.
   2. En el cuadro de diálogo Agregar nueva base de datos a la lista, haga lo siguiente y, a continuación, haga clic en **Agregar**:

      - **Nombre de base de datos o SID:** Especifique el nombre de la base de datos o el nombre de SID.
      - **Número de puerto:** Introduzca el número de puerto. El valor pre-

determinado del puerto es 1521.

- **Nombre del servicio:** Introduzca el nombre del servicio.



La nueva base de datos se agrega en la lista desplegable.

Seleccionar la base de datos existente

Seleccione la base de datos de la lista desplegable según sea necesario. Después de seleccionar la base de datos, se mueve fuera de la lista y aparece en el panel central.

Notas:

- Para evitar varias entradas para cada base de datos, agrupe las bases de datos que haya configurado con el mismo nombre de usuario y contraseña.
- Para agregar diferentes tipos de archivos a las bases de datos que tienen diferentes credenciales, seleccione las bases de datos individuales y, a continuación, agréguelos.
- Para eliminar la base de datos del grupo (en el panel central), haga lo siguiente:

  a. Haga clic en el nombre de la base de datos.

     Aparecerá un mensaje de confirmación.

  b. Haga clic en **Sí** para confirmar.

  Se elimina la base de datos correctamente y se vuelve a agregar a la lista desplegable.

c. Introduzca las credenciales de usuario del sistema para la base de datos de Oracle.

Notas:

- Todos los elementos que se van a proteger, como la base de datos (incluidos los archivos de datos y los espacios de tabla), los archivos de control, los archivos de parámetros y los registros del archivo de archivado están activados de forma predeterminada.
- Asegúrese de activar la base de datos ARCHIVELOG antes de que se active la operación de copia de seguridad. Para verificar si el modo de registro ARCHIVELOG está activado, consulte Revisión de los requisitos previos para la base de datos de Oracle. Si no se activa ARCHIVELOG, se producirá un error en la tarea de copia de seguridad.

d. Para Opciones, especifique lo siguiente:

Suprimir registros del archivo de archivado de la base de datos de origen después de una copia de seguridad correcta

Permite suprimir los registros del archivo de archivado de la base de datos de origen después de una copia de seguridad correcta

Número de canales

Le permite seleccionar el número de canales o subprocesos que se desean crear para la tarea de copia de seguridad.

Nota: El número máximo de canales admitidos es 10.

Activar seguimiento del bloque de cambios

Permite activar la función de seguimiento del bloque de cambios. Utilice esta opción para mejorar el rendimiento de RMAN. Ayuda a la utilidad RMAN o al binario a encontrar los datos diferenciales más rápidamente y a realizar la tarea de copia de seguridad.

Desactivar seguimiento del bloque de cambios

Permite desactivar la función de seguimiento del bloque de cambios.

Nota: Oracle solo admite la función Desactivar seguimiento del bloque de cambios para Enterprise Edition (EE).

e. Haga clic en **Agregar**.

Se enumeran todas las bases de datos agregadas.

Nota: Después de hacer clic en el botón Agregar, se verifican todas las credenciales de la base de datos y los parámetros del cortafuegos.

f. Para agregar varias bases de datos, siga los pasos otra vez. Se enumeran todas las bases de datos agregadas.

g. Haga clic en el símbolo de expansión situado junto a la dirección IP y, a continuación, verifique los detalles que se agregan.

Notas:

- Para editar las bases de datos agregadas de la lista, seleccione la base de datos que desea editar y haga clic en **Editar**.
- Para eliminar las bases de datos agregadas de la lista, seleccione las bases de datos que desea eliminar y haga clic en **Eliminar**.

8. Haga clic en **Guardar**.

Notas:

- Se pueden agregar varios nodos y varias bases de datos.
- Para eliminar el origen, seleccione la casilla de verificación situada junto al origen agregado y, a continuación, haga clic en **Eliminar**.

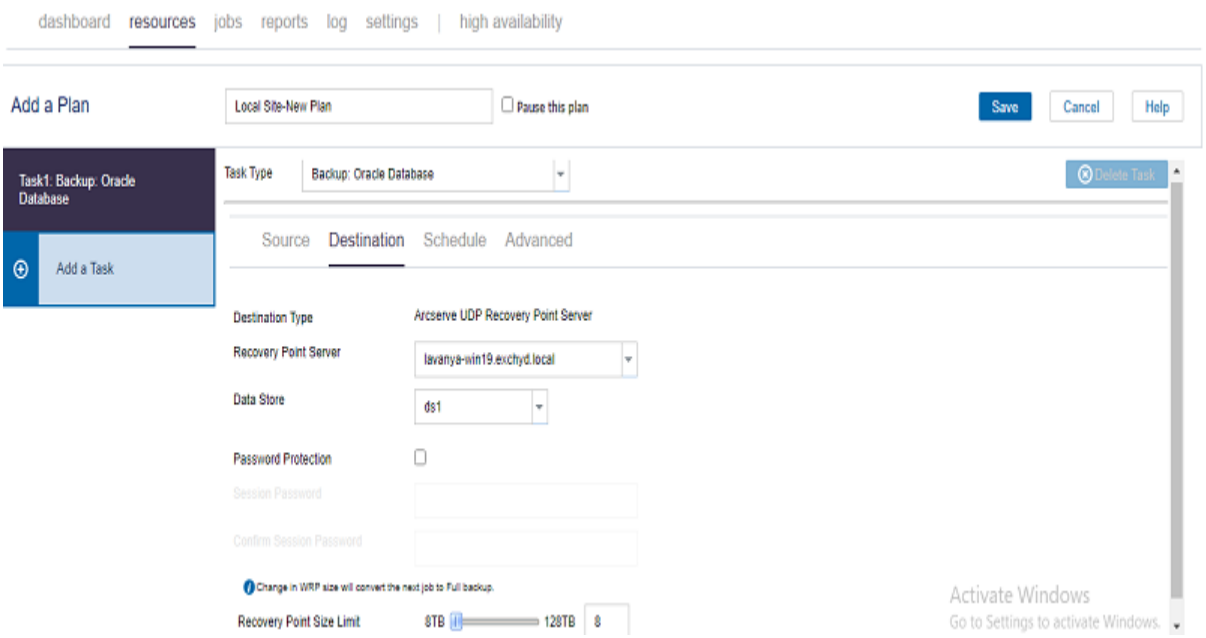
Se especifica el origen.

Especificación del destino

El destino es una ubicación donde se almacenan los datos de la copia de seguridad. Se debe especificar como mínimo el destino para guardar el plan.

Siga estos pasos:

1. Haga clic en la ficha **Destino**.



2. Realice los pasos siguientes:

   - **Servidor de puntos de recuperación**: En la lista desplegable, seleccione el servidor de puntos de recuperación (RPS).
   - **Almacén de datos**: En la lista desplegable, seleccione el almacén de datos de destino.
   - **Protección con contraseña**: Seleccione la casilla de verificación **Protección con contraseña**, proporcione la contraseña de sesión y, a continuación, vuelva a especificarla para confirmarla.

     Nota: La contraseña de la sesión es opcional cuando el destino de copia de seguridad es un almacén de datos del servidor de puntos de recuperación no cifrado.
   - **Límite del tamaño del punto de recuperación**: Especifica el tamaño del servidor de puntos de recuperación para la copia de seguridad. Establezca el tamaño del servidor de puntos de recuperación en la escala.

Intervalo: De 8 TB a 128 TB

Se especifica el destino.

Especificación de la programación

La página Programación le permite definir una programación para las funciones Copia de seguridad, Combinación y Regulador para que se repitan a intervalos específicos. Después de definir una programación, las tareas se ejecutan automáticamente según la programación. Se pueden agregar varias programaciones y se pueden proporcionar valores de configuración de retención.

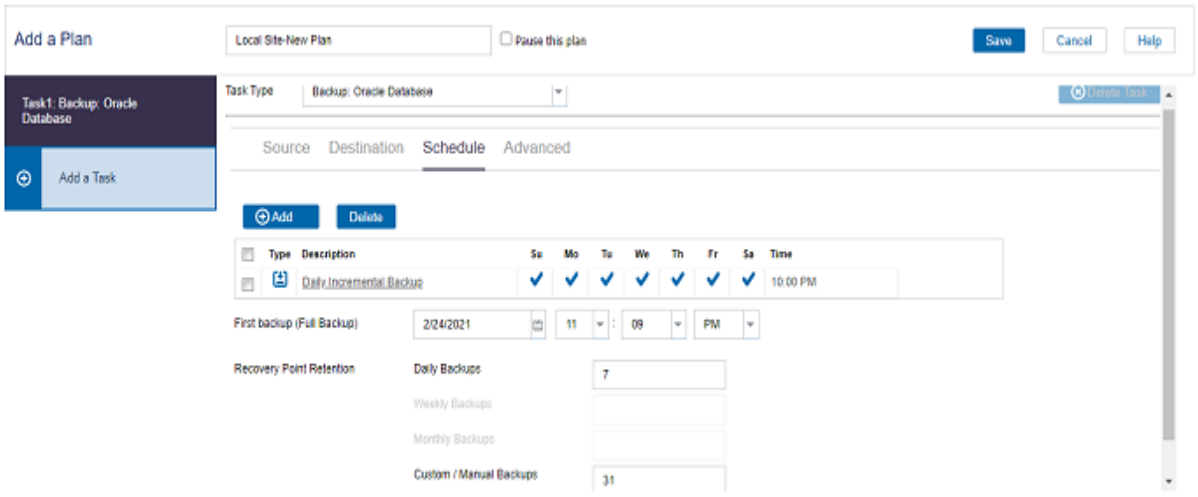
Una Programación de copia de seguridad hace referencia a una programación regular que se repite varias veces al día basándose en el número de horas o minutos que se seleccionan. Además de la programación regular, una programación de copia de seguridad también proporciona opciones para agregar programaciones diarias, semanales y mensuales.

Si el destino de la copia de seguridad es un servidor de puntos de recuperación, el valor predeterminado es una copia de seguridad incremental: Todos los tipos de archivo diaria a las 22:00 horas.

Se puede editar o suprimir una programación de la tarea de copia de seguridad.

Siga estos pasos:

1. Haga clic en la ficha **Programación** y, a continuación, agregue programaciones de la copia de seguridad, de la combinación y del regulador de la lectura del disco.

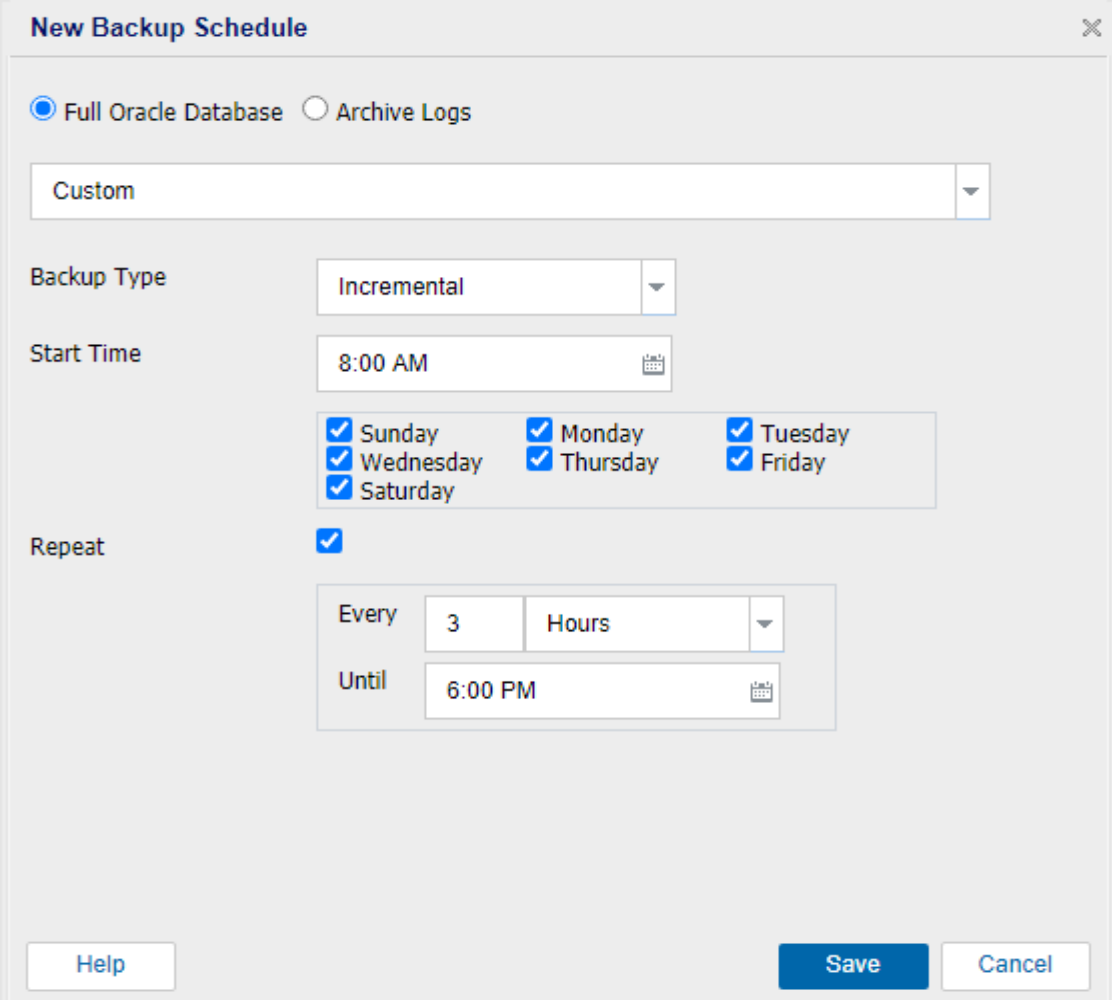


2. Para agregar una programación de la copia de seguridad, realice los pasos siguientes:

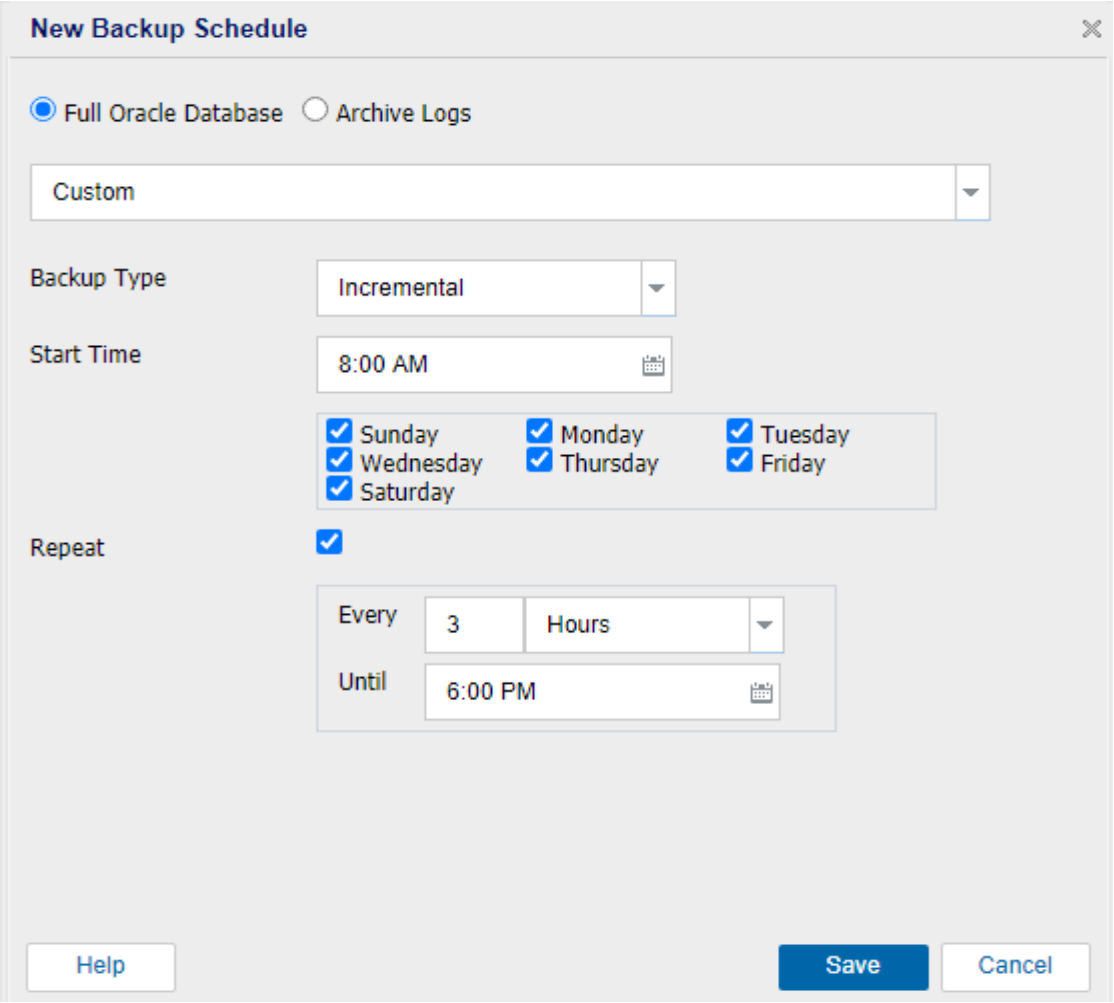
   a. Haga clic en **Agregar** y, a continuación, seleccione la opción **Agregar programación de copia de seguridad**.

      Se abrirá el cuadro de diálogo Nueva programación de la copia de seguridad.

b. En el cuadro de diálogo Nueva programación de la copia de seguridad, seleccione una de las siguientes opciones:



Base de datos de Oracle completa



Realice los pasos siguientes:

a. En la lista desplegable, seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

Cada hora

Especifica la programación de la copia de seguridad que ocurre cada hora.

Minuto

Especifica la programación de la copia de seguridad que se produce en un tiempo mínimo de 15 minutos.

b. En la lista desplegable Tipo de copia de seguridad, seleccione el tipo de copia de seguridad.

Completa

Determina la programación de la copia de seguridad para las copias de seguridad completas (todos los tipos de archivo). Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los tipos de archivo del equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales.

Según lo programado, Arcserve UDP realiza una copia de seguridad incremental de todos los tipos de archivo desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

Nota: Siempre se realiza una copia de seguridad completa del archivo de control para cualquier tipo de copia de seguridad.

c. Especifique la hora de inicio de la copia de seguridad.

d. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

Nota: Asegúrese de que el tiempo para repetir el programa no sea inferior a 15 minutos.

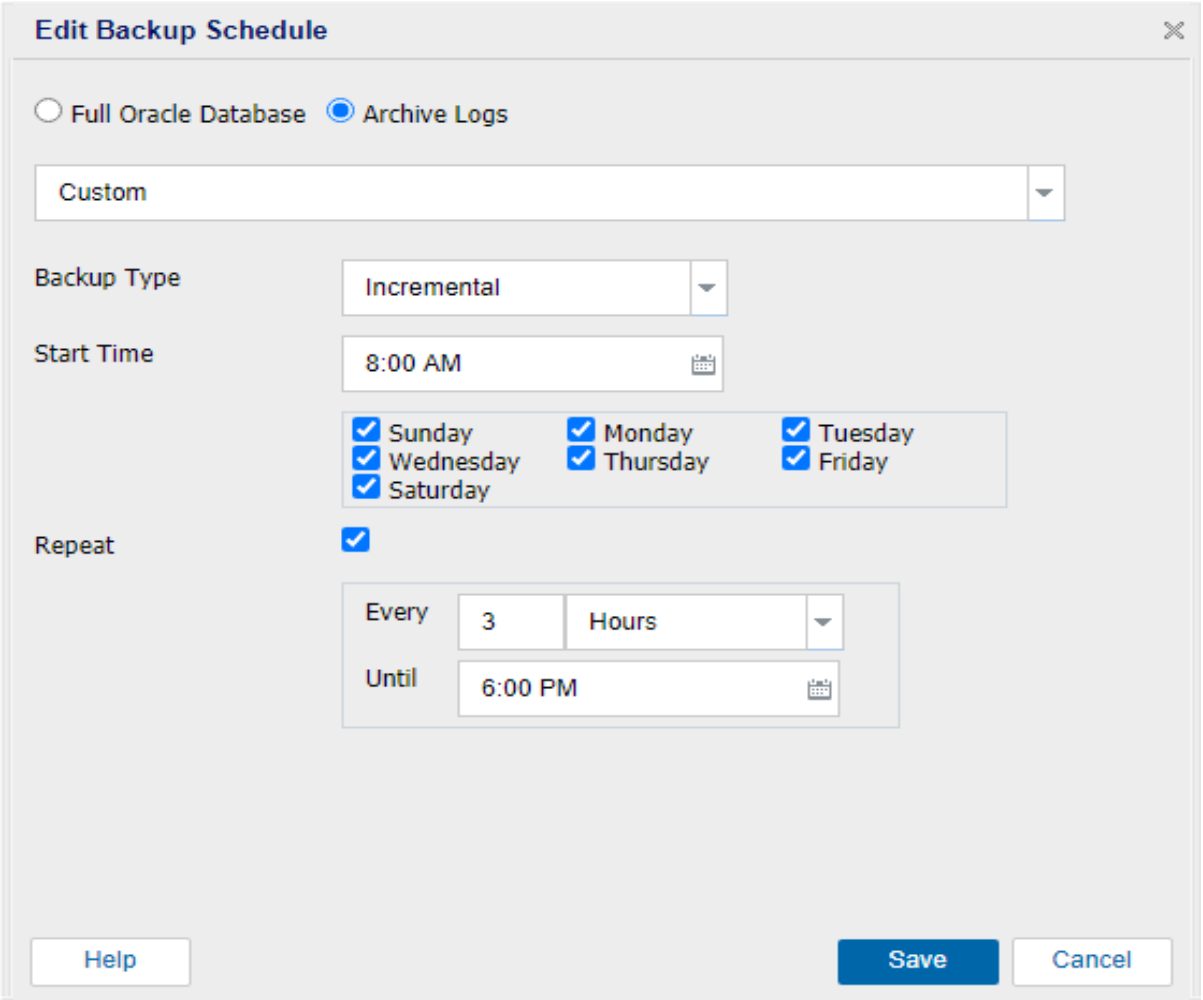
e. Si ha seleccionado la opción **Cada hora** en la lista desplegable, haga lo siguiente:

   1. Seleccione el tipo de copia de seguridad en la lista desplegable Tipo de copia de seguridad.
   2. Especifique la hora de inicio de la copia de seguridad.
   3. Especifique la hora de finalización de la copia de seguridad.
   4. Seleccione la hora de repetición de la copia de seguridad en la lista desplegable.

      Nota: Si desea personalizar el tiempo de repetición de la copia de seguridad, seleccione Personalizado en la lista desplegable y, a continuación, introduzca el tiempo en horas.

f. Haga clic en **Guardar**.

Registros archivados



Realice los pasos siguientes:

a. En la lista desplegable, seleccione una de las opciones siguientes:

Personalizada

Especifica la programación de la copia de seguridad que se repite varias veces al día.

Diario

Especifica la programación de la copia de seguridad que ocurre una vez al día. De forma predeterminada, todos los días de la semana se seleccionan para la copia de seguridad diaria. Si no se desea ejecutar la tarea de copia de seguridad en un día específico, elimine la selección de la casilla de verificación para el día de la semana en particular.

Cada semana

Especifica la programación de la copia de seguridad que ocurre una vez a la semana.

Cada mes

Especifica la programación de la copia de seguridad que ocurre una vez al mes.

Cada hora

Especifica la programación de la copia de seguridad que ocurre cada hora.

Minuto

Especifica la programación de la copia de seguridad que se produce en un tiempo mínimo de 15 minutos.

b. En la lista desplegable Tipo de copia de seguridad, seleccione el tipo de copia de seguridad.

Completa

Especifica la programación de la copia de seguridad para las copias de seguridad completas del registro del archivo de archivado. Tal y como se ha programado, Arcserve UDP realiza una copia de seguridad completa de todos los registros del archivo de archivado del equipo de origen. Una copia de seguridad completa normalmente consume tiempo en función del tamaño de la copia de seguridad.

Incremental

Especifica la programación de la copia de seguridad para las copias de seguridad incrementales del registro del archivo de archivado.

Tal y como se ha programado, Arcserve UDP solo realiza una copia de seguridad incremental de los registros del archivo de archivado que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Esta es la manera más óptima de realizar una copia de seguridad.

c. Especifique la hora de inicio de la copia de seguridad.

d. (Opcional) Seleccione la casilla de verificación **Repetición** y especifique la programación de repetición.

Nota: Asegúrese de que el tiempo para repetir el programa no sea inferior a 15 minutos.

e. Si ha seleccionado la opción **Cada hora** en la lista desplegable, haga lo siguiente:

1. Seleccione el tipo de copia de seguridad en la lista desplegable Tipo de copia de seguridad.
2. Especifique la hora de inicio de la copia de seguridad.
3. Especifique la hora de finalización de la copia de seguridad.
4. Seleccione la hora de repetición de la copia de seguridad en la lista desplegable.

Nota: Si desea personalizar el tiempo de repetición de la copia de seguridad, seleccione **Personalizado** en la lista desplegable y, a continuación, introduzca el tiempo en horas.

f. Haga clic en **Guardar**.

La Programación de la copia de seguridad se especifica y se muestra en la página Programación.

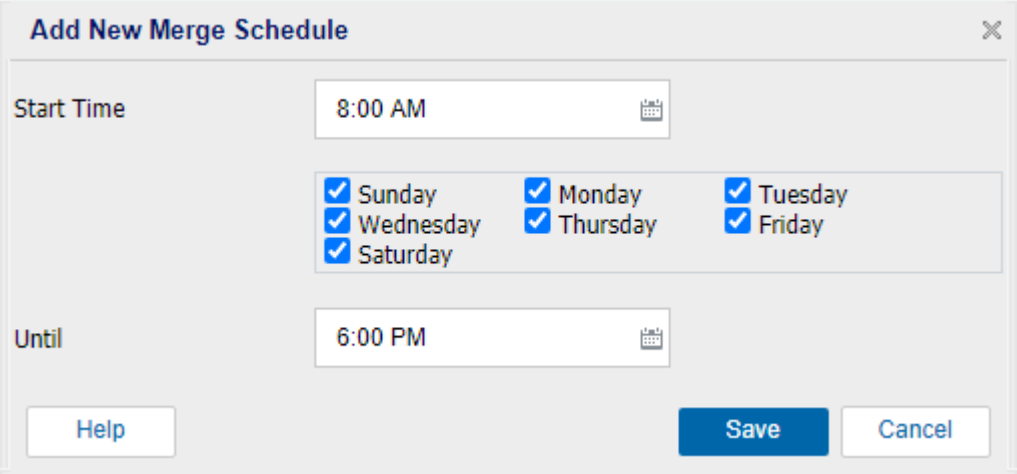
3. Para agregar una programación de la combinación, haga lo siguiente:

a. Haga clic en **Agregar** y, a continuación, seleccione la opción **Agregar programación de la combinación**.

Se abrirá el cuadro de diálogo Agregar nueva programación de la combinación.

b. En el cuadro de diálogo Agregar nueva programación de la combinación, haga lo siguiente:

- **Hora de inicio:** Especifique la hora de inicio para iniciar la tarea de combinación.
- **Hasta:** Especifique la hora de finalización de la tarea de combinación.



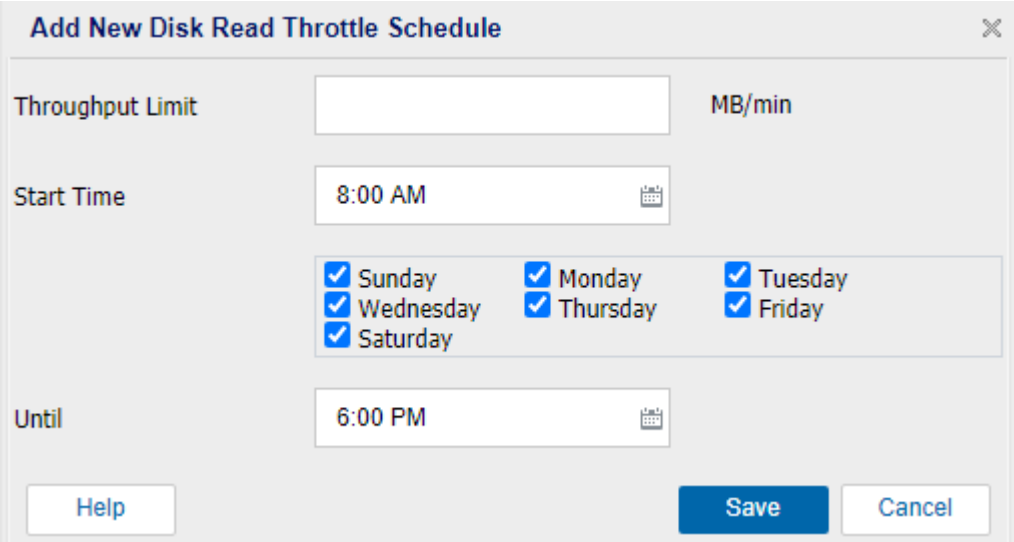
c. Haga clic en **Guardar**.

La programación de la combinación se especifica y se muestra en la página Programación.

4. Para agregar una programación del regulador de la lectura de disco, haga lo siguiente:
   a. Haga clic en **Agregar** y seleccione la opción **Agregar programación del regulador de la lectura de disco**.

      Se abre el cuadro de diálogo Agregar nueva programación del regulador de la lectura de disco.

   b. En el cuadro de diálogo Agregar nueva programación del regulador de la lectura de disco, haga lo siguiente:
      - **Límite de rendimiento:** Especifique el límite de rendimiento en MB por minuto.
      - **Hora de inicio:** Especifique la hora de inicio para iniciar la tarea de rendimiento de la copia de seguridad.
      - **Hasta:** Especifique la hora de finalización de la tarea de rendimiento de la copia de seguridad.



c. Haga clic en **Guardar**.

La programación del regulador de la lectura de disco se especifica y se muestra en la página Programación.

5. Especifique la hora de inicio para la copia de seguridad programada.



Nota: La captura de pantalla anterior no es válida para copias de seguridad de RMAN.

6. Especifique los valores de configuración de la retención de los puntos de recuperación para la programación Personalizada, Diaria, Semanal y Mensual.

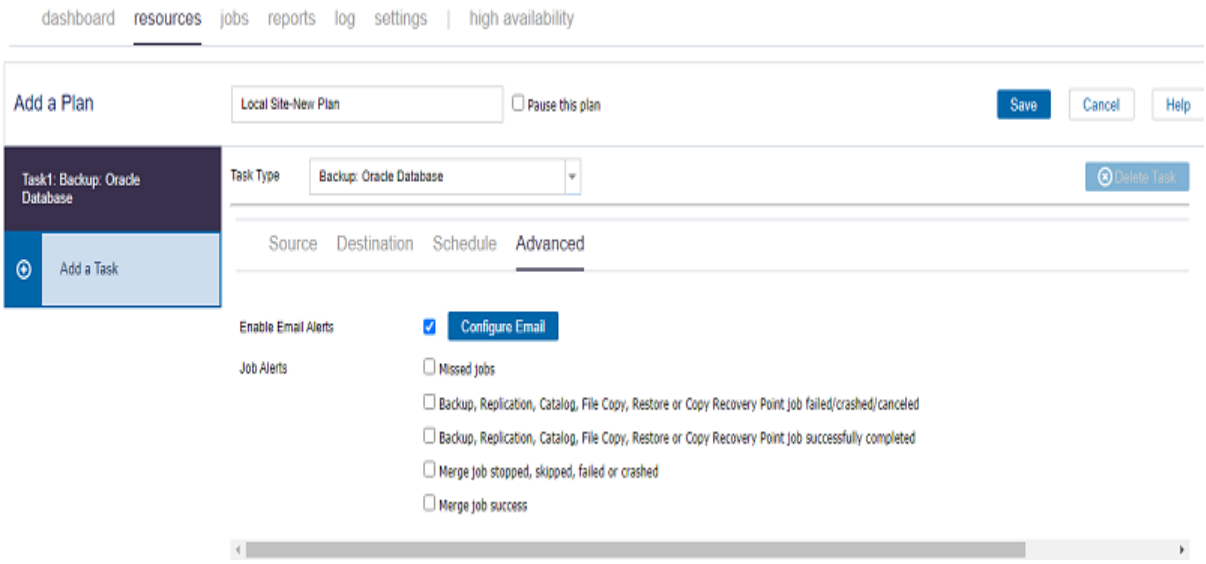
   Estas opciones se activan si se ha agregado la programación de la copia de seguridad correspondiente. Si se modifican los valores de configuración de la retención en esta página, los cambios se reflejan en el cuadro de diálogo Programación de la copia de seguridad.



Se especifica la programación.

Especificación de la configuración avanzada

La ficha Avanzada le permite especificar algunos valores de configuración avanzada para la tarea de copia de seguridad.



Siga estos pasos:

1. Especifique los siguientes detalles:

   Activar Alertas de correo electrónico

   Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y se pueden especificar los tipos de alertas que se desea recibir en un correo electrónico. Cuando se selecciona esta opción, las opciones siguientes estarán disponibles para su selección.

   Configurar correo electrónico

   Le permite configurar los valores de configuración del correo electrónico.

   Para configurar el servidor de correo electrónico y los detalles del servidor proxy, haga clic en **Configurar correo electrónico**.

   Alertas de tarea

   Le permite especificar los tipos de correos electrónicos de las tareas que se desean recibir.

2. Haga clic en **Guardar**.

Se especifica la configuración avanzada.

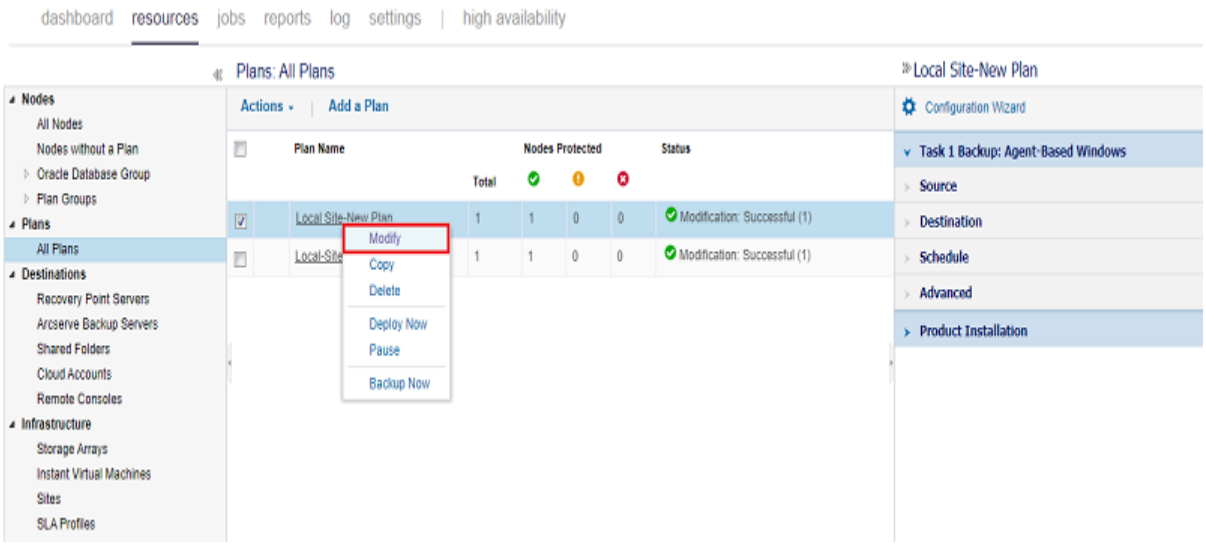
Adición de una tarea de recuperación asegurada al plan

Una tarea de recuperación asegurada incluye una tarea de recuperación asegurada para un plan de replicación/copia de seguridad existente. Cada tarea está formada por parámetros que definen el origen, la configuración de la prueba, la programación y la configuración avanzada. Cree una tarea de recuperación asegurada en función de la tarea de replicación o de copia de seguridad para verificar la recuperación asegurada y la accesibilidad de los datos y proporcione la comprobación de la integridad de los datos.

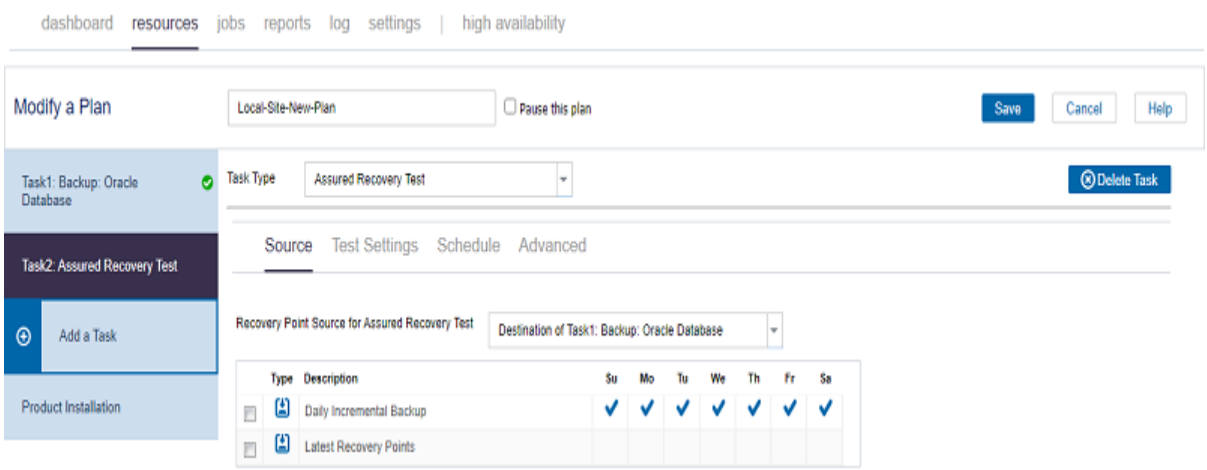
Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y, a continuación, haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic con el botón secundario del ratón en el plan de copia de seguridad existente y, a continuación, haga clic en **Modificar**.



4. En la página Modificar un plan, haga clic en **Agregar** una tarea en el panel izquierdo.



5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa el plan, la tarea de recuperación asegurada no se iniciará. Cuando se reanuda el plan, la tarea de recuperación asegurada no se reanuda automáticamente. Se debe ejecutar manualmente otra tarea de copia de seguridad para iniciar la tarea de recuperación asegurada.

6. En la lista desplegable Tipo de tarea, seleccione la opción **Prueba de recuperación asegurada**.

7. A continuación, especifique los detalles de Origen, Configuración de la prueba, Programación y Avanzada.

8. Haga clic en **Guardar**

   Los cambios se guardan y la tarea de recuperación asegurada se implementa automáticamente.

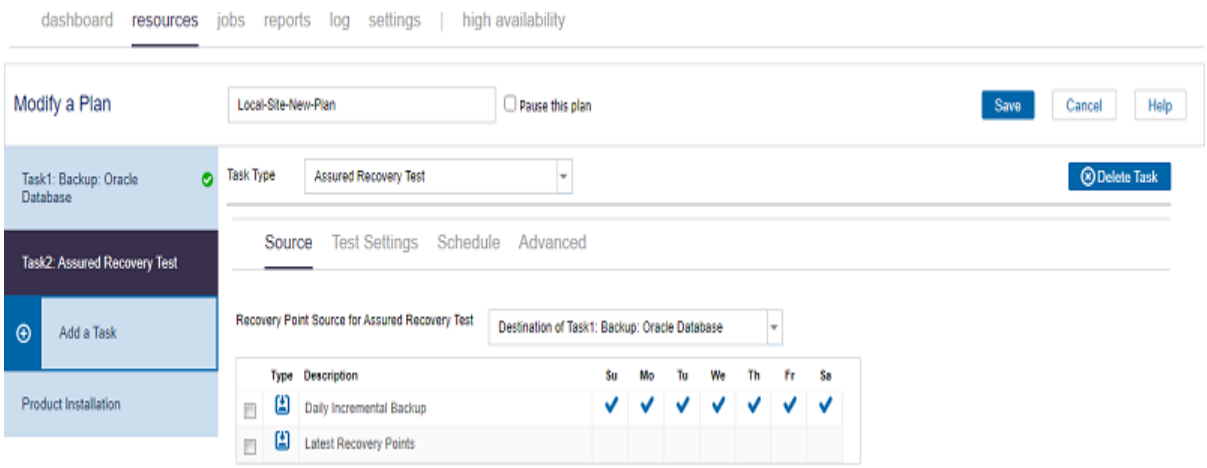
   Nota: Para comprobar y verificar la integridad de los datos de la copia de seguridad de Oracle como, por ejemplo, archivos de control, archivos de datos, registros de archivado y archivos de SP, la tarea de recuperación asegurada ejecuta el comando Restore Validate RMAN en el servidor de puntos de recuperación.

Especificación del origen

La ficha Origen le permite especificar el punto de recuperación de origen que se desea proteger.

Siga estos pasos:

1. En la ficha Origen, en la lista desplegable Origen del punto de recuperación para la prueba de recuperación asegurada, seleccione la opción deseada.



2. Seleccione los tipos de puntos de recuperación para la prueba de la recuperación asegurada. Puede seleccionar cualquiera de las dos siguientes opciones:

   - Prueba de la recuperación asegurada desde los tipos de copia de seguridad seleccionados

     Se puede seleccionar Copias de seguridad diarias, Copias de seguridad semanales o Copias de seguridad mensuales. Las opciones diarias, semanales o mensuales están disponibles en función de la programación de la copia de seguridad de origen. Por ejemplo, si la copia de seguridad de origen solo tiene programadas copias de seguridad mensuales, la prueba de la recuperación asegurada de la opción de los tipos de copia de seguridad seleccionados solo tendrá activada la opción Copias de seguridad mensuales.

   - Prueba de la recuperación asegurada de los puntos de recuperación más recientes

Se especifica el origen

Pasos siguientes:

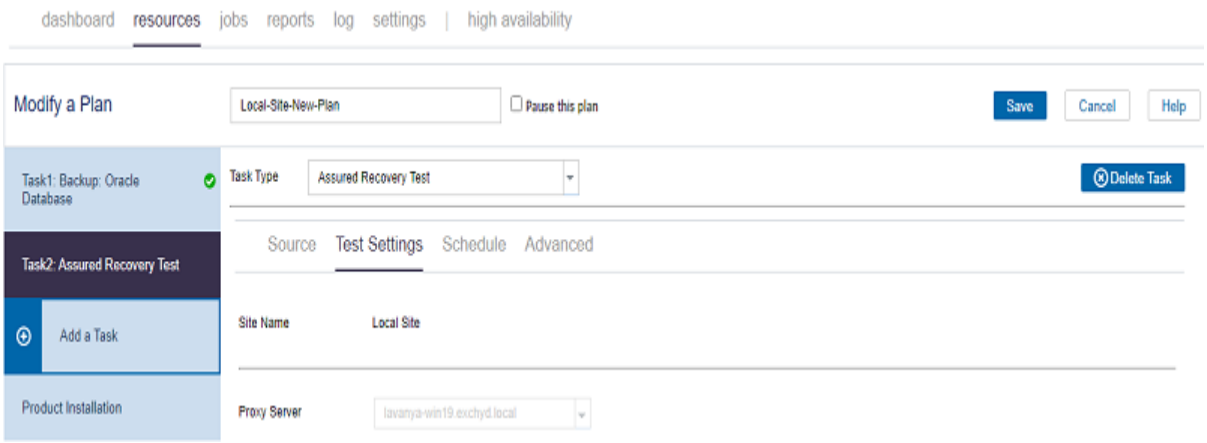
- Especificación de la configuración de prueba
- Especificación de la programación de la tarea de prueba de la recuperación asegurada
- Especificación de la configuración avanzada

Especificación de la configuración de prueba

La ficha Configuración de prueba permite especificar el servidor proxy.

Siga estos pasos:

1. Haga clic en la ficha **Configuración de prueba**.



2. En la lista desplegable Servidor proxy, seleccione el nodo del servidor proxy.

   Nota: Para Oracle, el servidor de puntos de recuperación actúa como servidor proxy en la prueba de recuperación asegurada.

   Se especifica la configuración de prueba.

Pasos siguientes:

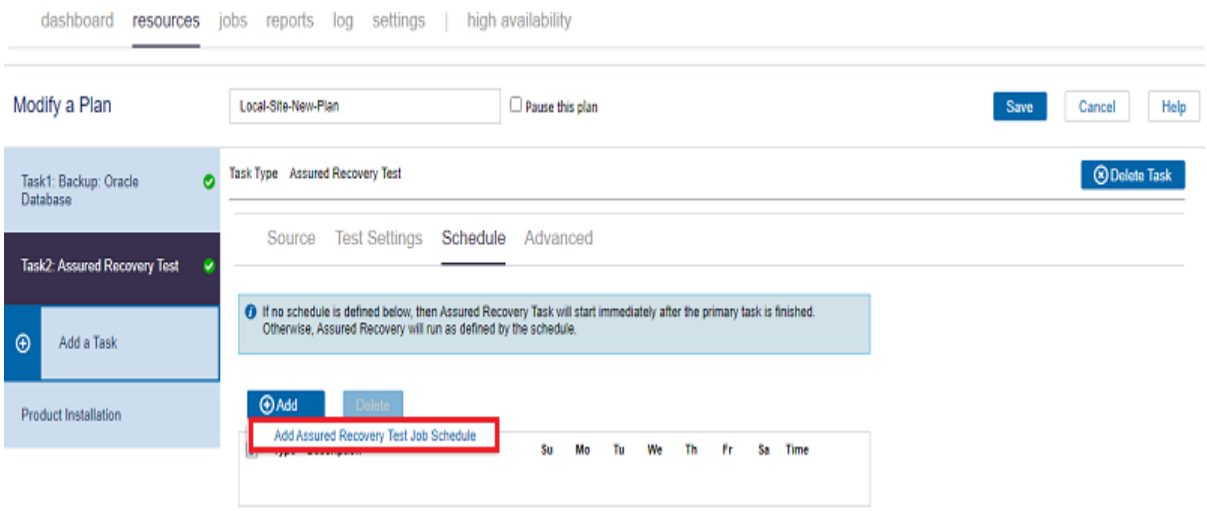
- Especificación de la programación de la tarea de prueba de la recuperación asegurada
- Especificación de la configuración avanzada

Especificación de la programación de la tarea de prueba de la recuperación asegurada

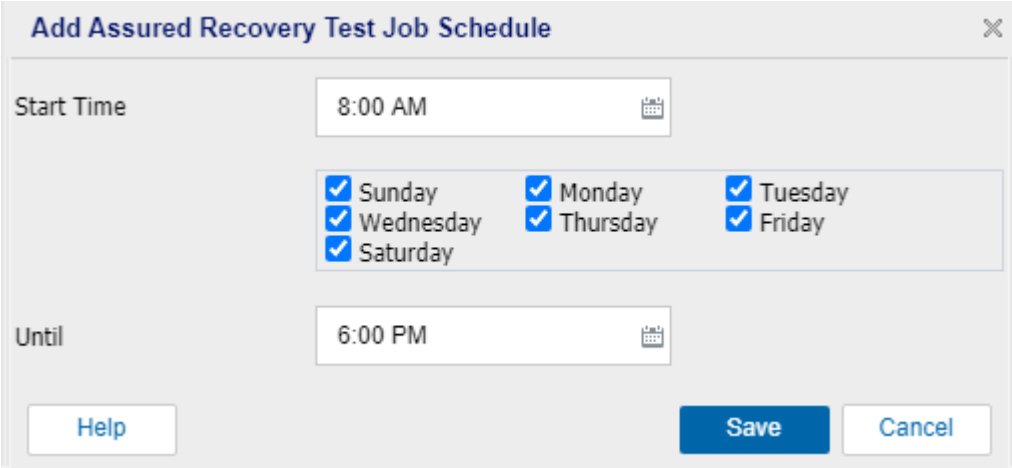
La ficha Programación permite especificar la programación de la tarea de prueba de la recuperación asegurada. Si no se especifica una programación, la tarea se inicia inmediatamente cuando se complete la tarea principal.

Siga estos pasos:

1. Haga clic en la ficha **Programación**.



2. Haga clic en **Agregar** y, a continuación, seleccione **Agregar programación de la tarea de prueba de la recuperación asegurada**.
3. En el cuadro de diálogo Agregar programación de la tarea de prueba de recuperación asegurada, haga lo siguiente y, a continuación, haga clic en **Guardar**:
   - **Hora de inicio**: Especifique la hora de inicio para iniciar la tarea de prueba de recuperación asegurada.
   - **Hasta:** Especifique la hora de finalización de la tarea de prueba de recuperación asegurada.



La tarea de prueba de recuperación asegurada se programa y aparece en la página Programación.

Notas:

- Si el origen de la recuperación asegurada es Puntos de recuperación más reciente y Activar la programación de la recuperación asegurada, el valor predeterminado es 1. Como resultado, se verifica el más reciente de forma predeterminada.

  Para el valor <= 0, se prueban todos los puntos de recuperación no verificados.

- Si el origen de la recuperación asegurada es diaria/semanal/mensual y Activar la programación de la recuperación asegurada, el valor predeterminado es 9 (diaria 7 + 1 semanal + 1 mensual).

  Para el valor <= 0, se prueban todos los puntos de recuperación no verificados.

- Si no se desea utilizar el valor predeterminado, se puede agregar una clave de registro DWORD de 32 bits en la ubicación siguiente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AssuredRecovery\MaxNumberOfRecoveryPoint

Paso siguiente:

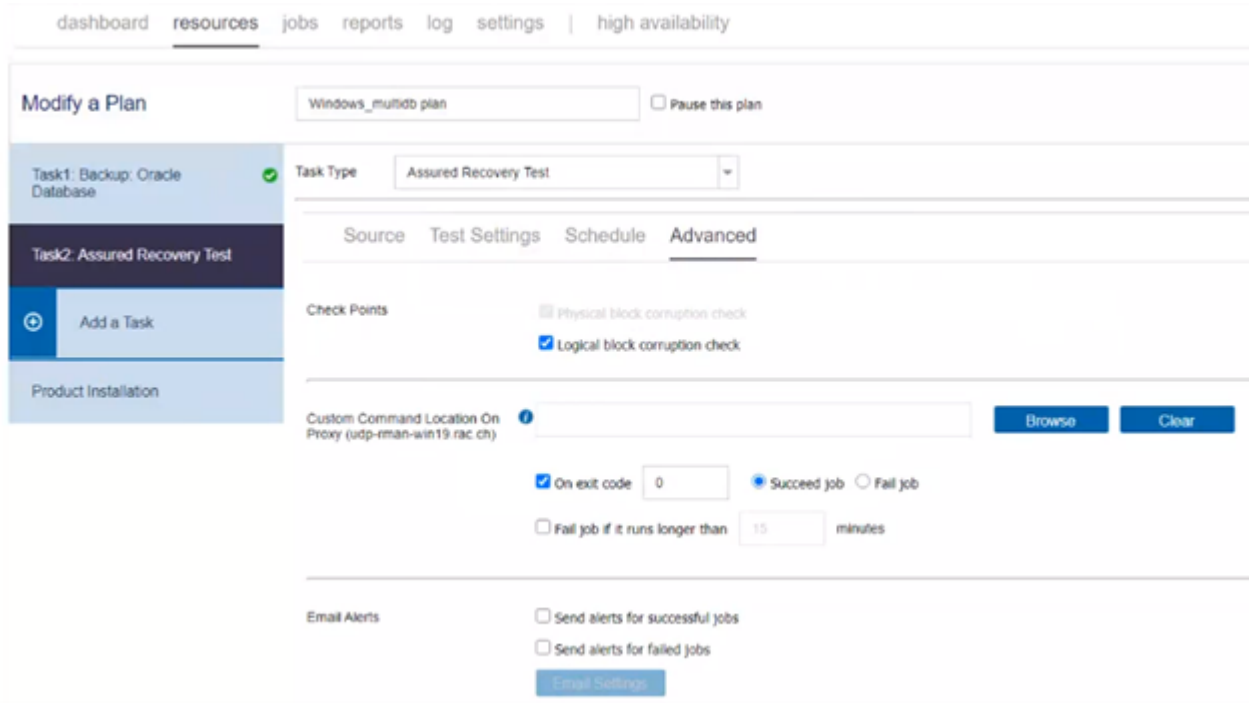
- Especificación de la configuración avanzada

Especificación de la configuración avanzada

La ficha Opciones avanzadas le ayudará a aplicar otros valores de configuración necesarios para completar el plan. Es una ficha opcional si no se necesita agregar más valores de configuración.

Siga estos pasos:

1. Haga clic en la ficha **Opciones avanzadas**.



2. Realice los pasos siguientes:

   Puntos de control

   Comprobación de la corrupción del bloque físico

   RMAN solo detecta los bloques físicamente dañados con cada copia de seguridad que realiza y almacena la información dañada en el archivo de control y en el archivo alert.log. De forma predeterminada, la opción **Comprobación de la corrupción del bloque físico** está activada.

   Comprobación de la corrupción del bloque lógico

   RMAN no detecta automáticamente los bloques dañados lógicamente de forma predeterminada. Seleccione la casilla de verificación **Comprobación de la corrupción del bloque lógico** para detectar la corrupción lógica junto con la corrupción física. Si se encuentra corrupción lógica, RMAN almacena la información del daño en el archivo alert.log.

Ubicación personalizada del comando en el servidor proxy

Nota: Esta opción solamente se muestra cuando se ha seleccionado la replicación o la copia de seguridad de Linux basada en agente como el origen del punto de recuperación de la prueba de recuperación asegurada.

Especifica el script personalizado que se almacena en el servidor proxy. Se puede explorar la información sobre el volumen del servidor proxy. Si se selecciona el tipo de recuperación asegurada de la máquina virtual instantánea, el script se copia en la máquina virtual y se ejecuta cuando se inicia la máquina virtual. Si se selecciona el tipo de recuperación asegurada del disco duro virtual instantáneo , el script se ejecuta en el servidor proxy.

Nota: La tarea de recuperación asegurada solo puede admitir el script .bat ejecutable de Windows o el binario ejecutable. Sin embargo, esta limitación no limita el uso de la tarea de recuperación asegurada. Se puede utilizar un script por lotes de Windows escrito para iniciar el script de PowerShell como, por ejemplo, el nombre test.bat con el contenido siguiente:

Powershell.exe -NoProfile -ExecutionPolicy ByPass -Command "& '%ScriptPath%\AR-check.ps1'"

Además, los siguientes argumentos pasan al script según sus requisitos.

- set PlanName=%1%

- set NodeName=%2%

- set ProxyServer=%3%

- set RecoveryPointName=%3%

- set MountPointRootPathName=%5% (aplicable solamente para el tipo de prueba Disco virtual instantáneo)

Como resultado, el archivo .bat se invoca y se ejecuta de la siguiente manera:

Para el tipo de prueba de la máquina virtual instantánea:

"%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName

Para el tipo de prueba del disco virtual instantáneo:

%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName MountPointRootPathName

En código de salida

Especifica el código de salida para una tarea realizada correctamente o para una tarea errónea.

Tarea correcta

Especifica que la tarea de recuperación asegurada está configurada para realizarse correctamente cuando el script devuelva el código de salida.

Tarea errónea

Especifica que la tarea de recuperación asegurada está configurada para realizarse erróneamente cuando el script devuelva el código de salida.

Tarea errónea si se ejecuta durante más tiempo que

Especifica si el script se ejecuta durante más tiempo que el especificado.

Valor predeterminado: 15 minutos.

Alertas de correo electrónico

Le permite activar alertas de correo electrónico. Se pueden configurar valores de configuración del correo electrónico y especificar el tipo de alertas que se desea recibir en un correo electrónico.

- Si desea recibir alertas de correo electrónico sobre la realización correcta de la tarea de recuperación asegurada, seleccione la casilla de verificación **Enviar alertas para las tareas correctas**.
- Si desea recibir alertas de correo electrónico para los errores de las tareas de recuperación asegurada, seleccione la casilla de verificación **Enviar alertas para las tareas erróneas**.

  Nota: No está disponible para aquellas tareas que se ejecutan con el servidor de copia de seguridad de Linux.

Configuración del correo electrónico

Le permite configurar los valores de configuración del correo electrónico.

Para configurar el servidor de correo electrónico y los detalles del servidor proxy, haga clic en **Configuración del correo electrónico**. Para obtener más información sobre cómo configurar el correo electrónico, consulte la sección Configuración del correo electrónico y alertas.

Se especifica la configuración avanzada.

(Opcional) Realización de una copia de seguridad manual

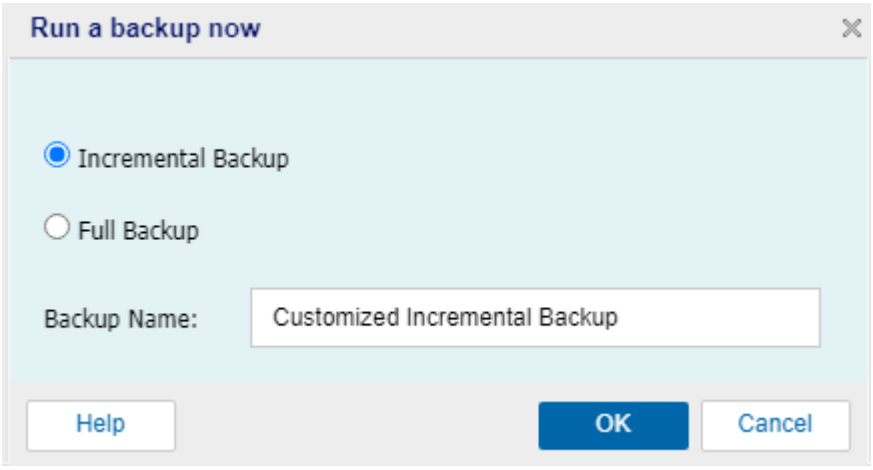
Normalmente se realizan copias de seguridad automáticamente y las controlan los valores de configuración de programación. Además de la copia de seguridad programada, una copia de seguridad manual le proporciona la opción de realizar copias de seguridad de los nodos según sea necesario. Por ejemplo, si tiene una programación de repetición para las copias de seguridad completas e incrementales y desea hacer cambios importantes en el equipo, debe realizar una copia de seguridad manual inmediata sin necesidad de esperar a la siguiente copia de seguridad programada.

Siga estos pasos:

1. Inicie sesión en la Consola de Arcserve UDP.
2. Vaya a **recursos** > **Plan** > **Todos los planes**.

   La lista de todos los planes se muestra en el panel central.
3. Haga clic con el botón secundario del ratón en el plan y, a continuación, seleccione **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo Ejecutar ahora una copia de seguridad.
4. En el cuadro de diálogo Ejecutar una copia de seguridad ahora, seleccione el tipo de copia de seguridad que desea realizar y, a continuación, especifique el nombre de la copia de seguridad si es necesario.



A continuación se especifican las opciones disponibles:

Copia de seguridad incremental

Inicia una copia de seguridad incremental del equipo. Una copia de seguridad incremental sólo hará una copia de seguridad de los bloques que han cambiado desde la copia de seguridad anterior.

Nota: Si está realizando una copia de seguridad por primera vez, la copia de seguridad completa se iniciará automáticamente aunque haya seleccionado la opción Copia de seguridad incremental.

Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Ésta es la manera más óptima de realizar copias de seguridad.

Copia de seguridad completa

Inicia una copia de seguridad completa del equipo o los volúmenes seleccionados.

Notas:

- También se puede ejecutar la copia de seguridad manualmente desde la página Nodos.
- Si no se especifica ningún nombre de copia de seguridad, de forma predeterminada se llamará Copia de seguridad incremental o completa personalizada.

5. Haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Información de progreso.

6. Espere hasta que finalice la tarea de copia de seguridad y, a continuación, haga clic en **Aceptar**.

7. Para controlar las tareas de copia de seguridad, vaya a **tareas** > **Tareas en ejecución**.

   Espere hasta que la tarea de copia de seguridad haya finalizado.

   Nota: Solamente se puede restaurar una tarea cada vez. Si intenta iniciar una tarea de copia de seguridad manualmente cuando se está ejecutando otra tarea al mismo tiempo, aparecerá un mensaje de alerta para informar de que otra tarea está en ejecución y solicitará intentarlo de nuevo más tarde.

   La copia de seguridad manual se realiza correctamente.

Cómo restaurar una base de datos de Oracle utilizando RMAN

Se puede restaurar toda la base de datos de Oracle o realizar una recuperación granular de los espacios de tabla y de las tablas. También se puede restaurar la base de datos desde el punto de recuperación a la ubicación de la base de datos de Oracle, a una ubicación alternativa o a un nodo.

Para restaurar la base de datos de Oracle, siga estos pasos:

1. Selección de los elementos de la base de datos de Oracle para restaurar
2. Definición de las opciones de restauración

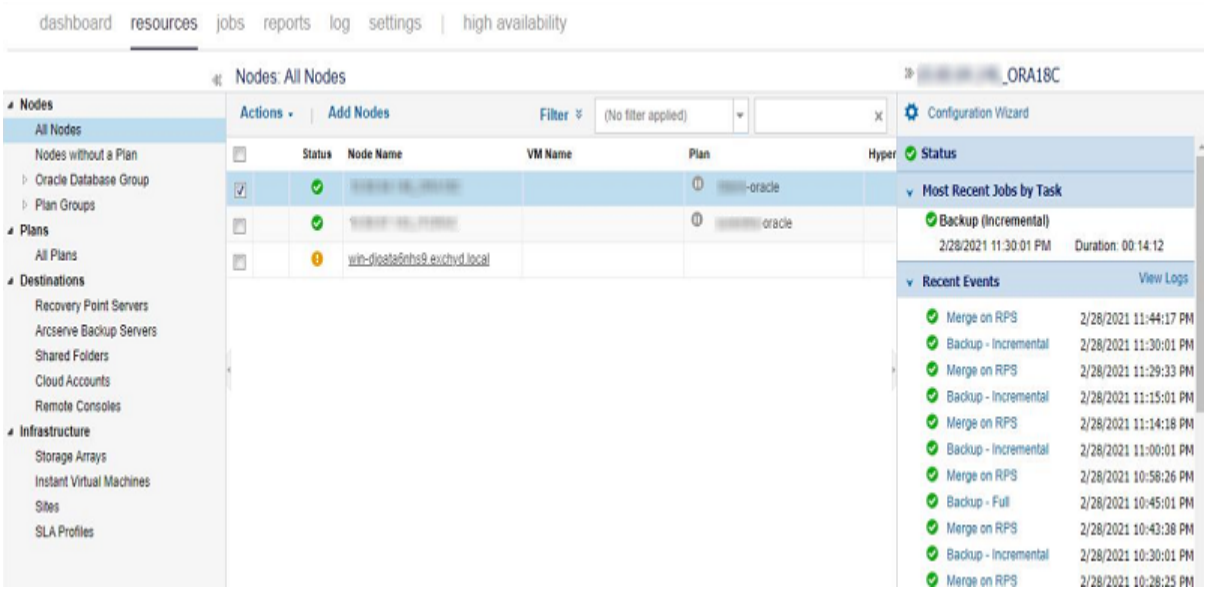
Selección de los elementos de la base de datos de Oracle para restaurar

Esta sección proporciona información sobre cómo examinar y seleccionar elementos de la base de datos de Oracle para restaurarlos.

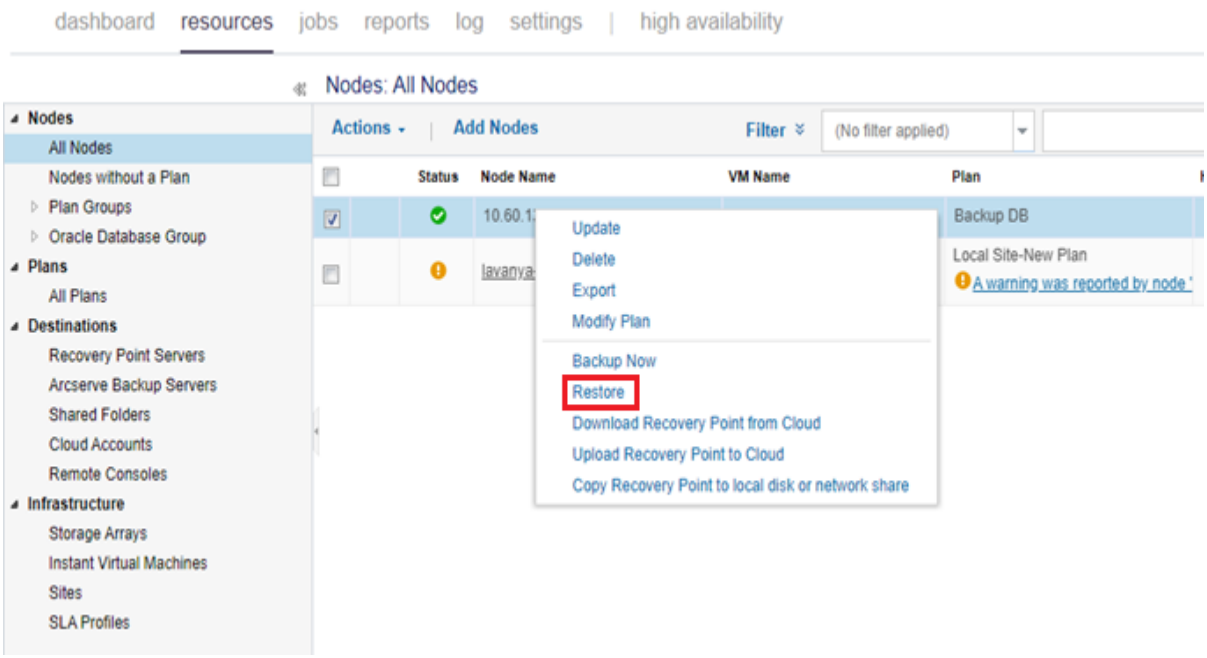
Siga estos pasos:

1. Inicie sesión en la cuenta de la Consola de UDP.
2. En la página de la Consola de UDP, haga clic en la ficha **recursos**.
3. En el panel izquierdo, vaya a **Nodos** > **Todos los nodos**.

   La lista de nodos existentes aparece en el panel central.



4. Haga clic con el botón secundario del ratón en el nodo de Oracle y, a continuación, seleccione la opción **Restaurar**.

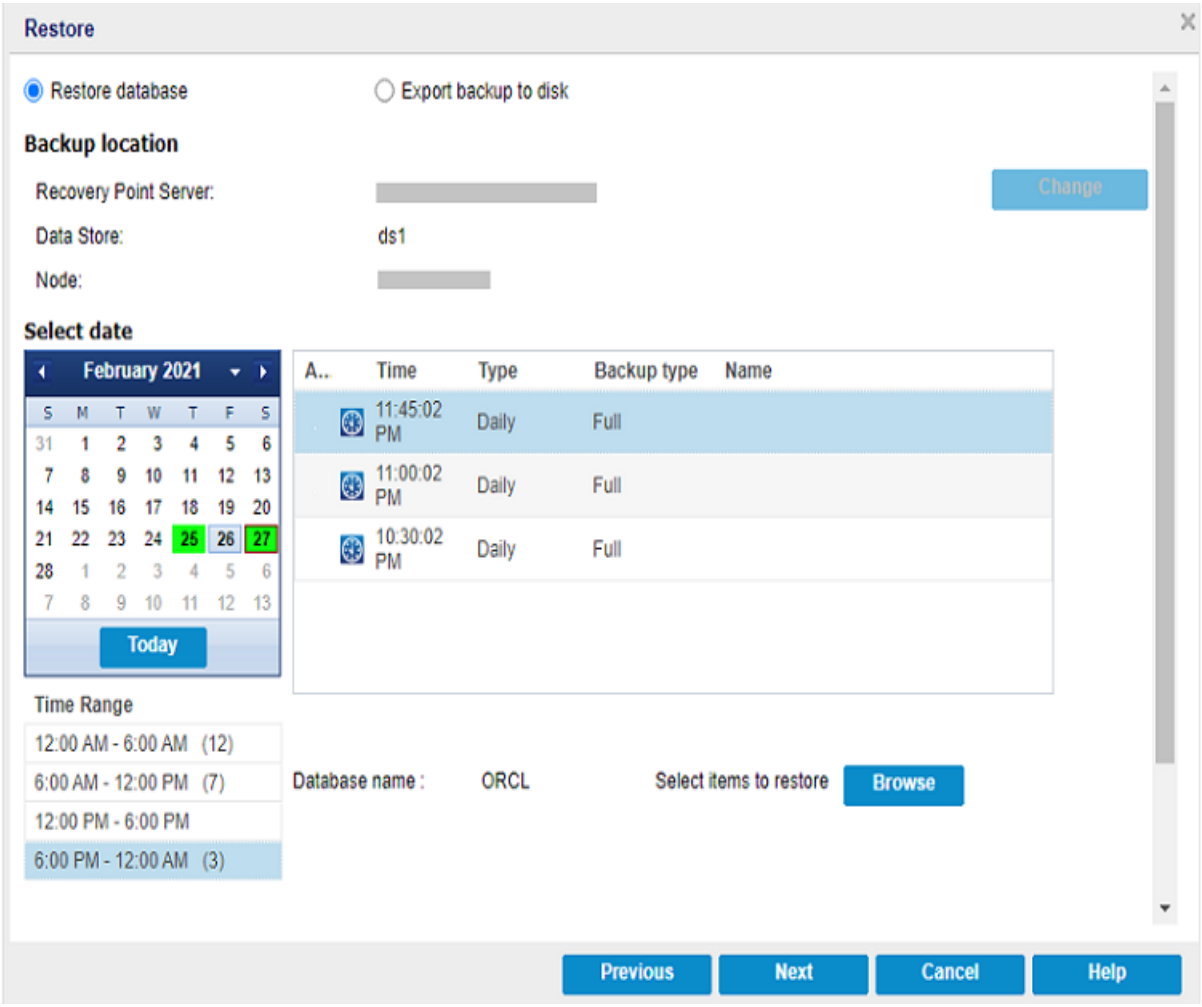


Se inicia sesión automáticamente en el nodo del agente y aparece el Asistente de restauración.

5. En el Asistente de restauración, seleccione una de las siguientes opciones:

   Restaurar base de datos

   La restauración de la base de datos incluye los pasos para la restauración completa y granular de la base de datos.



Para seleccionar los elementos de la base de datos de Oracle, siga estos pasos:

a. (Opcional) Para modificar los detalles de la ubicación de la copia de seguridad, haga clic en **Cambiar**.

   Nota: Esta opción solo es válida cuando se selecciona la opción Exportar copia de seguridad a disco.

b. En la sección Seleccionar fecha, seleccione una fecha.

   En función de la selección, se muestra la lista de puntos de recuperación de la copia de seguridad con la hora de la copia de seguridad, el tipo de copia de seguridad que se ha realizado (completa o incremental) y el nombre de la copia de seguridad.

c. En la lista de puntos de recuperación de la copia de seguridad, seleccione el punto de recuperación de la copia de seguridad que desee restaurar.

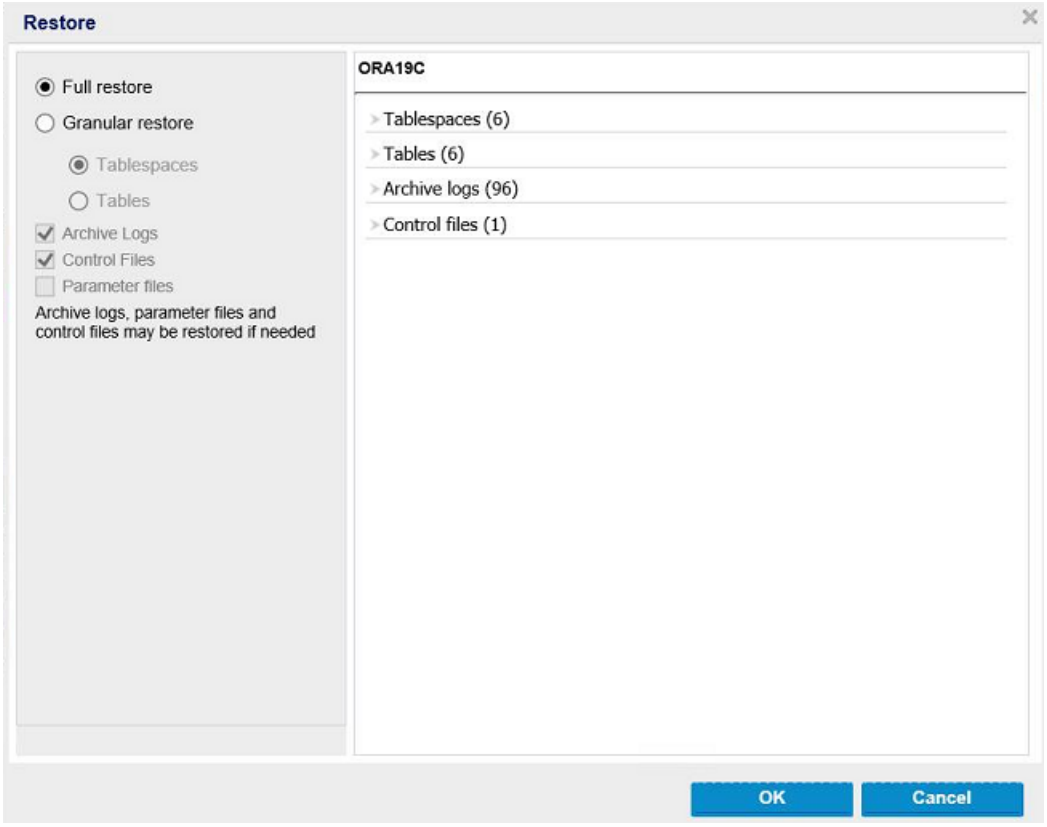
Nota: De forma predeterminada, se selecciona el último punto de recuperación de la copia de seguridad.

d. Para seleccionar los elementos de la base de datos, siga estos pasos:

- Haga clic en el botón **Examinar**.

  Aparecerá el cuadro de diálogo Restauración.

- En el cuadro de diálogo Restauración, haga lo siguiente:



  - En el panel izquierdo, realice lo siguiente:
    - Para realizar la restauración completa de todos los elementos de la base de datos, seleccione **Restauración completa**.
    - Para realizar la restauración de los espacios de tabla y de las tablas, seleccione **Restauración granular**.

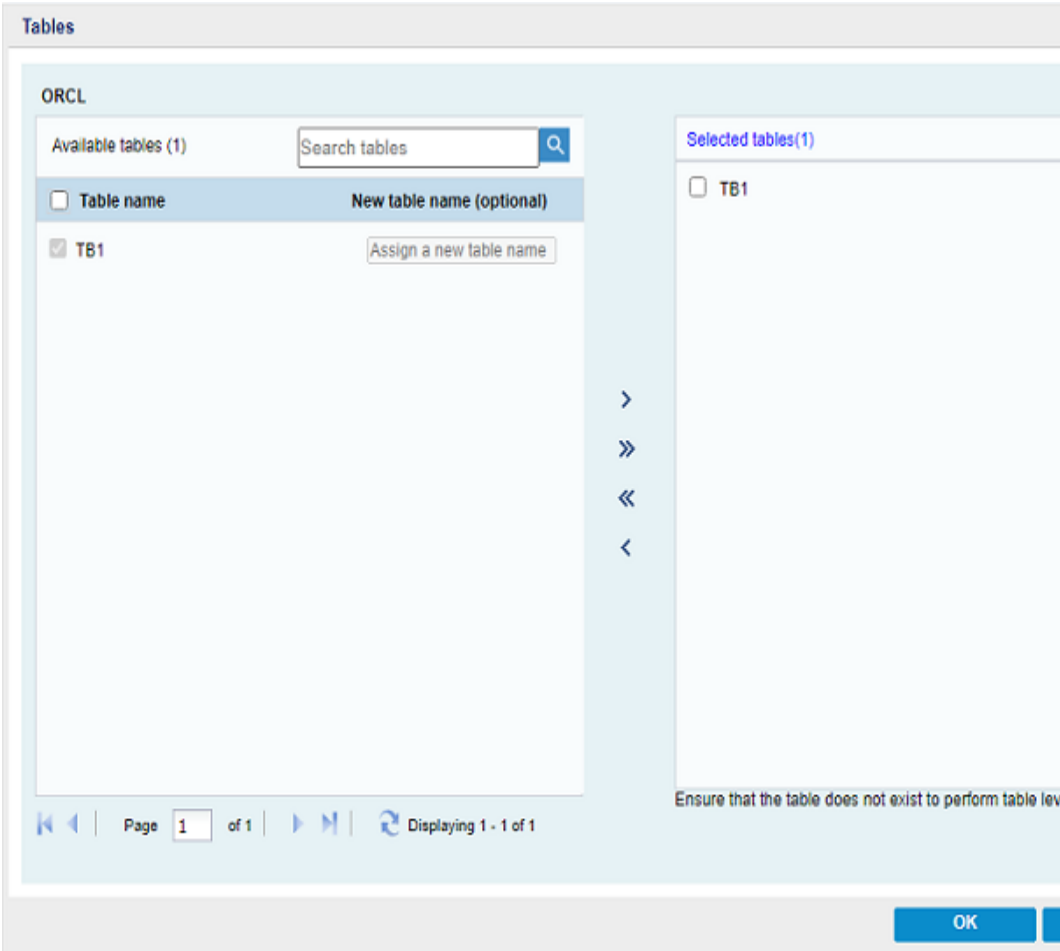
    Nota: Los elementos de la base de datos de Oracle como los registros archivado, los archivos de control y los archivos de parámetros se seleccionan de forma predeterminada cuando aparece el cuadro de diálogo

Restauración. Además, estos elementos se restauran si es necesario.

- En el panel derecho, haga clic en cada archivo para expandirlo y, a continuación, consulte los detalles.
- (Opcional) Para seleccionar las tablas específicas, en el panel derecho haga clic en la opción **Tablas**.

  Aparece un cuadro de diálogo de selección de tabla.

  En el cuadro de diálogo de selección de tabla, haga lo siguiente y, a continuación, haga clic en **Aceptar**:



  - En el panel izquierdo, realice lo siguiente:
    - Para buscar las tablas disponibles, seleccione el nombre de la tabla en el cuadro de búsqueda y, a continuación, haga clic en el icono de búsqueda.

- Seleccione las tablas que desea restaurar.
- (Opcional) Escriba el nuevo nombre de la tabla que desea restaurar.

Después de seleccionar las tablas, haga clic en la flecha hacia la derecha (>) para moverlas a la lista de tablas seleccionadas().

- En el panel derecho, anule la selección de las tablas que no desea restaurar y, a continuación, haga clic en la flecha hacia la izquierda (<) para moverlas a la lista de ablas disponibles().

- Haga clic en **Aceptar**.

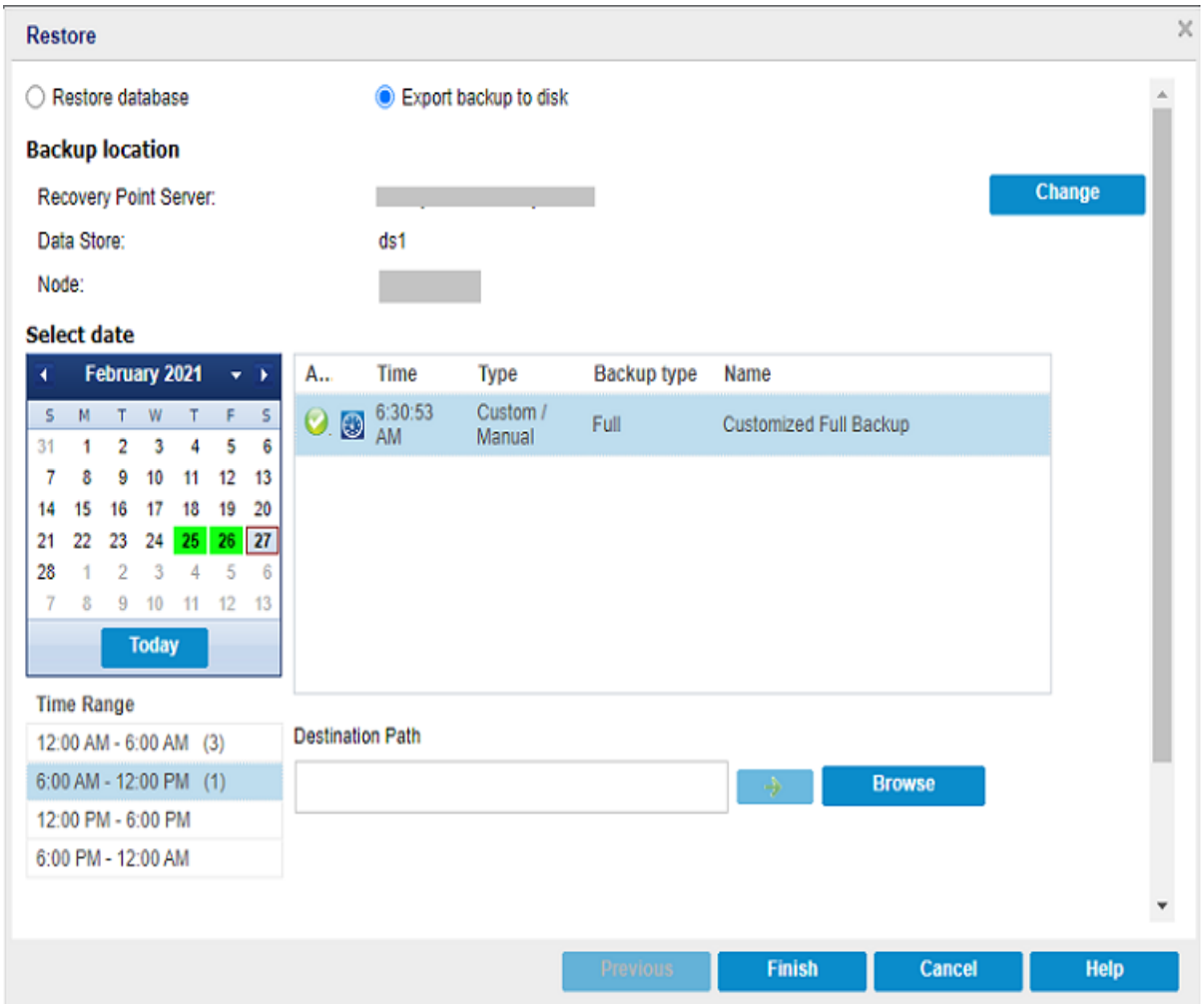
e. Haga clic en **Siguiente**.

Aparecerá el cuadro de diálogo Opciones de restauración de

Se seleccionan los elementos de la base de datos de Oracle que se van a restaurar. Ahora, se pueden definir las opciones de restauración.

Exportar base de datos a disco

Restaura los elementos de la base de datos de Oracle a una carpeta o carpeta compartida en el disco.



Para exportar la copia de seguridad al disco, siga estos pasos:

a. (Opcional) Para modificar los detalles de la ubicación de la copia de seguridad, haga clic en **Cambiar**.

b. En la sección Seleccionar fecha, seleccione una fecha.

   En función de la selección, se muestra la lista de puntos de recuperación de la copia de seguridad con la hora de la copia de seguridad, el tipo de copia de seguridad que se ha realizado (completa o incremental) y el nombre de la copia de seguridad.

c. En la lista de puntos de recuperación de la copia de seguridad, seleccione el punto de recuperación de la copia de seguridad que desee restaurar.

   Nota: De forma predeterminada, se selecciona el último punto de recuperación de la copia de seguridad.

d. En el campo Ruta de destino, proporcione la ruta completa del recurso compartido de red remoto.

e. Para validar la conexión, haga clic en el icono de la flecha verde situado junto al campo Ruta de destino, introduzca el nombre de usuario y la contraseña según sea necesario y, a continuación, haga clic en **Aceptar**.

f. Si la conexión se realiza correctamente al recurso compartido de red remoto, haga clic en el botón **Examinar**.

   Aparece el cuadro de diálogo Selección de la ubicación de la copia de seguridad.

g. En el cuadro de diálogo Seleccionar ubicación de copia de seguridad, seleccione una carpeta para restaurar y, a continuación, haga clic en **Aceptar**.

h. Haga clic en **Finalizar**.

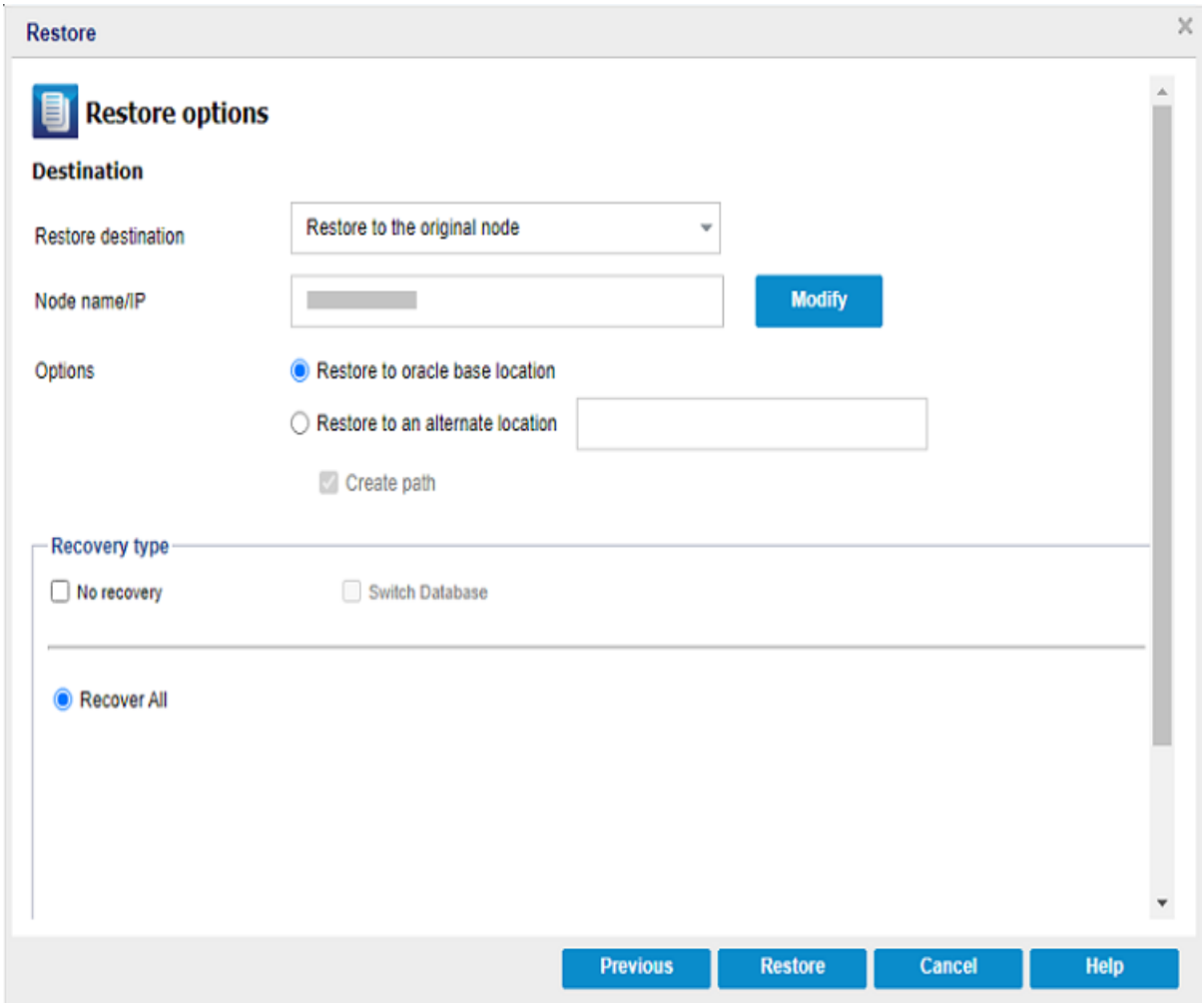
   Los elementos de la base de datos de Oracle se exportan al disco.

Definición de las opciones de restauración

Esta sección proporciona información sobre cómo definir las opciones de restauración para los elementos seleccionados de la base de datos de Oracle.

Siga estos pasos:

1. En el cuadro de diálogo Opciones de restauración, seleccione el destino para la restauración.



Notas:

- Durante la restauración, para cualquier punto de recuperación de la copia de seguridad completa, solo estará disponible la opción Recuperar todo.
- Los puntos de recuperación asociados a las copias de seguridad incrementales incluyen todas las opciones como Recuperar todo, A un

momento dado, Hasta SCN y Hasta el número de secuencia de registro para la restauración.

A continuación se especifican las opciones de destino disponibles:

Restaurar en el nodo original

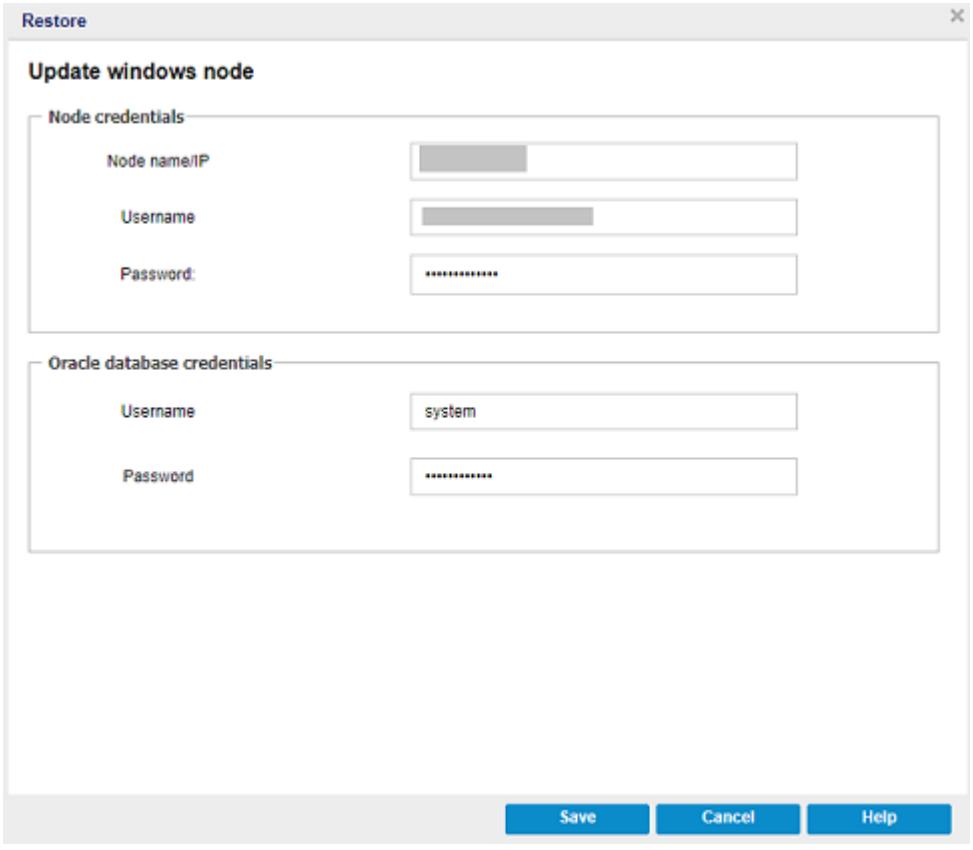
Para restaurar en el nodo original, realice los siguientes pasos:

- Los detalles del Nombre o dirección IP del nodo existente aparecen automáticamente. **En caso de que sea necesario cambiar los detalles del Nombre o dirección IP del nodo, haga clic en Modificar**.

  En función del tipo de nodo, aparecerá el cuadro de diálogo Actualizar nodo de Windows o Actualizar nodo de Linux.

  Actualizar nodo de Windows

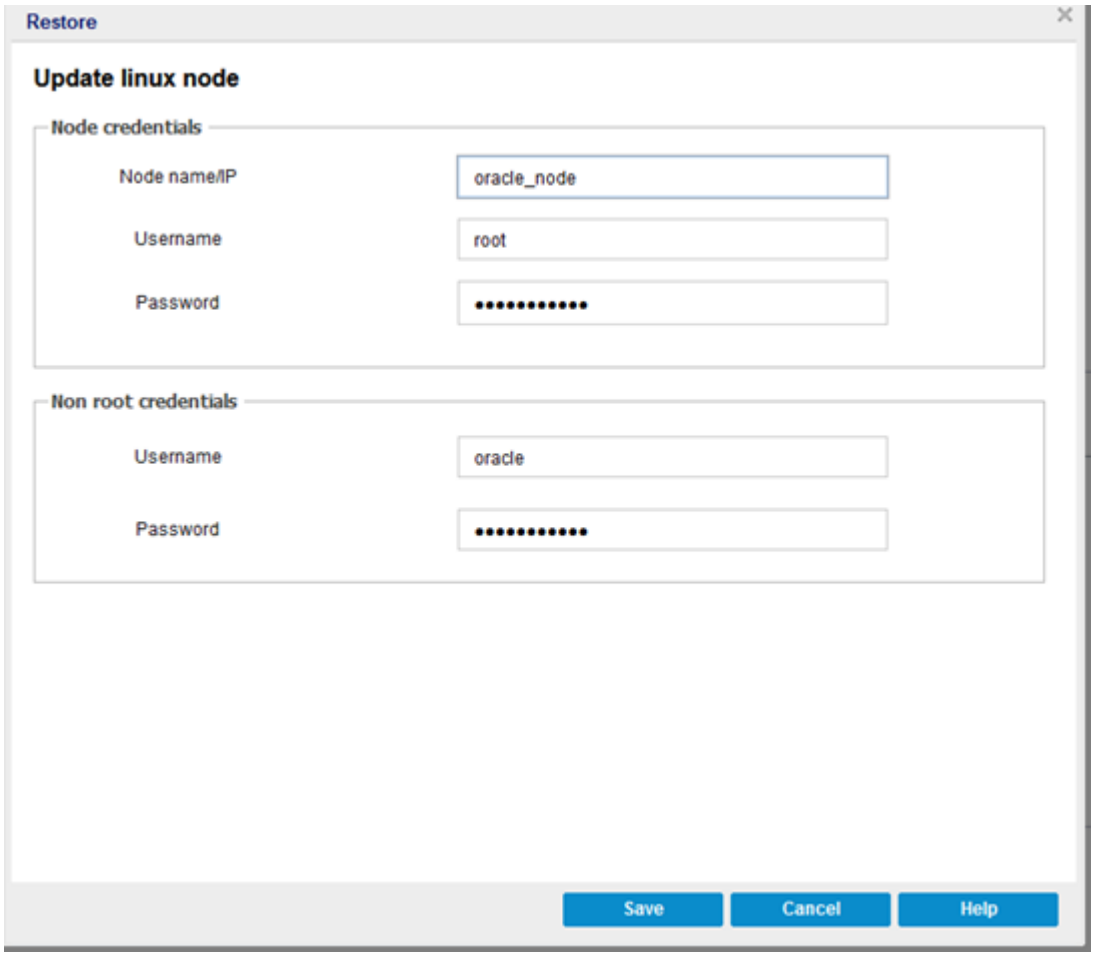
  En el cuadro de diálogo Actualizar nodo de Windows, introduzca el Nombre o dirección IP del nodo, el Nombre de usuario y la Contraseña según sea necesario y, a continuación, haga clic en **Guardar**.



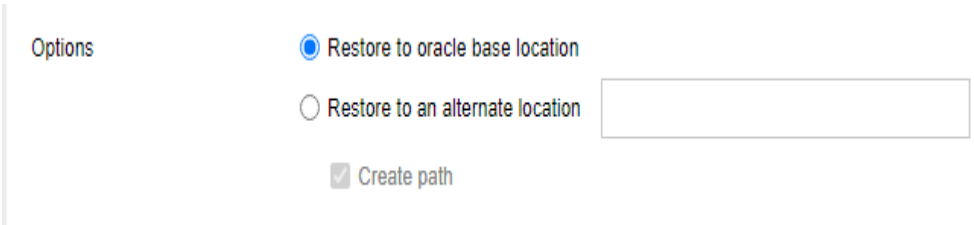
Actualizar nodo de Linux

En el cuadro de diálogo Actualizar nodo de Linux, actualice los siguientes detalles y, a continuación, haga clic en **Guardar**:

- Para las credenciales de nodo, introduzca el Nombre o dirección IP del nodo, el Nombre de usuario y la Contra-seña según sea necesario.
- Para las credenciales no raíz, introduzca el Nombre de usuario y la Contraseña según sea necesario.



- Para ver las opciones, seleccione una de las siguientes:



A continuación se especifican las opciones disponibles:

Restaurar en la ubicación base de Oracle

Restaura los elementos seleccionados de la base de datos en la ubicación base de Oracle desde la que se ha realizado la copia de seguridad.

Restaurar en una ubicación alternativa

Restaura en una ubicación alternativa. Cuando se selecciona esta opción, se debe agregar la ruta de la ubicación alternativa.

Nota: La casilla de verificación **Crear ruta** se selecciona automáticamente cuando se selecciona la opción **Restaurar en una ubicación alternativa**.

Restaurar en el nodo alternativo

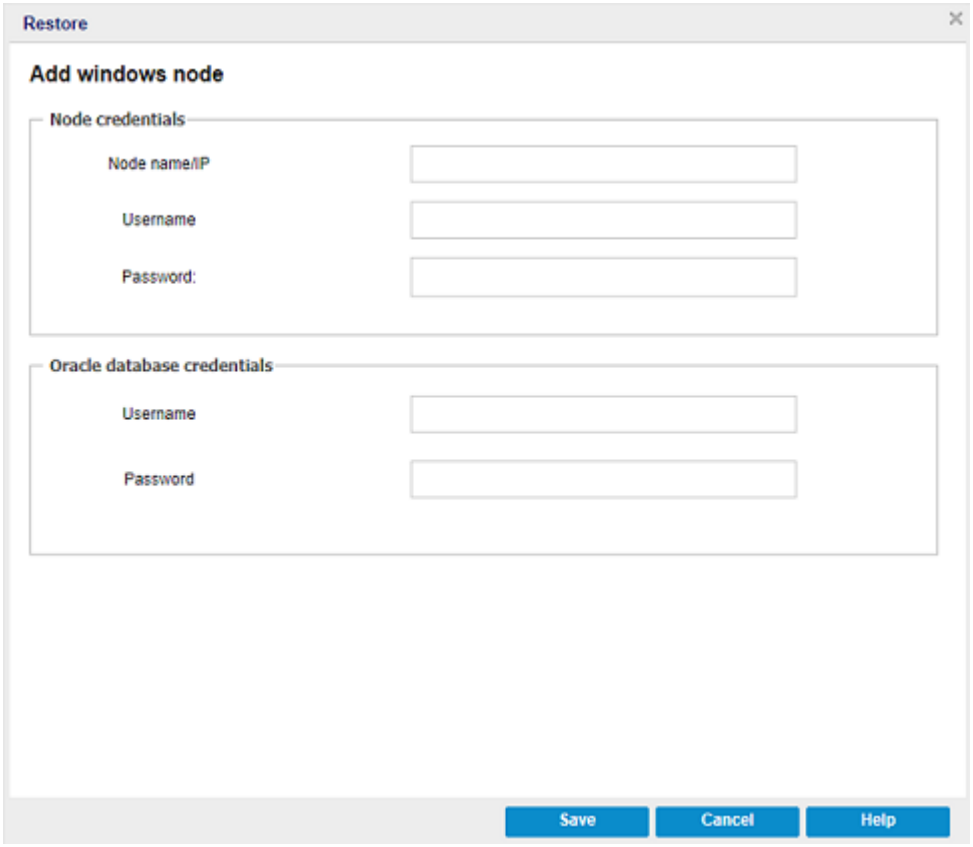
Para restaurar al nodo alternativo, realice lo siguiente:

- Para agregar un nuevo nodo o dirección IP, haga clic en el botón **Agregar**.

  En función del tipo de nodo, aparecerá el cuadro de diálogo Agregar nodo de Windows o Agregar nodo de Linux.

  Agregar nodo de Windows

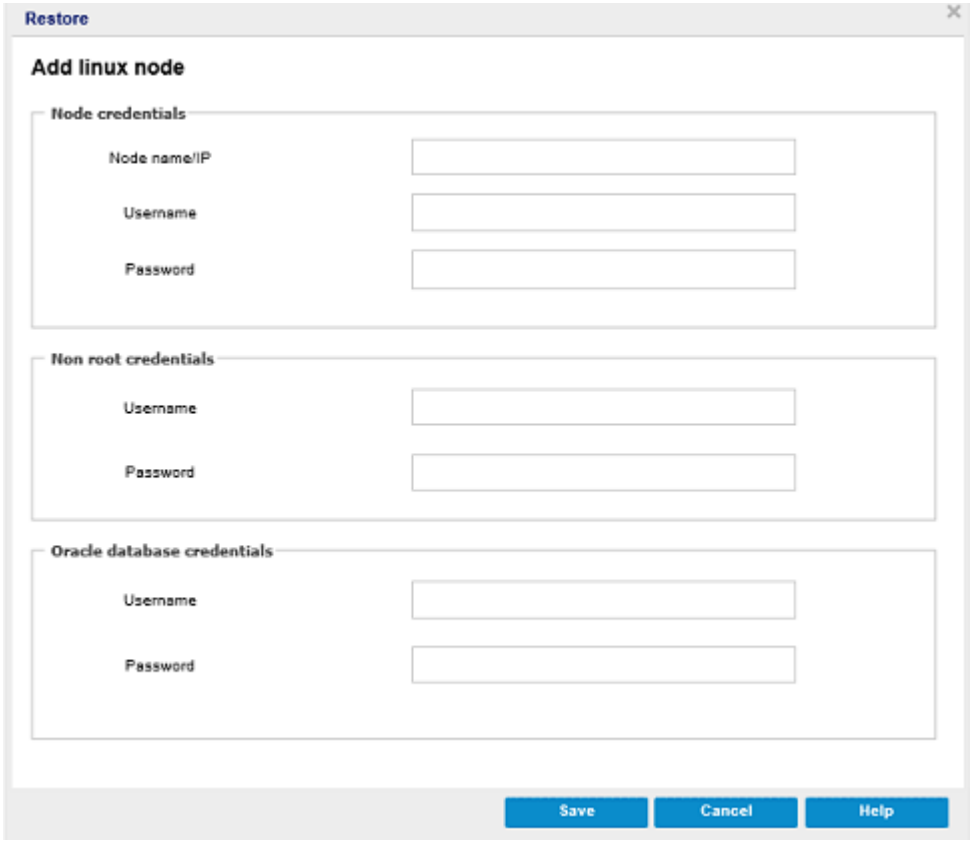
  En el cuadro de diálogo Agregar nodo de Windows, introduzca el Nombre o dirección IP del nodo, el Nombre de usuario y la Contraseña según sea necesario y, a continuación, haga clic en **Guardar**.



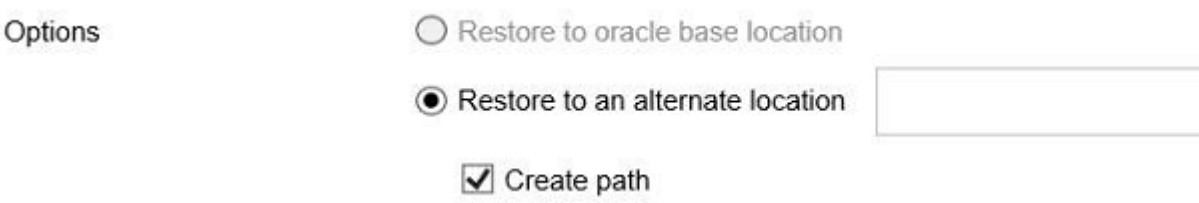
Agregar nodo de Linux

En el cuadro de diálogo Agregar nodo de Linux, agregue los detalles siguientes y, a continuación, haga clic en **Guardar**:

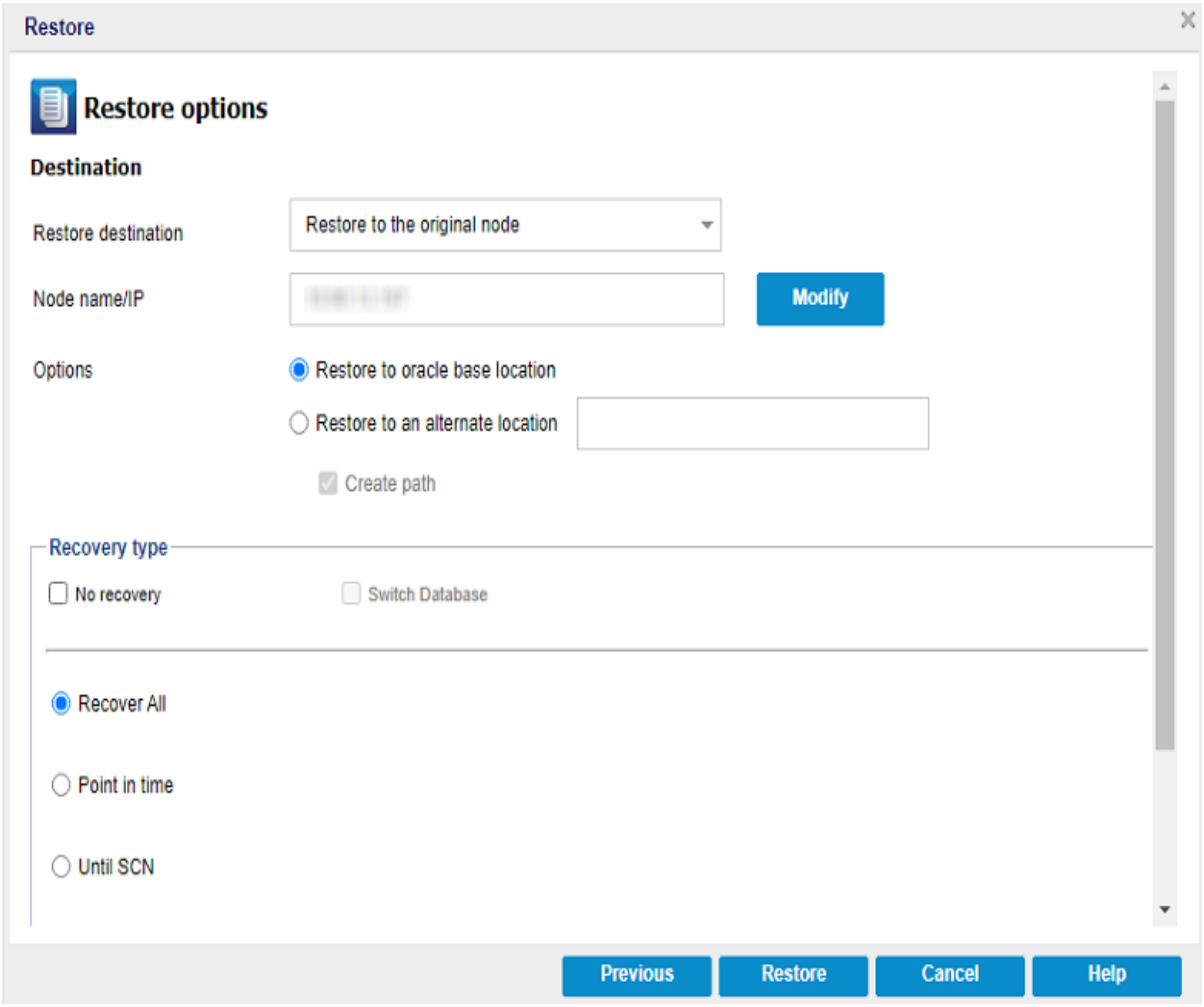
- Para las credenciales de nodo, introduzca el nuevo Nombre o dirección IP del nodo, el Nombre de usuario y la Contraseña según sea necesario.
- Para las credenciales no raíz, introduzca el nuevo Nombre de usuario y la Contraseña según sea necesario.



- En Opciones, la opción **Restaurar en una ubicación alternativa** está seleccionada de forma predeterminada. Introduzca la ruta de la ubicación alternativa.



2. En la sección Tipo de recuperación, haga lo siguiente:



- Si no desea ejecutar la recuperación, seleccione la casilla de verificación **Sin recuperación**. En función de la selección, se activa la siguiente opción:

  Cambiar base de datos

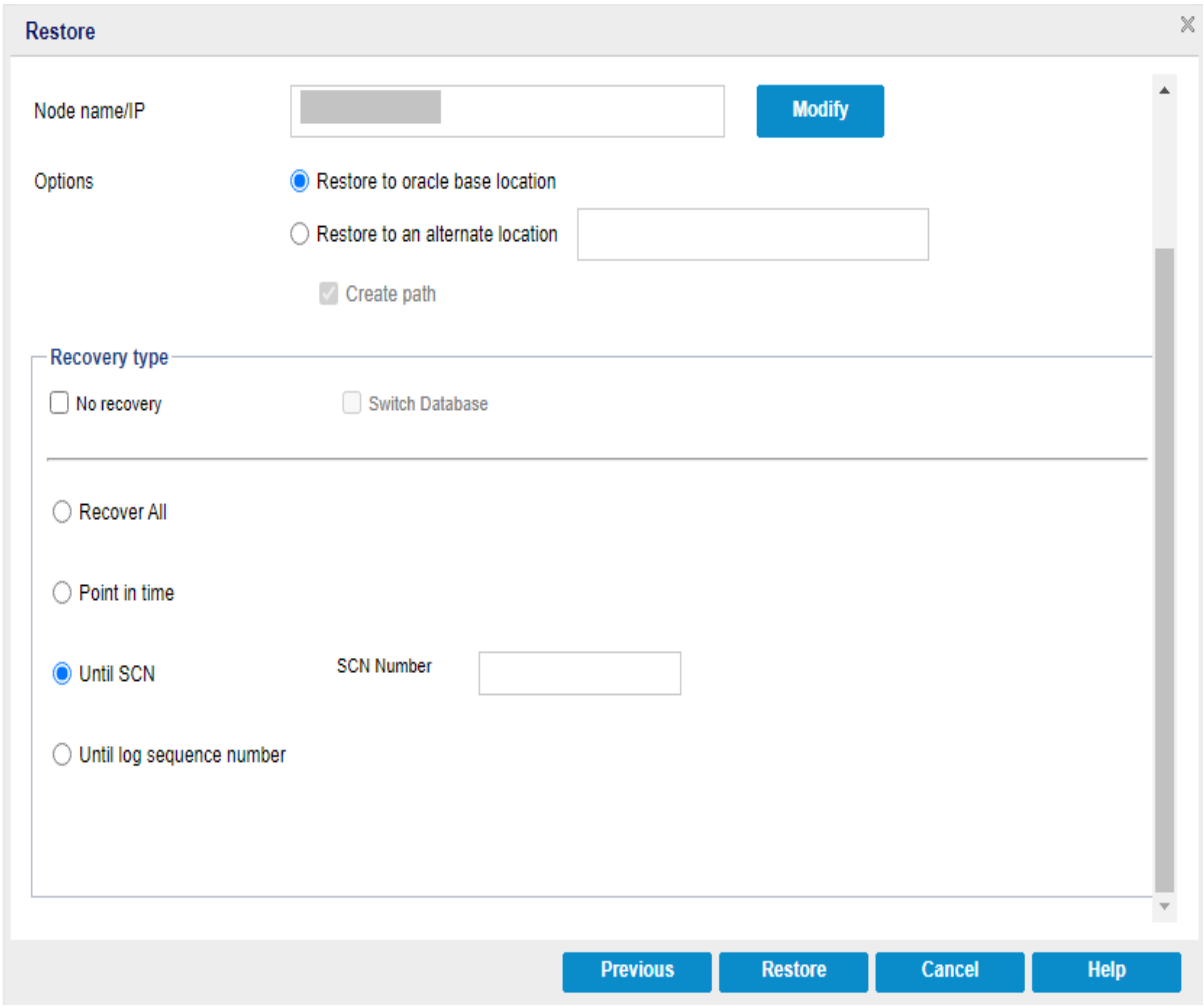
  Si desea cambiar los elementos de la base de datos a la nueva ubicación, seleccione la casilla de verificación **Cambiar base de datos**.

  Nota: La opción Cambiar base de datos solo se admite cuando se realiza la restauración a una ubicación o nodo alternativo.

- Si desea realizar la restauración a un momento determinado, seleccione **Momento determinado** y, a continuación, realice lo siguiente:
  - Seleccione una fecha para ejecutar la restauración a un momento determinado.
  - Seleccione la hora de inicio según sea necesario.

Nota: La fecha y la hora de inicio para la restauración a un momento determinado deben ser anteriores al punto de recuperación de la copia de seguridad seleccionado y posteriores al punto de recuperación anterior.

- Si desea recuperar todos los elementos de la base de datos hasta la marca de tiempo del Número de cambio del sistema (SCN), seleccione **Hasta SCN** y, a continuación, especifique el valor para el Número de SCN según sea necesario.



- Si desea recuperar todos los elementos de la base de datos hasta el número de secuencia de registro especificado, seleccione **Hasta número de secuencia de registro** y, a continuación, introduzca los valores de Secuencia de registro y Número de subproceso según sea necesario.

3. Haga clic en **Restaurar**.

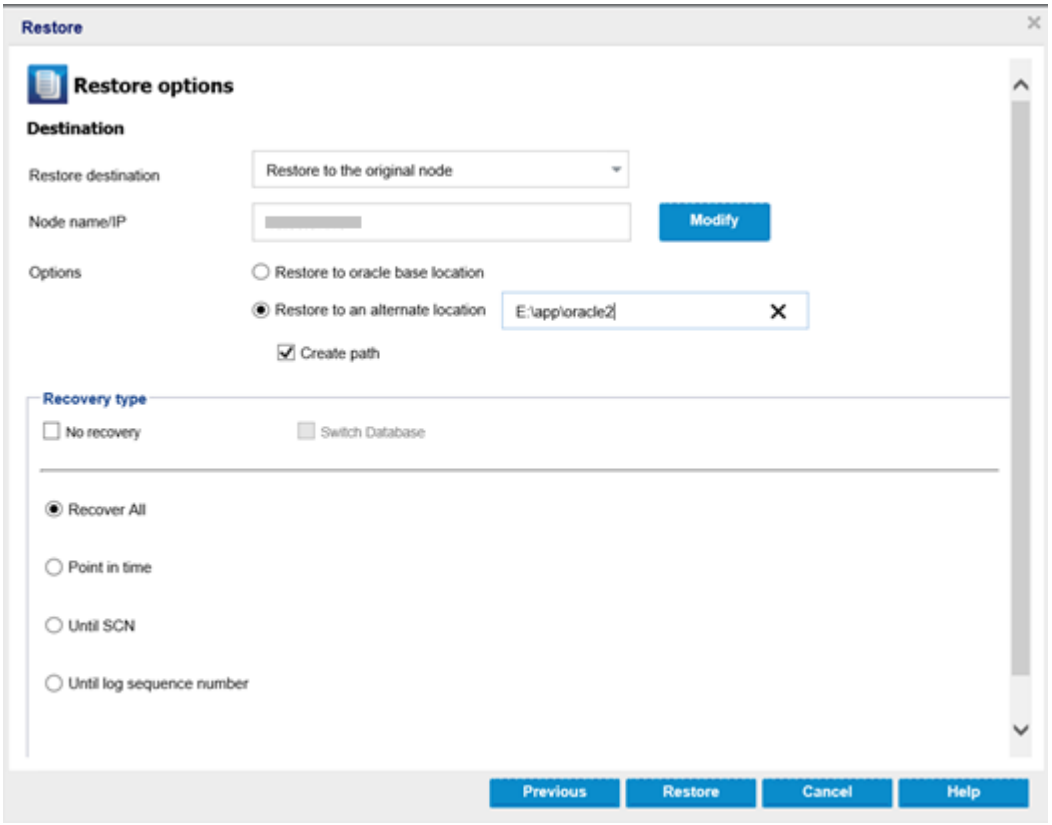
Se restauran los elementos de la base de datos de Oracle.

Cómo restaurar la base de datos a una ubicación alternativa en Windows

Esta sección proporciona información sobre cómo restaurar la base de datos a una ubicación alternativa en Windows.

Siga estos pasos:

1. En la Consola de UDP, seleccione el punto de recuperación desde el que necesita realizar la restauración. Para obtener más información, consulte Definición de las opciones de restauración.
2. En el cuadro de diálogo Opciones de restauración, en la lista desplegable Destino de la restauración, seleccione **Restaurar en el nodo original**.



3. Para Nombre o dirección IP del nodo, introduzca el nombre de nodo o la dirección IP.
4. En Opciones, seleccione la opción **Restaurar en una ubicación alternativa** y, a continuación, agregue una ruta de la ubicación alternativa.

   Notas:

- Asegúrese de que la ruta agregada no contenga caracteres especiales ni espacios.
- La casilla de verificación **Crear ruta** se selecciona automáticamente cuando se selecciona la opción **Restaurar en una ubicación alternativa**.
- Si la base de datos no se ha cerrado, aparecerá una notificación y se le solicitará que cierre la base de datos. Para confirmar, haga clic en **Aceptar**.

5. Confirme que la tarea de restauración es correcta desde la Consola de UDP.
6. Conéctese a **sqlplus** y confirme que la base de datos está en funcionamiento.

   La base de datos restaurada está operativa con la ubicación alternativa especificada. Sin embargo, después de reiniciar la base de datos, es posible que la base de datos vuelva a la copia anterior o que no se devuelva correctamente debido a un problema conocido. Para evitar más problemas después de la restauración en una ubicación alternativa, se recomienda seguir los siguientes pasos. Estos pasos ayudan a crear o colocar una copia correcta de spfile/pfile.

   a. Vaya a **%ORACLE_HOME%\database** y renombre spfile<SID>.ora.
   b. Conéctese a **sqlplus**.
   c. Vaya al símbolo del sistema SQL y ejecute el siguiente comando:

      sqlplus > create pfile from spfile.
   d. Vaya a **%ORACLE_HOME%\database**, abra **init <SID>.ora** en cualquier editor y, a continuación, haga lo siguiente:

      1. Actualice el valor de "db_create_file_dest" con la ruta especificada para la ubicación restaurada alternativa.
      2. Elimine las barras '\' adicionales del final de la ruta en el parámetro *diagnóstico_dest*.

         Cambie lo siguiente:

         De *diagnostic_dest='E:\app\oracle2\ORA19C280220211833\'*

         A *diagnostic_dest='E:\app\oracle2\ORA19C280220211833'*
      3. Guarde el archivo.
   e. Vaya al símbolo del sistema SQL y ejecute los siguientes comandos:

      Sqlplus > shutdown immediate

      sqlplus > startup

      sqlplus > create spfile from pfile

Nota: Si la base de datos no se inicia desde *spfile*, las restauraciones desde las copias de seguridad correspondientes se limitarán únicamente al nodo original. Para evitarlo, reinicie la base de datos de nuevo después de la creación de *spfile*. Para reiniciar, ejecute los siguientes comandos:

Sqlplus > shutdown immediate

sqlplus > startup

Cómo restaurar la base de datos en un nodo alternativo en Windows

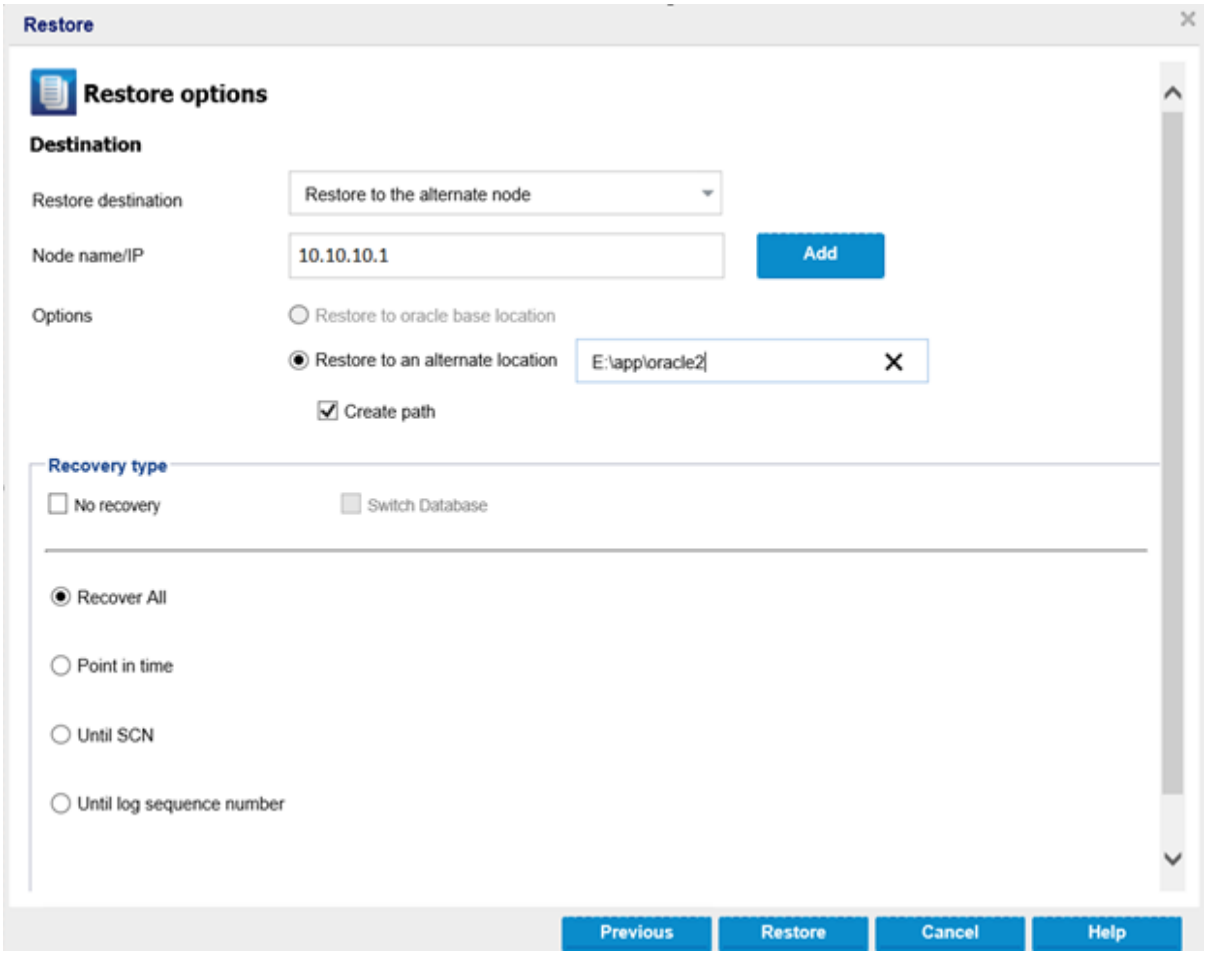
Esta sección proporciona información sobre cómo restaurar la base de datos en un nodo alternativo en Windows.

Notas:

- Cuando se desactiva el **Seguimiento de bloques modificados** y se realiza la restauración en el nodo alternativo, es posible que se produzca un error en la restauración. Por lo tanto, seleccione la opción de solo restaurar cuando tenga los registros necesarios disponibles y pueda recuperar la base de datos manualmente después de la restauración. Como solución alternativa, active **Seguimiento de bloques modificados** antes de realizar la restauración en el nodo alternativo en el nodo de origen.
- Asegúrese de instalar la misma versión del software de Oracle y de crear la base de datos con el mismo SID en el nodo alternativo donde planeaba realizar la restauración como el nodo original (nodo de origen). Por ejemplo, cuando el SID del nodo de origen es orcl, cree orcl en el nodo alternativo antes de iniciar la restauración. Esto es necesario cuando el software de Oracle se instala con la cuenta del dominio. No es necesario mientras se utiliza la cuenta virtual.

Siga estos pasos:

1. En la Consola de UDP, seleccione el punto de recuperación desde el que necesita realizar la restauración. Para obtener más información, consulte Definición de las opciones de restauración.
2. En el cuadro de diálogo Opciones de restauración, en la lista desplegable Destino de la restauración, seleccione **Restaurar en el nodo alternativo**.



3. Para Nombre o dirección IP del nodo, introduzca el nombre de nodo o la dirección IP.
4. En Opciones, seleccione la opción **Restaurar en una ubicación alternativa** y, a continuación, agregue una ruta de la ubicación alternativa.

   Notas:

   - Asegúrese de que la ruta agregada no contenga caracteres especiales ni espacios.
   - La casilla de verificación **Crear ruta** se selecciona automáticamente cuando se selecciona la opción **Restaurar en una ubicación alternativa**.
   - Si la base de datos no se ha cerrado, aparecerá una notificación y se le solicitará que cierre la base de datos. Para confirmar, haga clic en **Aceptar**.
5. Confirme que la tarea de restauración es correcta desde la Consola de UDP.

6. Conéctese a **sqlplus** en el nodo alternativo y confirme que la base de datos está en funcionamiento.

   La base de datos restaurada está operativa con la ubicación alternativa especificada. Sin embargo, después de reiniciar la base de datos, es posible que la base de datos vuelva a la copia anterior o que no se devuelva correctamente debido a un problema conocido. Para evitar más problemas después de la restauración en una ubicación alternativa, se recomienda seguir los siguientes pasos. Estos pasos ayudan a crear o colocar una copia correcta de spfile/pfile.

   a. Vaya a **%ORACLE_HOME%\database** y renombre spfile<SID>.ora.

   b. Conéctese a **sqlplus**.

   c. Vaya al símbolo del sistema SQL y ejecute el siguiente comando:

      sqlplus > create pfile from spfile.

   d. Vaya a **%ORACLE_HOME%\database**, abra **init <SID>.ora** en cualquier editor y, a continuación, haga lo siguiente:

      1. Actualice el valor de "db_create_file_dest" con la ruta especificada para la ubicación restaurada alternativa.

         Ejemplo: **.db_create_file_dest='E:\app\oracle2\ORA19C280220211833'*

      2. Elimine las barras '\' adicionales del final de la ruta en el parámetro *diagnóstico_dest*.

         Cambie lo siguiente:

         De *diagnostic_dest='E:\app\oracle2\ORA19C280220211833\'*

         A *diagnostic_dest='E:\app\oracle2\ORA19C280220211833'*

      3. Guarde el archivo.

   e. Vaya al símbolo del sistema SQL y ejecute los siguientes comandos:

      Sqlplus > shutdown immediate

      sqlplus > startup

      sqlplus > create spfile from pfile

      Nota: Si la base de datos no se inicia desde *spfile*, las restauraciones desde las copias de seguridad correspondientes se limitarán únicamente al nodo original. Para evitarlo, reinicie la base de datos de nuevo después de la creación de *spfile*. Para reiniciar, ejecute los siguientes comandos:

Sqlplus > shutdown immediate

sqlplus > startup

Limitaciones

Se ha comprobado la existencia de las siguientes limitaciones en la versión actual:

- Si se cambia el servidor de puntos de recuperación, la copia de seguridad subsiguiente será una copia de seguridad completa.
- No se admite la restauración a un nodo alternativo si el origen y el destino están en dos versiones diferentes de Oracle.
- Después de actualizar a la versión 8.1, cuando se realiza la tarea de restauración a una ubicación alternativa o a un nodo alternativo, los puntos de recuperación del registro de archivado que se crearon antes de la actualización a la versión 8.0 dejan de ser válidos. Los puntos de recuperación dejan de ser válidos porque no contienen detalles de la asignación de DataFile en la base de datos de Flash según sea necesario.
- Para las restauraciones de registros de archivado a una ubicación alternativa o a un nodo alternativo en la versión 8.1, primero se debe realizar la copia de seguridad incremental (Todos los tipos de datos) y, a continuación, se pueden utilizar las programaciones de registros de archivado subsiguientes para las restauraciones.
- Cuando Oracle Listener se configura en la ubicación no predeterminada, la base de datos de Oracle no aparece automáticamente en la lista de nodos y se debe agregar manualmente durante la creación del plan.
- La opción Pausar/Reanudar no está disponible en el menú Nodo para los nodos de Oracle.
- Oracle no admite el espacio de tabla si el nombre del espacio de tabla contiene el signo de dólar ($) en Oracle 19c.
- No se admite la restauración granular cuando la base de datos de Oracle se instala mediante una cuenta virtual.
- UDP 8.1 no admite la copia de seguridad de bases de datos de diferentes versiones de Oracle instaladas en el mismo servidor.
- Recuperación de tablas según las limitaciones de Oracle:
    - Las tablas creadas desde el espacio de tabla SYSTEM y SYSAUX no se pueden recuperar.

- Las tablas creadas desde el sistema o desde el usuario del sistema no se pueden recuperar.

- El servidor de puntos de recuperación actúa como agente de copia de seguridad, restauración y recuperación asegurada.
- Para Standard Edition, solo se admite la restauración de la base de datos completa con la opción Recuperar todo y a un momento determinado (PIT) desde los puntos de recuperación más recientes e intermedios.
- Para Standard Edition, se admite la restauración del espacio de tabla con la opción Recuperar todo desde el último punto de recuperación y la cláusula UNTIL no es compatible con el script RMAN.
- Para Standard Edition, Oracle no admite las restauraciones a nivel de tabla.
- Después de una restauración completa de la base de datos, la siguiente copia de seguridad incremental se convertirá automáticamente en una copia de seguridad completa.
- Si el tamaño de la protección contra escritura cambia, la siguiente copia de seguridad será una copia de seguridad completa.
- El número máximo de canales admitidos es 10.

Capítulo 5: Protección del entorno de Microsoft SharePoint

Esta sección incluye los siguientes temas:

Consideraciones sobre la instalación para el entorno de Microsoft SharePoint

Este tema proporciona la información que necesita para instalar y configurar al agente de Arcserve UDP en entornos de Microsoft SharePoint. La información de esta sección presupone un conocimiento de las características y requisitos del conjunto de servidores de Microsoft SharePoint.

Consideraciones acerca del entono

Los entornos SharePoint pueden ser complejos y estar distribuidos entre varios equipos. Microsoft debe soportar la configuración de conjuntos de servidores. Por ejemplo, un entorno SharePoint distribuido debería tener los siguientes componentes:

- Uno o más servidores Web de cliente.
- Uno o más servidores de base de datos utilizados por el conjunto de SharePoint Server.
- En la mayoría de los casos, SharePoint está instalado en un entorno de dominio. Habrá uno o varios servidores DNS y controladores de dominio.

Consideraciones sobre la instalación

Tenga en cuenta la siguiente información cuando instale los agentes:

- SharePoint es un entorno distribuido. Es recomendable instalar al Agente de UDP en cada servidor de la granja de SharePoint, incluidos los servidores web de cliente y servidores de base de datos.
- Se recomienda también proteger todo el entorno de dominio, incluido el controlador de dominio y servidor DNS. Estos elementos son necesarios para restaurar la granja, la configuración de la granja y la aplicación web.

Cómo realizar copias de seguridad de servidores de Microsoft SharePoint

Se pueden realizar copias de seguridad de los servidores de Microsoft SharePoint mediante Arcserve UDP. Para asegurarse de que la opción de restauración funciona como se espera, se recomienda proteger todo el equipo, y no volúmenes seleccionados en todos los servidores de SharePoint.

Para los servidores de controlador de dominios y de DNS, siempre que los servicios de dominio y de DNS funcionen correctamente después de que la máquina virtual de la instancia los inicie, puede realizar copias de seguridad de los volúmenes seleccionados.

- Revisión de las consideraciones
- Creación de una copia de seguridad del servidor de SharePoint

Revisión de las consideraciones

Se recomienda agregar todos los servidores, incluidos los servidores web de cliente, los servidores de base de datos, los controladores de dominio y los servidores DNS, a un plan con la misma programación de copia de seguridad. Como resultado, se realiza la copia de seguridad de todos los servidores prácticamente al mismo tiempo. Esto es muy importante en un entorno distribuido. Al realizar una restauración, se puede obtener el mismo resultado de los puntos de recuperación cuya copia de seguridad se realice al mismo tiempo en todos los servidores.

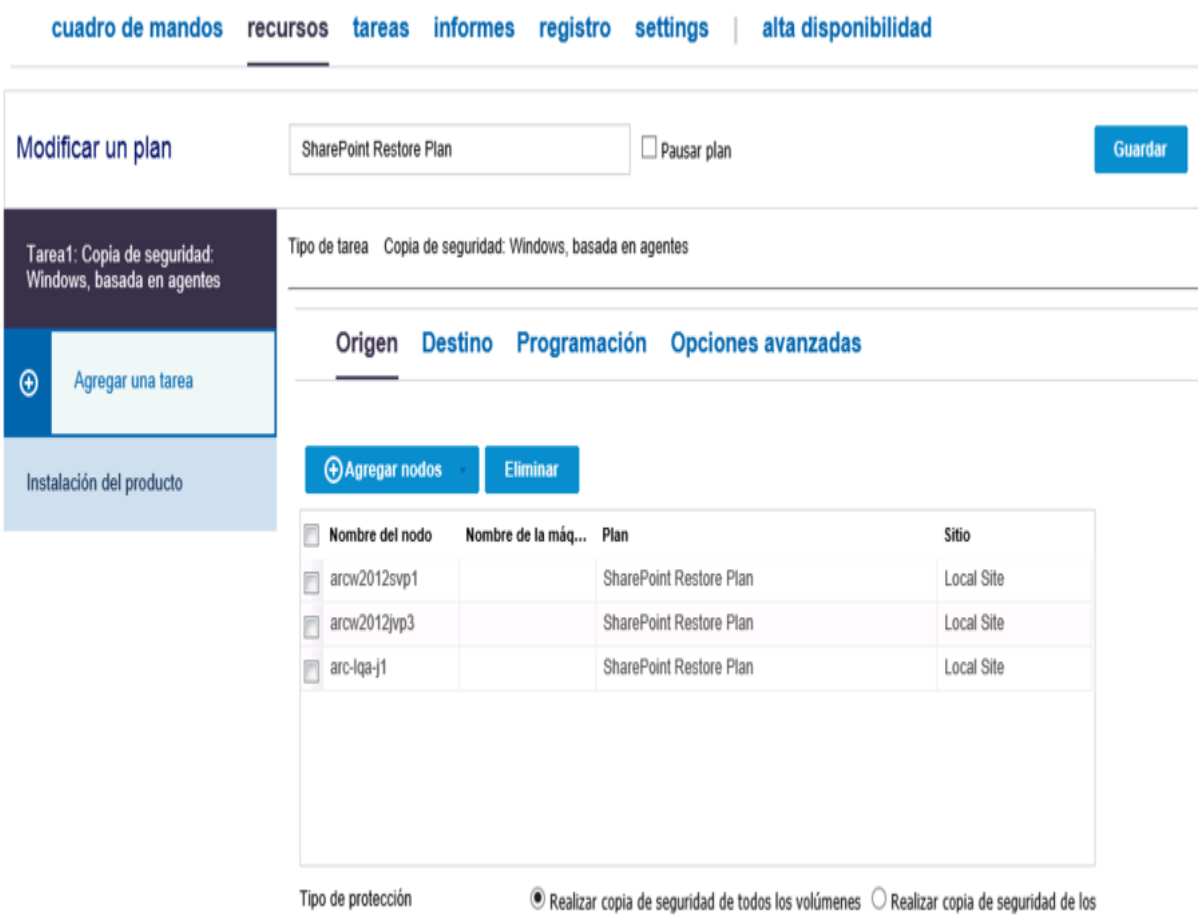
Nota: Si se ha cambiado la topología de la granja de SharePoint, se agregan nuevos servidores para mejorar el equilibrio de carga de SharePoint. Se deben agregar los nuevos servidores inmediatamente al mismo plan.

Creación de una copia de seguridad del servidor de SharePoint

Utilice la Consola de Arcserve UDP para realizar la copia de seguridad del nivel de base de datos en el entorno de SharePoint.

Siga estos pasos:

1. Inicie sesión en la Consola.
2. Haga clic en **Recursos** y vaya a **Nodos** en el panel de **navegación** izquierdo.
3. Haga clic en **Todos los nodos**.
4. Agregue todos los nodos en el entorno de granja de SharePoint.
5. (Opcional) Cree un almacén de datos.
6. Expanda **Planes** en el panel de **navegación** y haga clic en **Todos los planes**.
7. Haga clic en **Agregar** para crear un nuevo plan.
8. En la ficha **Origen**, agregue todos los nodos que se encuentren en el entorno de la granja de SharePoint.



9. Configure otros valores de configuración y guarde el plan.

   Se crea el plan para el entorno de la granja de SharePoint. Los valores de configuración del plan se implementa en todos los nodos. La tarea de copia de seguridad se inicia a la hora programada.

   Se puede iniciar manualmente la tarea de copia de seguridad haciendo clic en Realizar copia de seguridad ahora. Se inicia la tarea de copia de seguridad en todos los nodos de la granja de SharePoint. Los datos se guardan en el mismo almacén de datos.


cuadro de mandos
recursos
tareas
informes
registro
settings
alta disponib
Exploración
Nodos
Todos los nodos
Nodos sin un plan
Grupos de vCenter/ESX
Grupos de Hyper-V
Grupos de planes
Nuevo plan Agent
Nuevo plan Agentless
Plan de protección 1
SharePoint Restore Plan
Grupos del proxy de c
Grupos de servidores
Destinos
Planes
Infrastructure
Nodos: SharePoint Restore Plan
Acciones
Agregar nodos
Filtrar
(Ningún filtro aplicado)
Estado
Nombre del nodo
Plan
arc-lqa-j1
SharePoint Restore Plan
arcw2012jvp3
SharePoint Restore Plan
arcw2012svp1
SharePoint Restore Plan
Realizar copia de seguridad ahora
Cancel Backup
Exportar nodos

Cómo restaurar un entorno de SharePoint

Se admiten las siguientes restauraciones de granularidades:

- Granja
- Granja solo con configuración
- Servicios de SharePoint
- Aplicaciones web
- Base de datos de contenido
- Recopilaciones de sitios
- Sitios
- Listas
- Elementos de lista (incluidos documentos)

Se restauran granularidades diferentes si se usan soluciones diferentes:

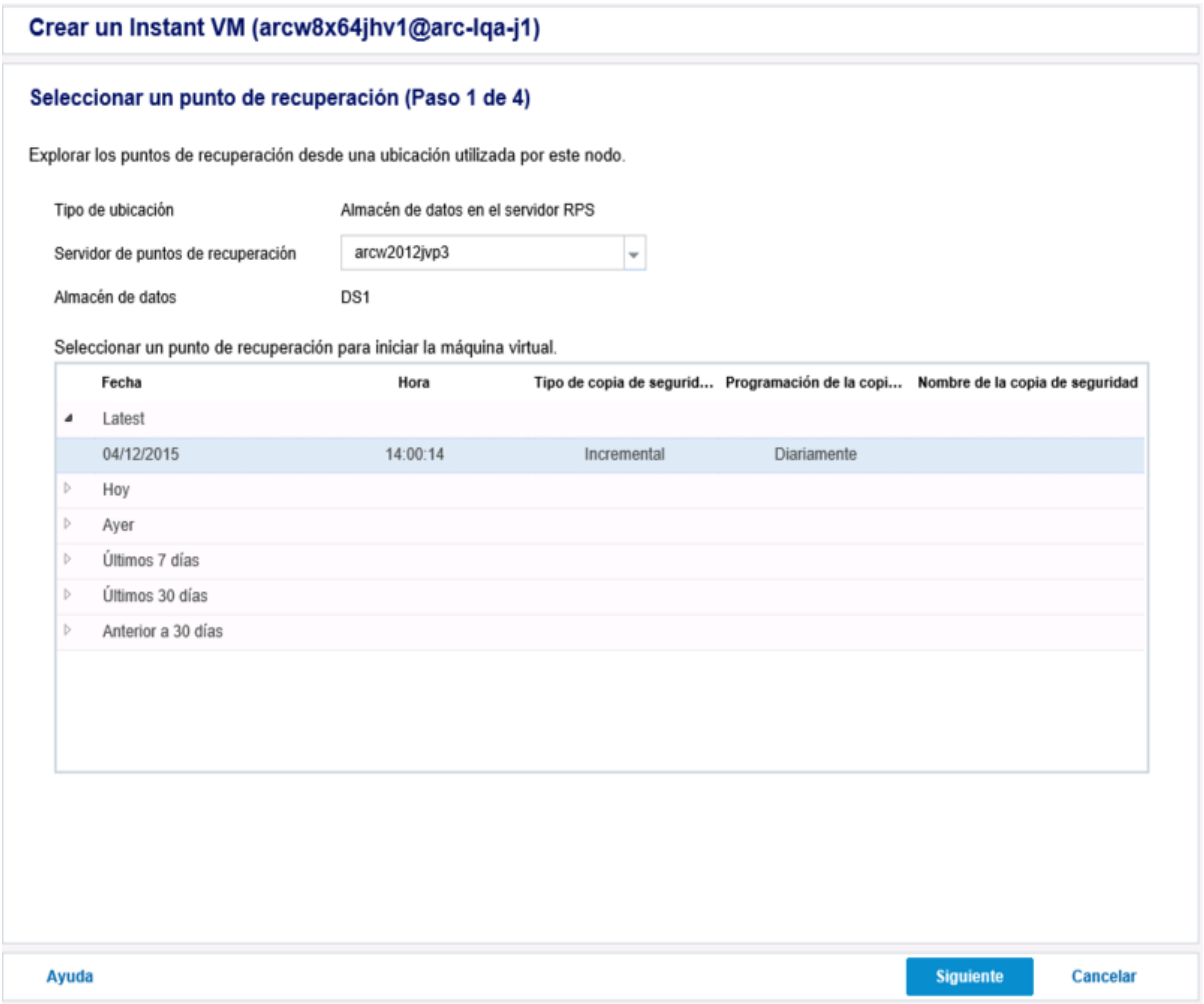
- Restauración utilizando la máquina virtual instantánea: Es compatible con Granja, Granja solo con configuración, Servicios de SharePoint y Aplicaciones web.
- Restauración utilizando la interfaz de usuario del Agente de Arcserve UDP: Es compatible con las bases de datos de contenido.
- Restauración utilizando la base de datos de montaje del punto de recuperación: Es compatible con Recopilaciones de sitios, Sitios, Listas y Elementos de lista.

Restauración mediante máquina virtual instantánea

Siga estos pasos:

1. Inicie sesión en la Consola.
2. Haga clic en **Recursos**, **Nodos**.
3. Haga clic con el botón secundario del ratón en el nodo que se encuentra en el plan para el entorno de SharePoint.
4. Haga clic en **Create an Instant VM (Crear una máquina virtual instantánea)** para crear máquinas virtuales instantáneas para el equipo del entorno de SharePoint.

   Se abre el asistente **Create an Instant VM (Crear una máquina virtual instantánea)**.
5. Examine los puntos de recuperación desde una ubicación y seleccione un punto de recuperación para iniciar la instantánea de la máquina virtual.

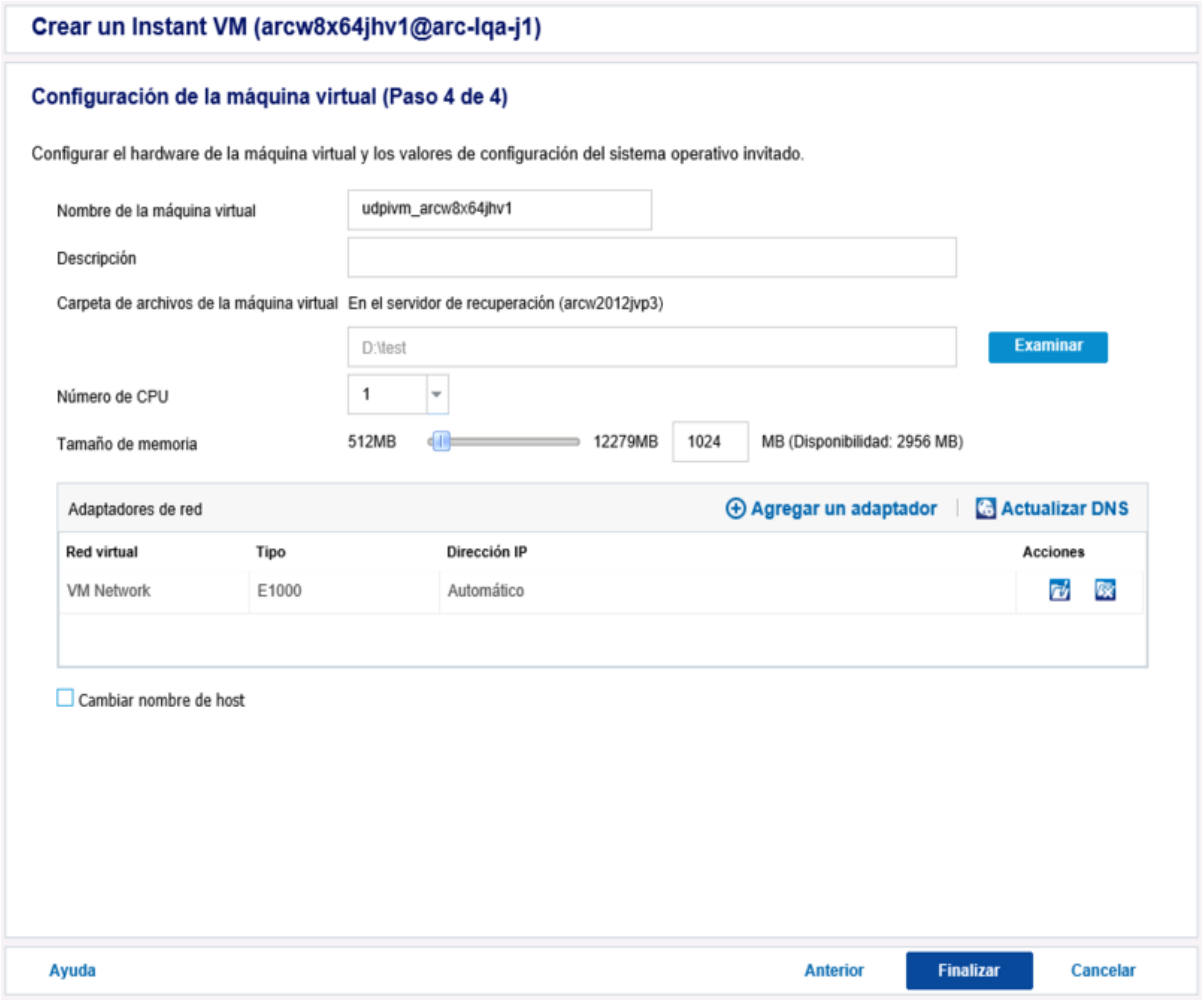


6. Haga clic en **Siguiente**.

7. Especifique una ubicación en VMware vSphere o Microsoft Hyper-V para hospedar la máquina virtual instantánea. Por ejemplo: El tipo de hipervisor es VMware vSphere.
8. Haga clic en **Siguiente**.
9. Especifique un equipo para ejecutar la máquina virtual instantánea.

   Por ejemplo, utilice el servidor puntos de recuperación actual.
10. Haga clic en **Siguiente**.
11. Establezca los valores de configuración del sistema y del hardware de la máquina virtual instantánea.
12. Cree una nueva red virtual como un entorno de red aislado para la recuperación de SharePoint. Para obtener más información sobre cómo crear un entorno de red aislado, consulte Creación de una red aislada para la recuperación de SharePoint.
13. Haga clic en el icono del signo más para agregar un adaptador de red.
14. Seleccione la red virtual correcta, que es un entorno de red aislado para la recuperación de SharePoint, y utilice la configuración predeterminada de los valores de configuración de TCP/IP "Origen:XXX.XXX.XXX.XXX".

    Importante: Al crear una máquina virtual instantánea para un equipo que utiliza servidores cliente web para el entorno de SharePoint, se debe agregar un adaptador de red adicional para transferir el archivo de datos de la copia de seguridad. La dirección IP del nuevo adaptador debe ubicarse en la misma red virtual con los servidores cliente web originales para SharePoint y en el mismo segmento IP. A continuación, el entorno de SharePoint original puede utilizar el adaptador de red para acceder a cualquier carpeta compartida con la máquina virtual instantánea.



15. Haga clic en **Finalizar**.

    Se abre el cuadro de diálogo Arrancar máquina virtual.

16. Haga clic en **Iniciar más tarde**.

    Se crea una nueva máquina virtual instantánea que aparece en la sección **Infraestructuras**, **Máquinas virtuales instantáneas** de la Consola.

17. Cree la máquina virtual instantánea para todos los nodos del entorno de granja de SharePoint.

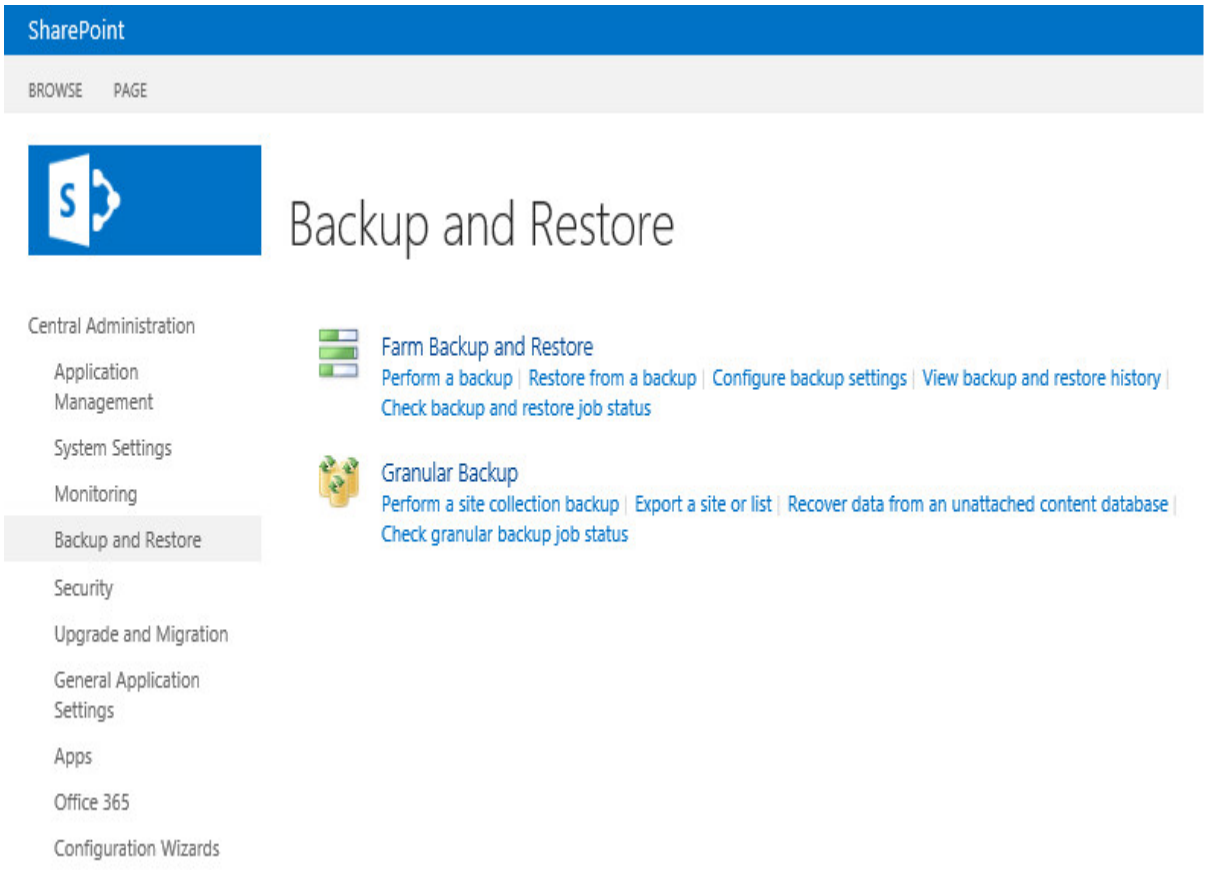
18. Una vez creadas las máquinas virtuales instantáneas de todos los nodos, inícielas una a una.

    - Inicie primero el Controlador de dominio y, a continuación, el Servidor DNS.
    - Después, inicie el Servidor de la base de datos y, por último, los servidores cliente web.

19. Haga clic con el botón secundario del ratón en la máquina virtual de instantánea que se desea iniciar y seleccione **Encender** para iniciar la máquina virtual instantánea.
20. Espere a que se hayan encendido las máquinas virtuales instantáneas para los equipos del entorno de SharePoint..

    El entorno de SharePoint temporal se ha configurado.
21. Inicie sesión en la máquina virtual instantánea en la que el equipo utiliza los servidores cliente web para el entorno de SharePoint. Abra Administración Central, haga clic en el encabezado Copias de seguridad y restauración y seleccione el vínculo Realizar copia de seguridad.

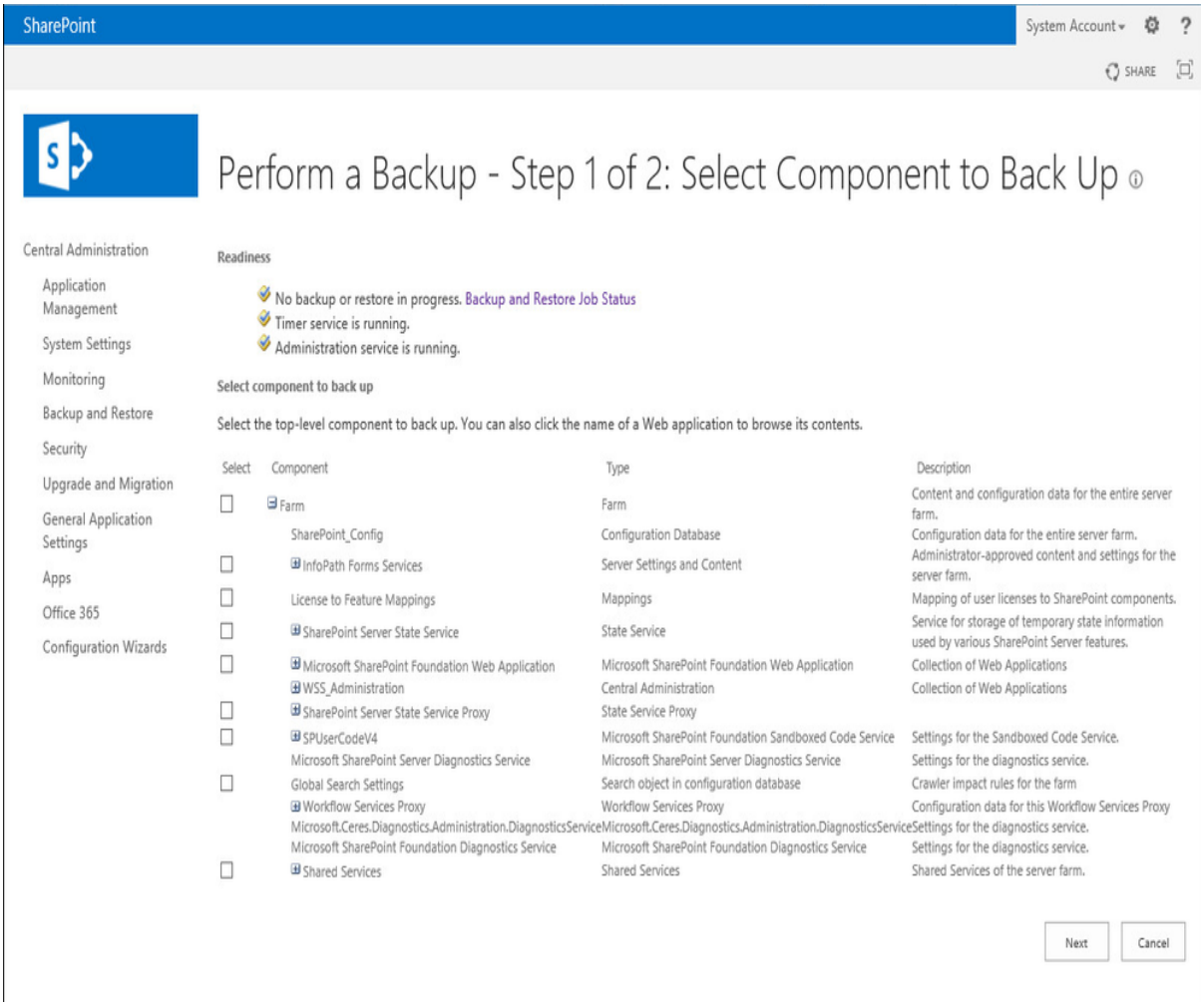
    Nota: Si aparece el error HTTP 404 tras abrir la aplicación web, como Sharepoint - 80, desactive IPv6 y anule la selección de la casilla de verificación **Protocolo de Internet versión 6 (TCP/IP)** en la ventana Propiedades de la red de área local.



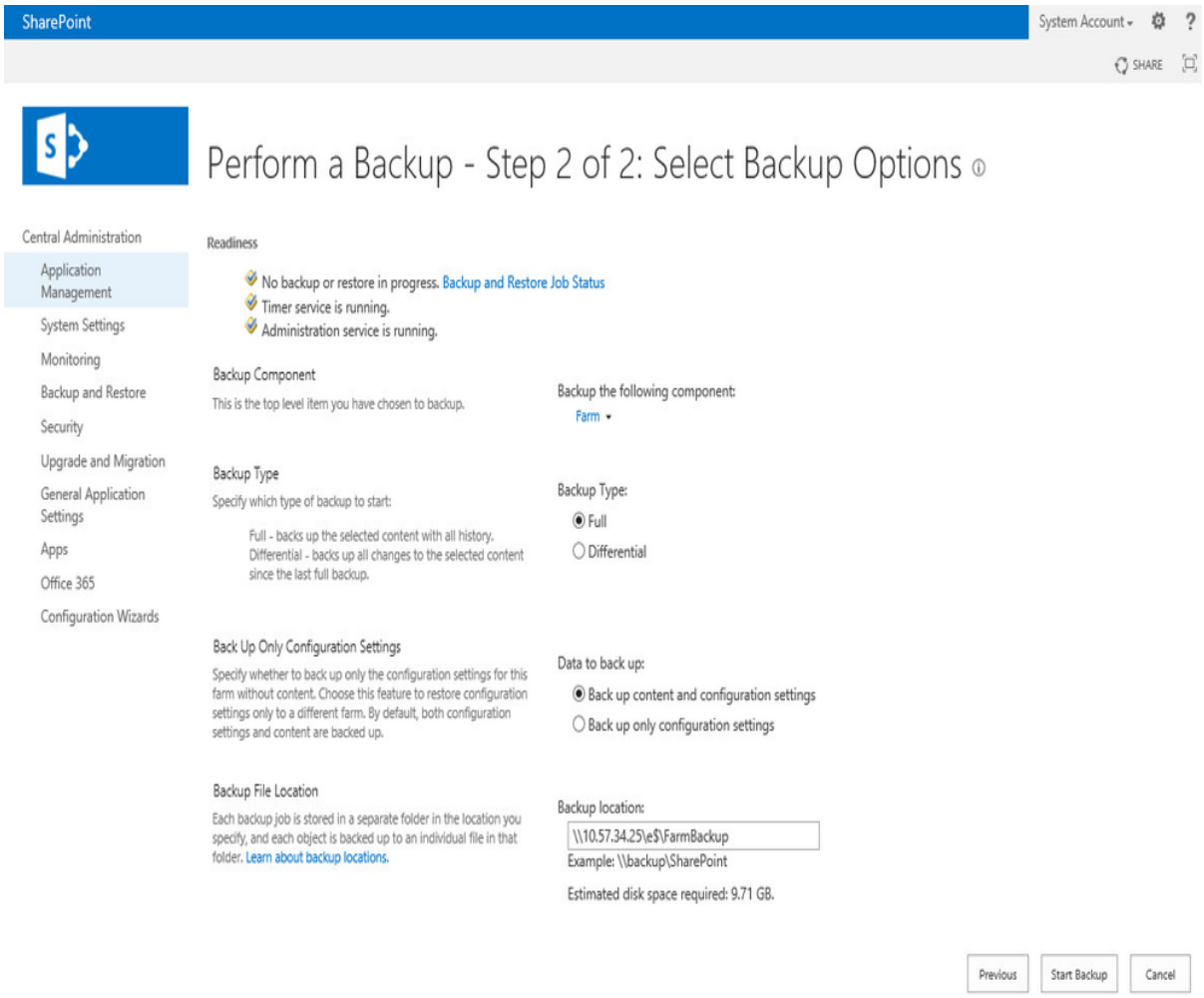
22. Seleccione el componente que desee restaurar para la granja y haga clic en **Siguiente**.

Por ejemplo, Copia de seguridad de las aplicaciones web de SharePoint – 80. Expanda el nodo Aplicación web de Microsoft SharePoint Foundation y seleccione el componente SharePoint – 80

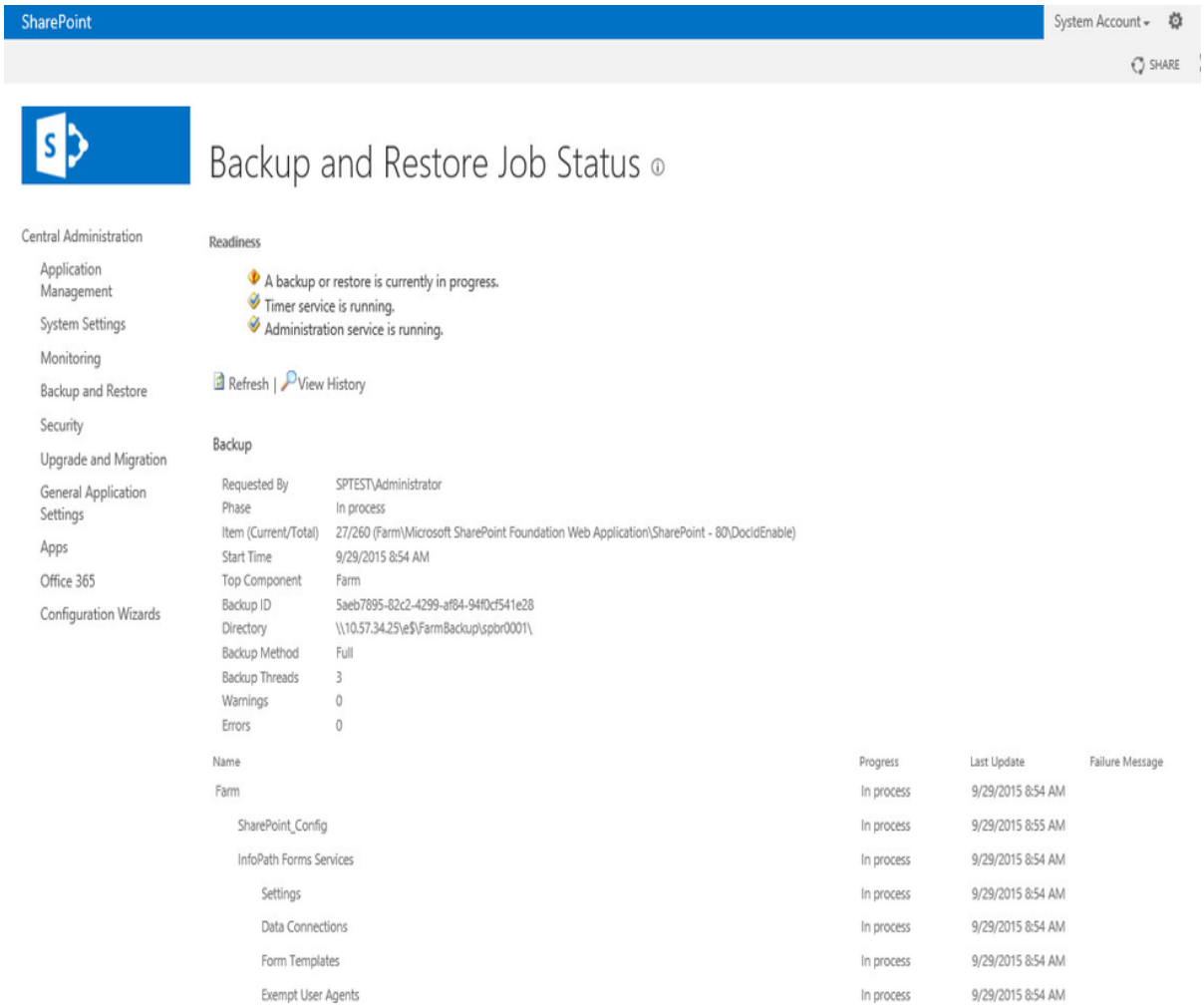
Realizar copia de seguridad de los servicios de acceso. Expanda el nodo Aplicaciones de servicios compartidos bajo Servicios compartidos y seleccione el componente Servicios de Access 2010



23. Especifique el tipo de copia de seguridad como Completa.
24. Cree una carpeta compartida en la máquina virtual instantánea, en la que el equipo utilice los servidores cliente web para el entorno de SharePoint.
25. Proporcione el acceso Control total a todos los usuarios de la carpeta compartida.
26. Proporcione la ruta a la carpeta compartida en Ubicación de archivo de copia de seguridad para almacenar el archivo de copia de seguridad y, a continuación, haga clic en **Iniciar copia de seguridad**.

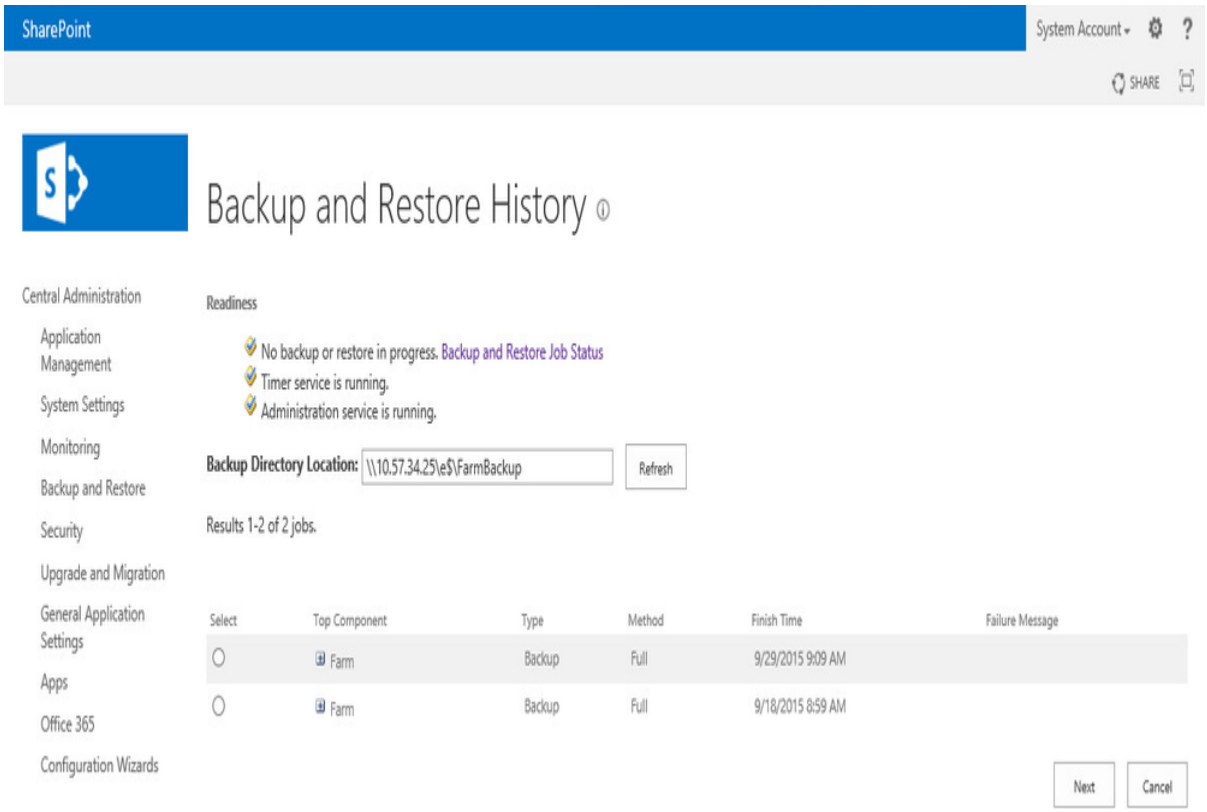


27. Espere hasta que la tarea de copia de seguridad se haya completado.



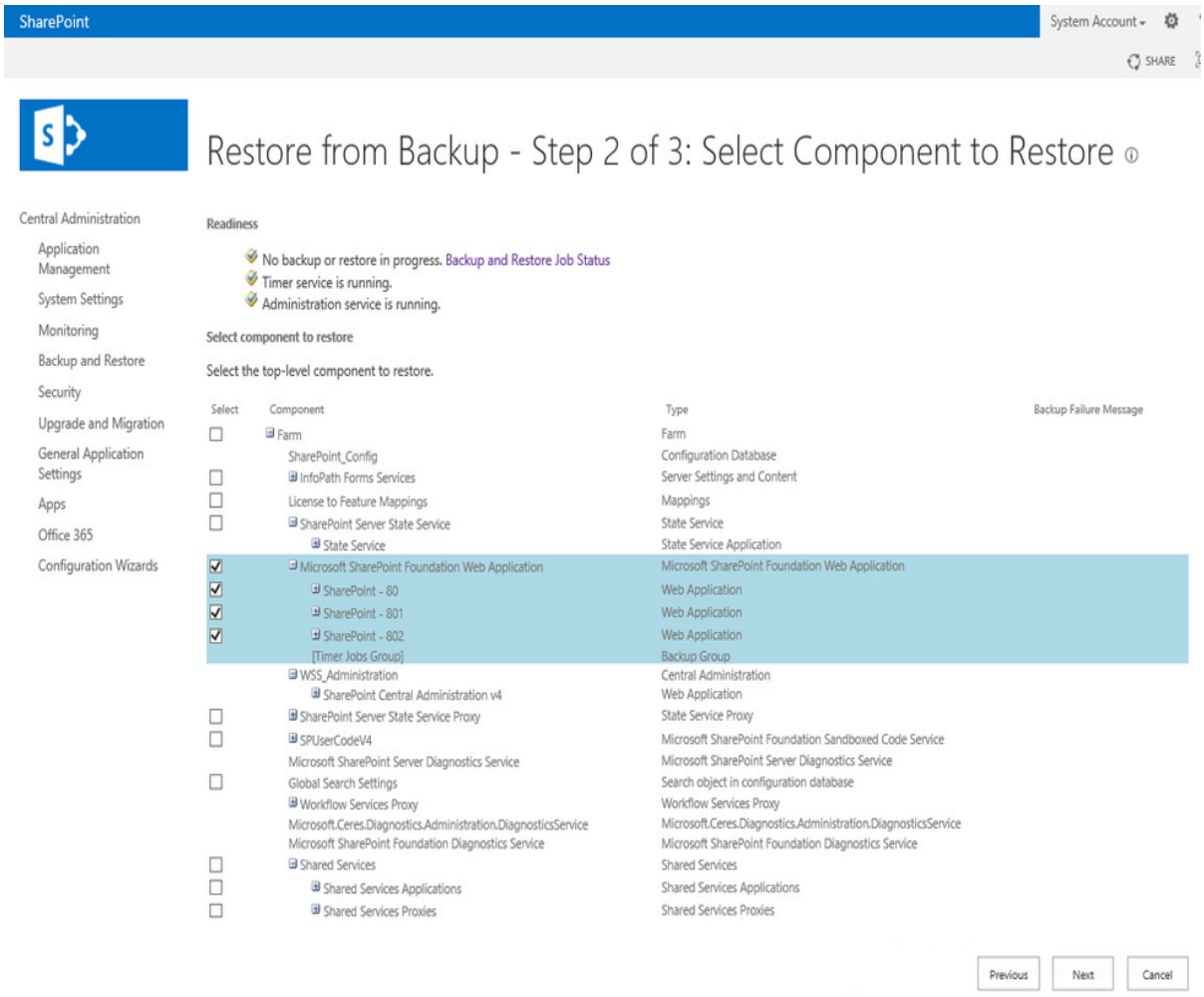
28. Una vez que la tarea de copia de seguridad de la granja haya finalizado, inicie sesión en el equipo de los servidores cliente web para el entorno de SharePoint original.
29. Abra Administración Central, haga clic en Copias de seguridad y restauración y seleccione el vínculo Restaurar a partir de una copia de seguridad.
30. Especifique la carpeta compartida en el campo Ubicación del directorio de copia de seguridad y haga clic en **Actualizar**.

    Nota: La carpeta compartida ya se ha creado en uno de los pasos anteriores.
31. Seleccione la instancia de la copia de seguridad de la lista del historial y haga clic en el botón **Siguiente**.



32. Seleccione la configuración y el contenido de la granja para restaurar y, a continuación, haga clic en **Siguiente**.

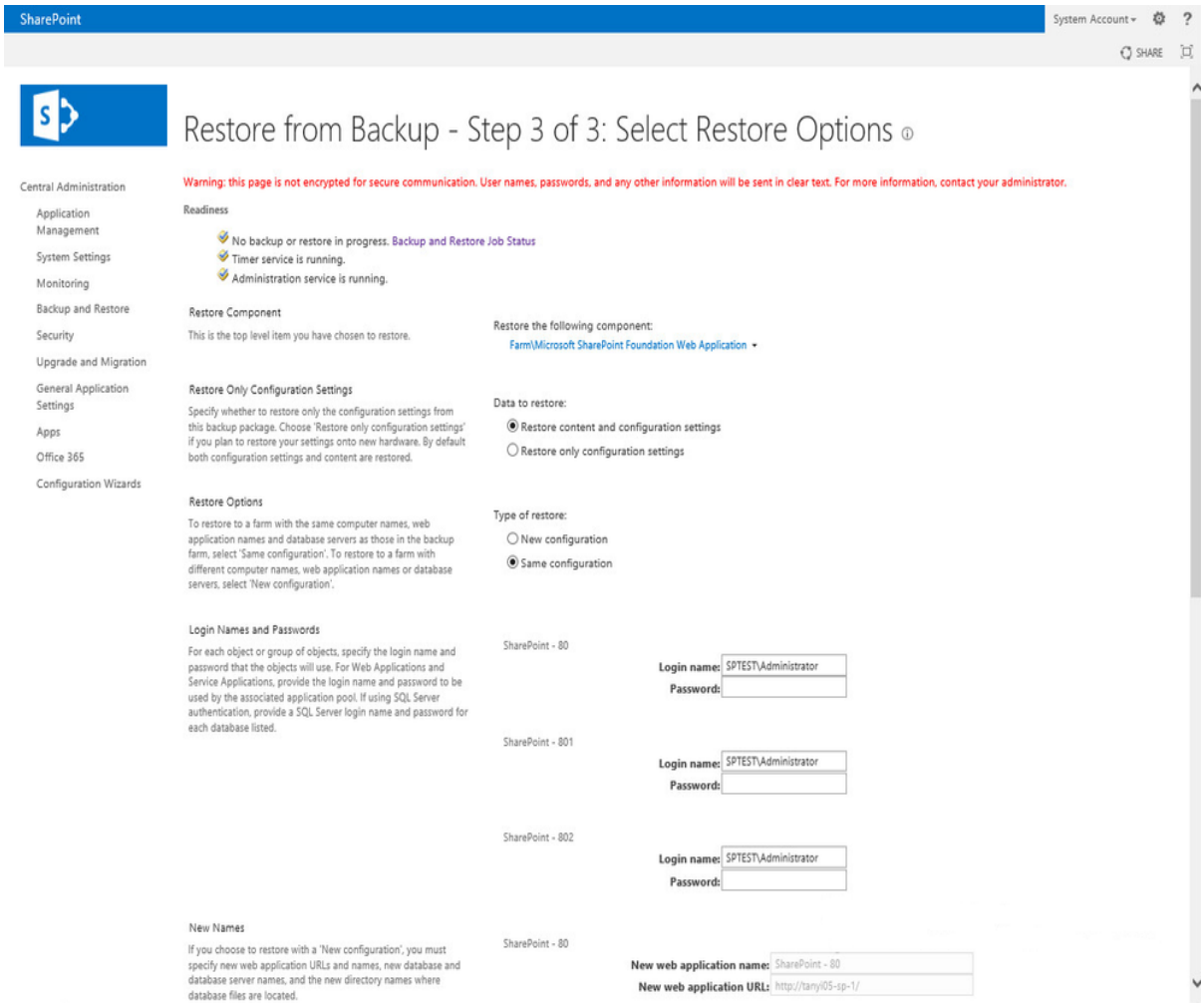
    Por ejemplo, seleccione todos los componentes Granja, Servicios de SharePoint o Aplicaciones web.



La página muestra varias opciones para la configuración del servicio y del contenido seleccionada.

33. Decida si desea:

- restaurar el contenido y la configuración o restaurar la configuración únicamente.
- sobrescribir la configuración o crear nuevas opciones de restauración.



34. Haga clic en el botón **Iniciar restauración** para comenzar el proceso de restauración.

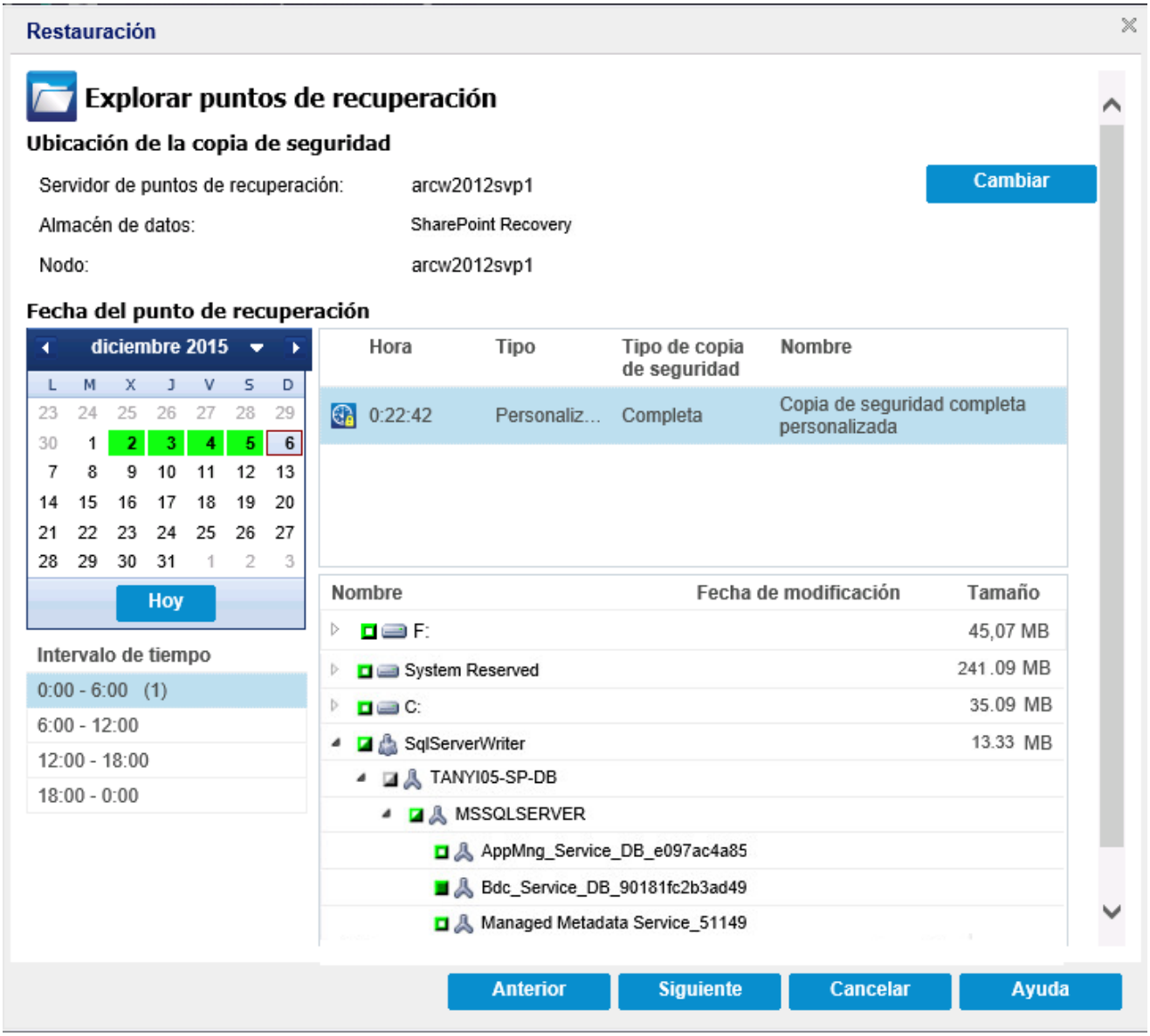
    Una vez que se ha completado la tarea de restauración, se restauran los componentes seleccionados de la granja.

Restauración mediante la interfaz de usuario del Agente de Arcserve UDP

Siga estos pasos:

1. Inicie sesión en la consola.
2. Haga clic con el botón secundario en el nodo que sea el servidor de base de datos utilizado por SharePoint.
3. Haga clic en el botón Restaurar.

   Se abrirá la interfaz de usuario del Agente de Arcserve UDP hospedado en el servidor de base de datos.
4. Seleccione Explorador de puntos de recuperación
5. Haga clic en el punto de recuperación que contenga la base de datos que se desee restaurar.
6. Seleccione la base de datos en SqlServerWriter/{nombreDeServidorSQL}/{nombreInstantáneasServidorSQL} para restaurar.
7. Haga clic en Siguiente.



8. Seleccione el destino de la restauración y haga clic en Siguiente.

   Si selecciona Restaurar en la ubicación original, la base de datos se restaurará en la ubicación original. Si selecciona Restaurar en una ubicación alternativa, la base de datos se restaurará en la ubicación especificada. La base de datos restaurada se adjuntará automáticamente a SQL Server. Si selecciona Solo archivo de vaciado, el archivo de datos de la base de datos y el archivo de registro se guardan en la ubicación especificada.

9. Haga clic en Finalizar y espere a que termine la tarea de restauración.

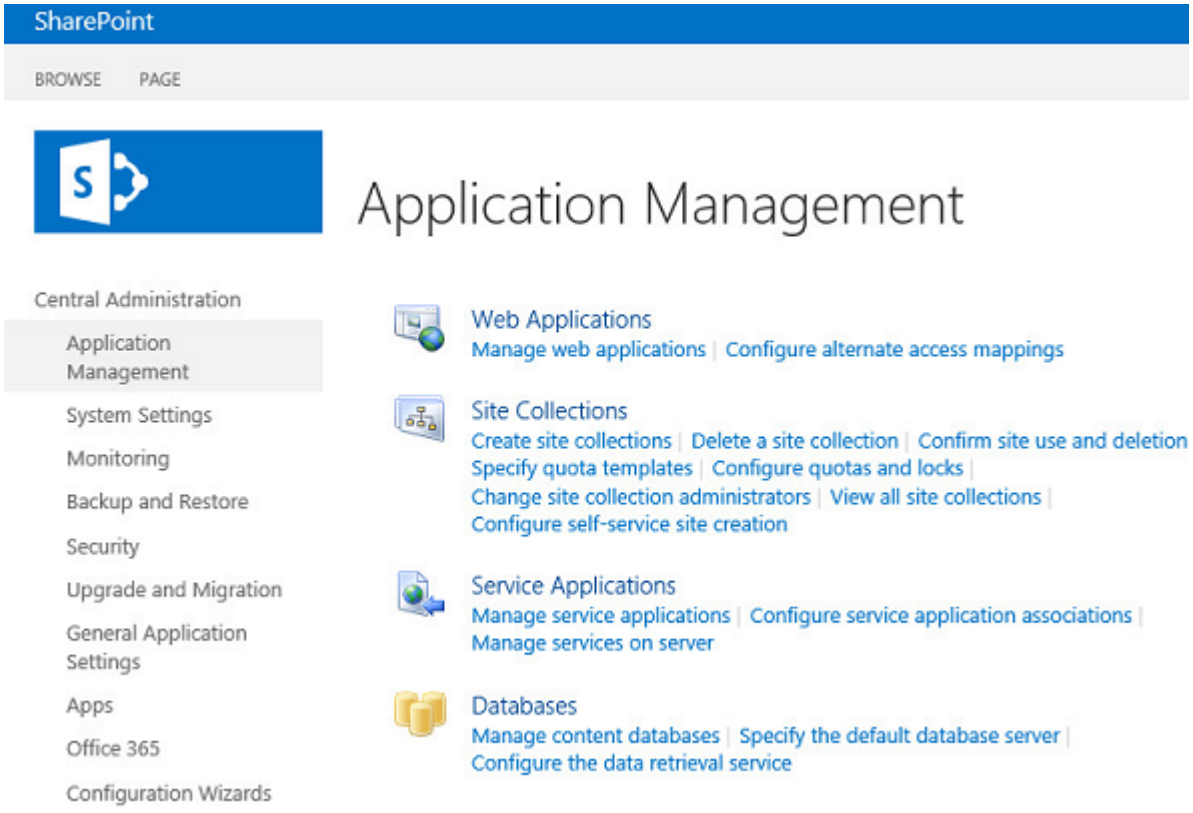
   Nota: Después de seleccionar Solo archivo de vaciado, adjunte primero la base de datos. Siga los pasos descritos en Restauración mediante una base de datos montada desde un punto de recuperación y compruebe si la base de datos con con-

tenido nuevo está asociada a su aplicación web original. De lo contrario, agregue la base de datos con contenido restaurado a la aplicación web original.

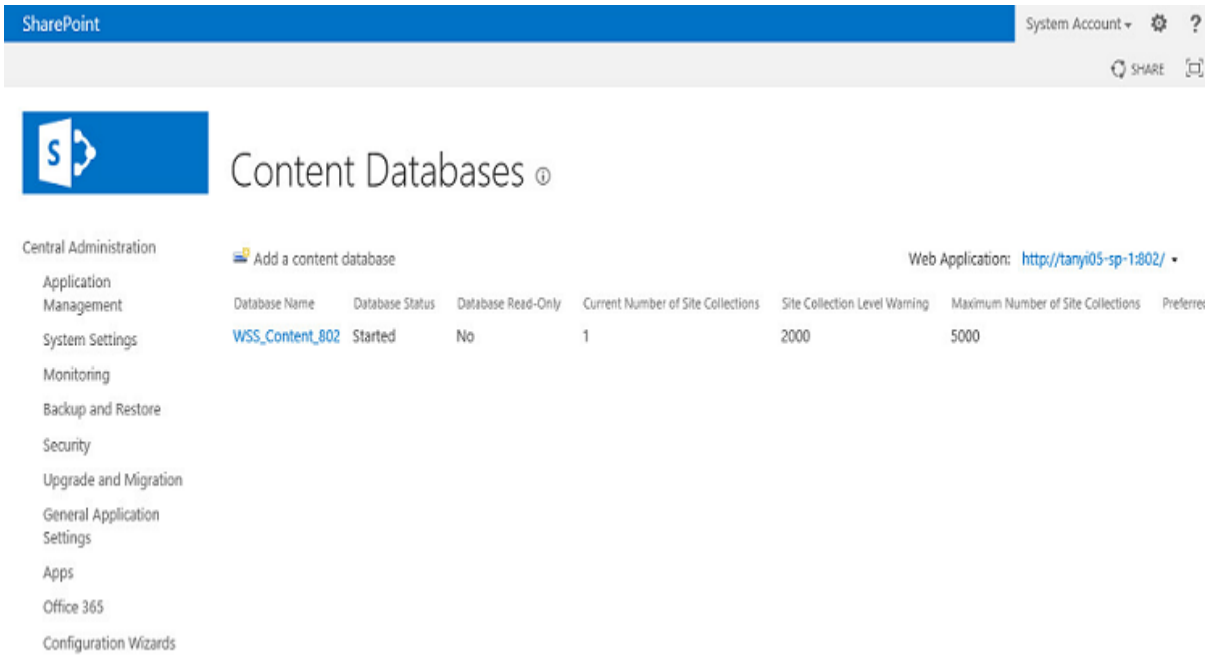
Adición de la base de datos de contenido restaurado a la aplicación web original

Siga estos pasos:

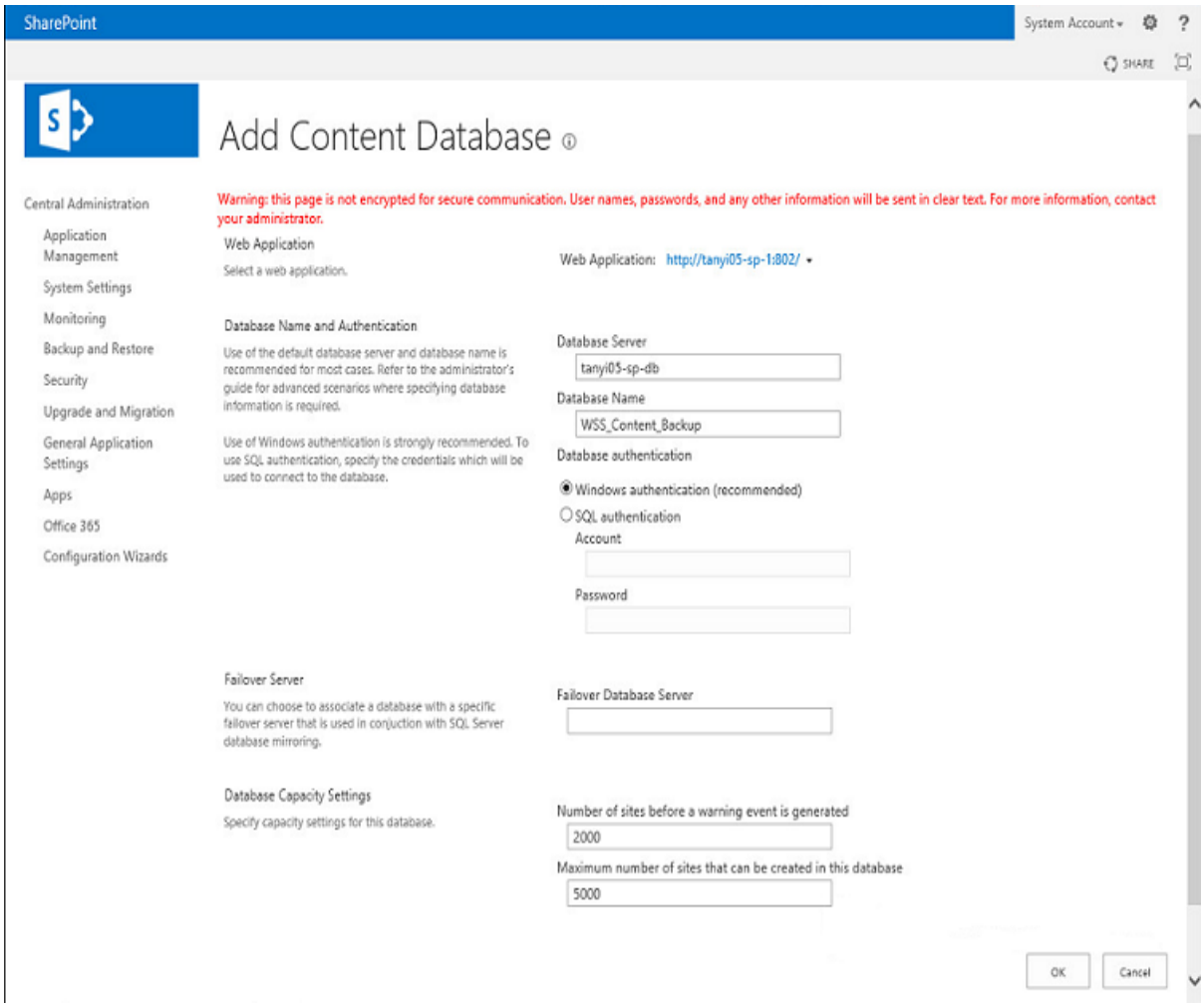
1. Abra la Administración central de SharePoint y seleccione Administración de aplicaciones.



2. Seleccione Administrar bases de datos de contenido.



3. Seleccione la aplicación web y haga clic en Agregar una base de datos de contenido.
4. Escriba el nombre y el servidor de la base de datos (por ejemplo, WSS_Content_ Backup) y haga clic en Aceptar.

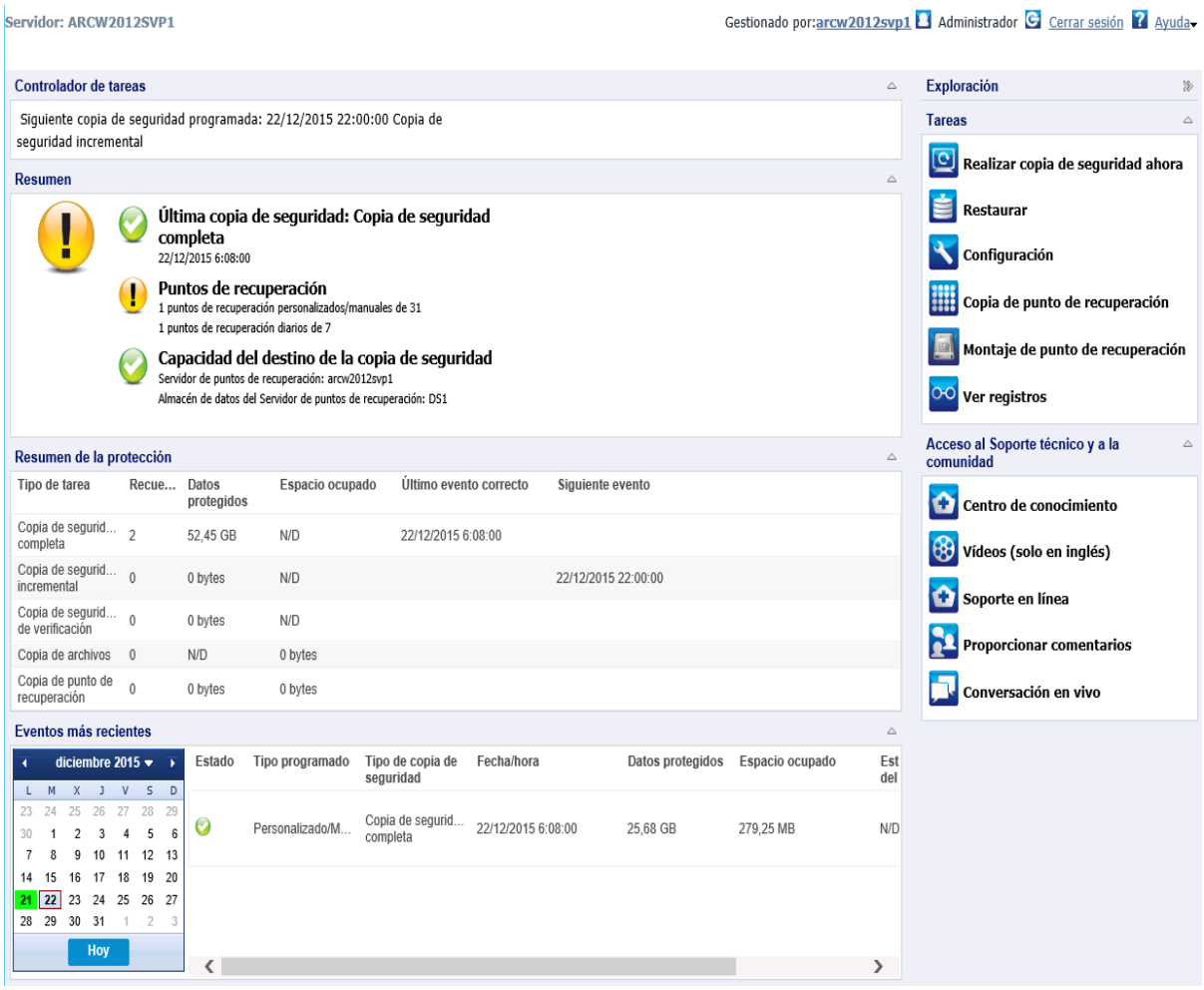


La base de datos de contenido estará ahora asociada a su aplicación web original.

Restauración mediante el montaje de la base de datos desde el punto de recuperación

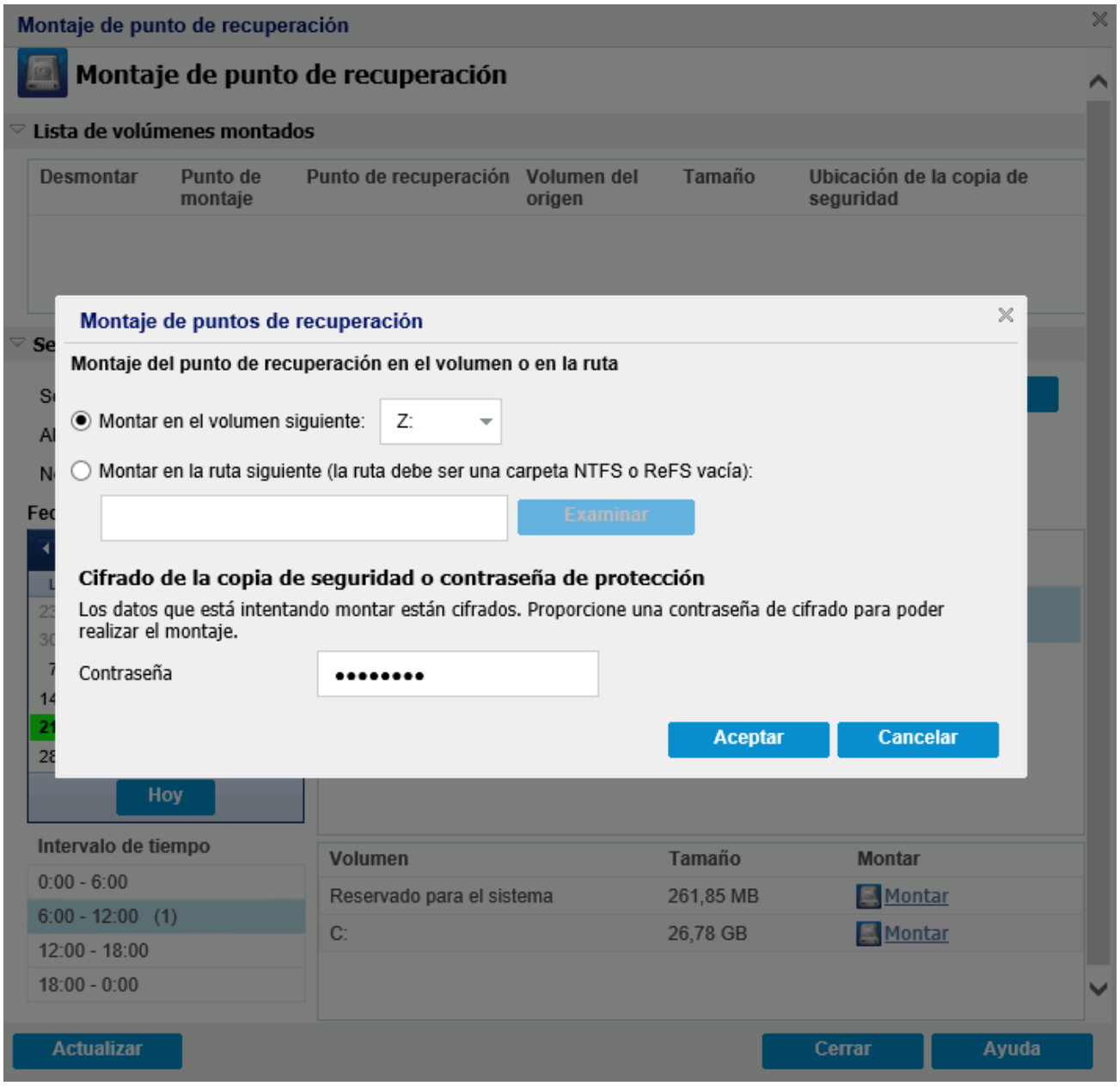
Siga estos pasos:

1. Abra la interfaz de usuario del Agente de Arcserve UDP que está alojado en el servidor de la base de datos.

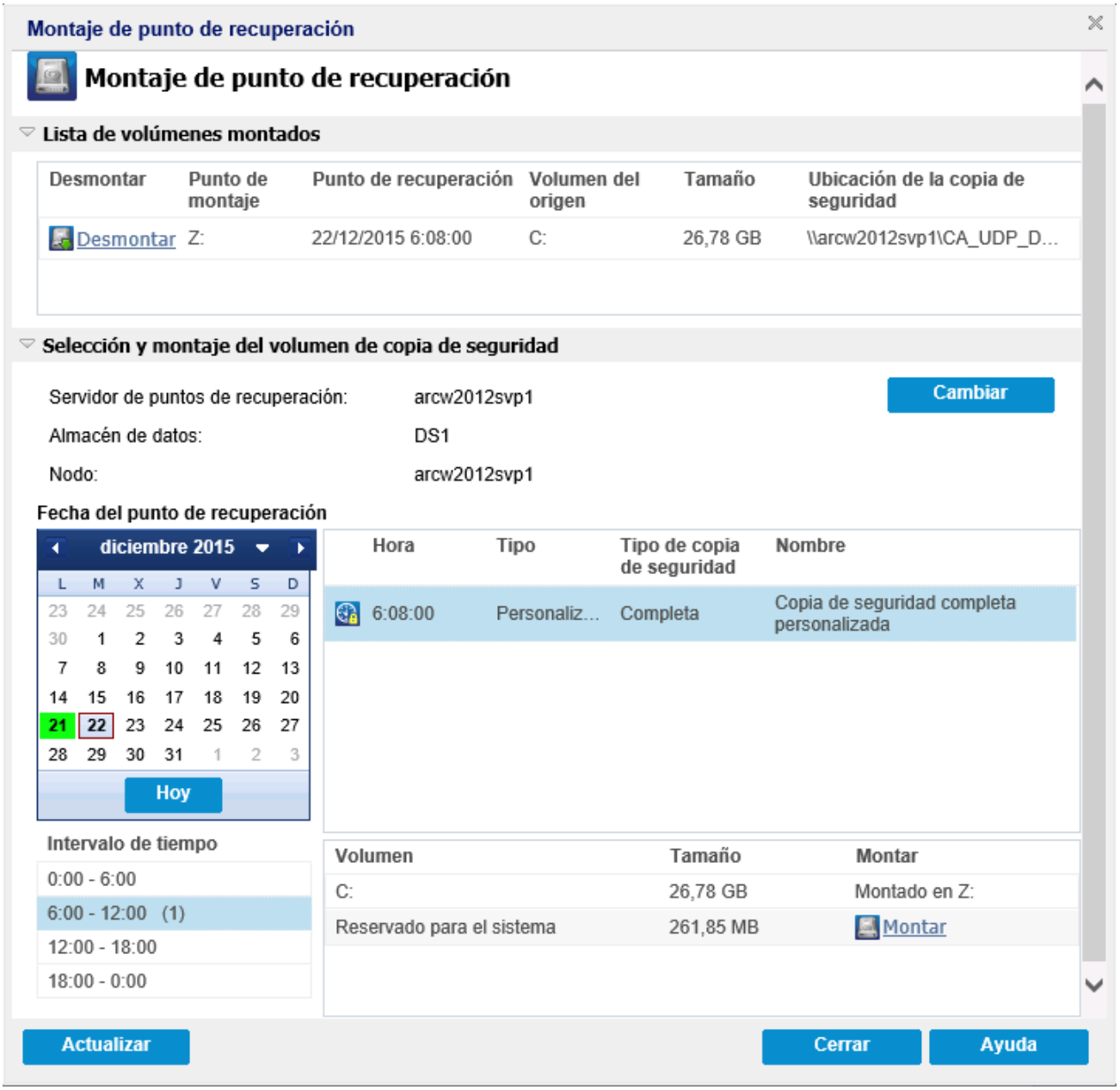


2. Haga clic en **Montar punto de recuperación** en el panel Tareas.
3. Seleccione el volumen que incluye la base de datos de SQL Server para SharePoint.

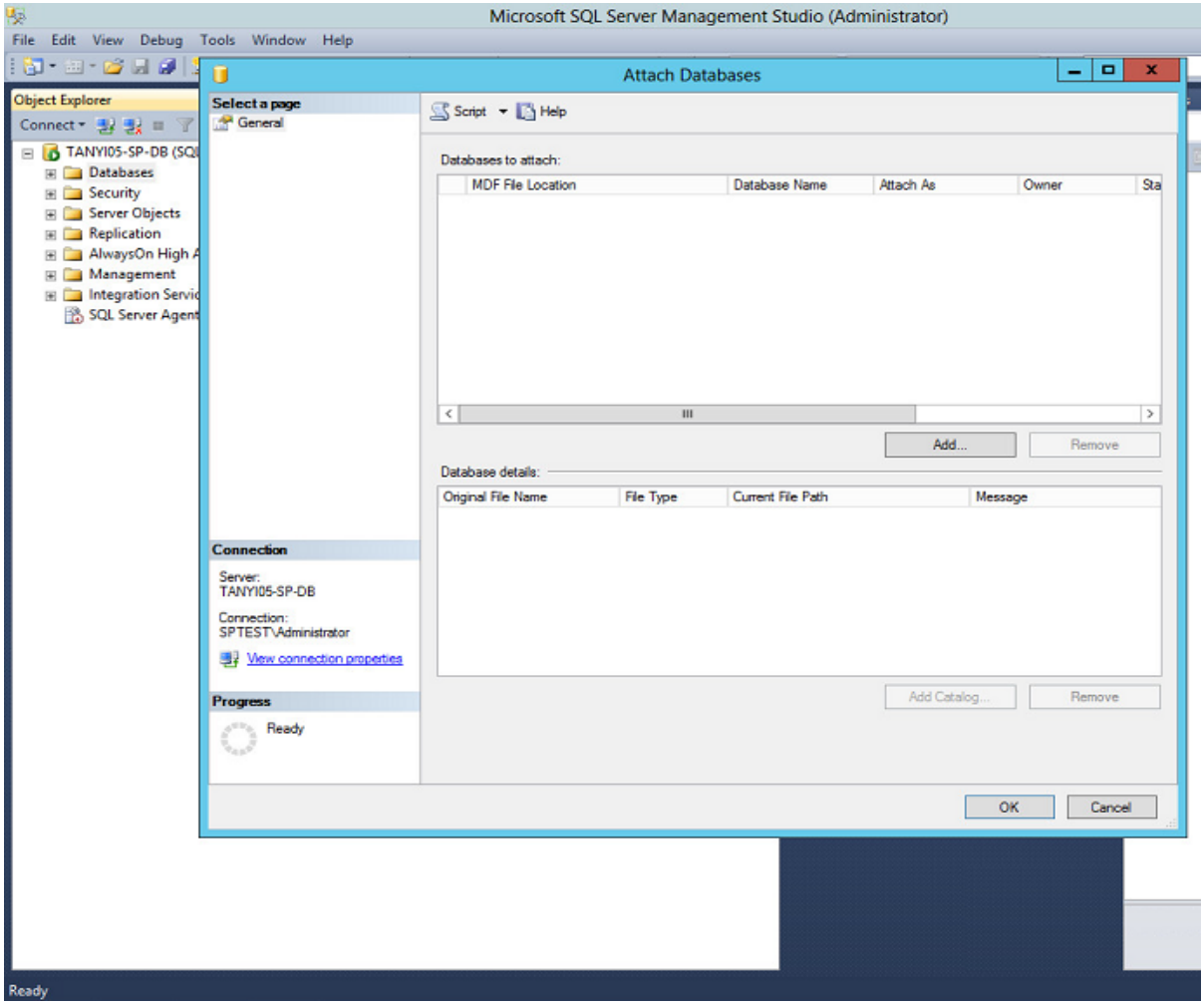
   Por ejemplo, de forma predeterminada, se guarda el archivo de la base de datos en C:\Archivos de programa\Microsoft SQL Server\MSSQL12. MSSQLSERVER\MSSQL\DATA y se selecciona el volumen C.
4. Introduzca un nuevo nombre del volumen que se debe montar en el siguiente cuadro de diálogo y haga clic en **Aceptar**.



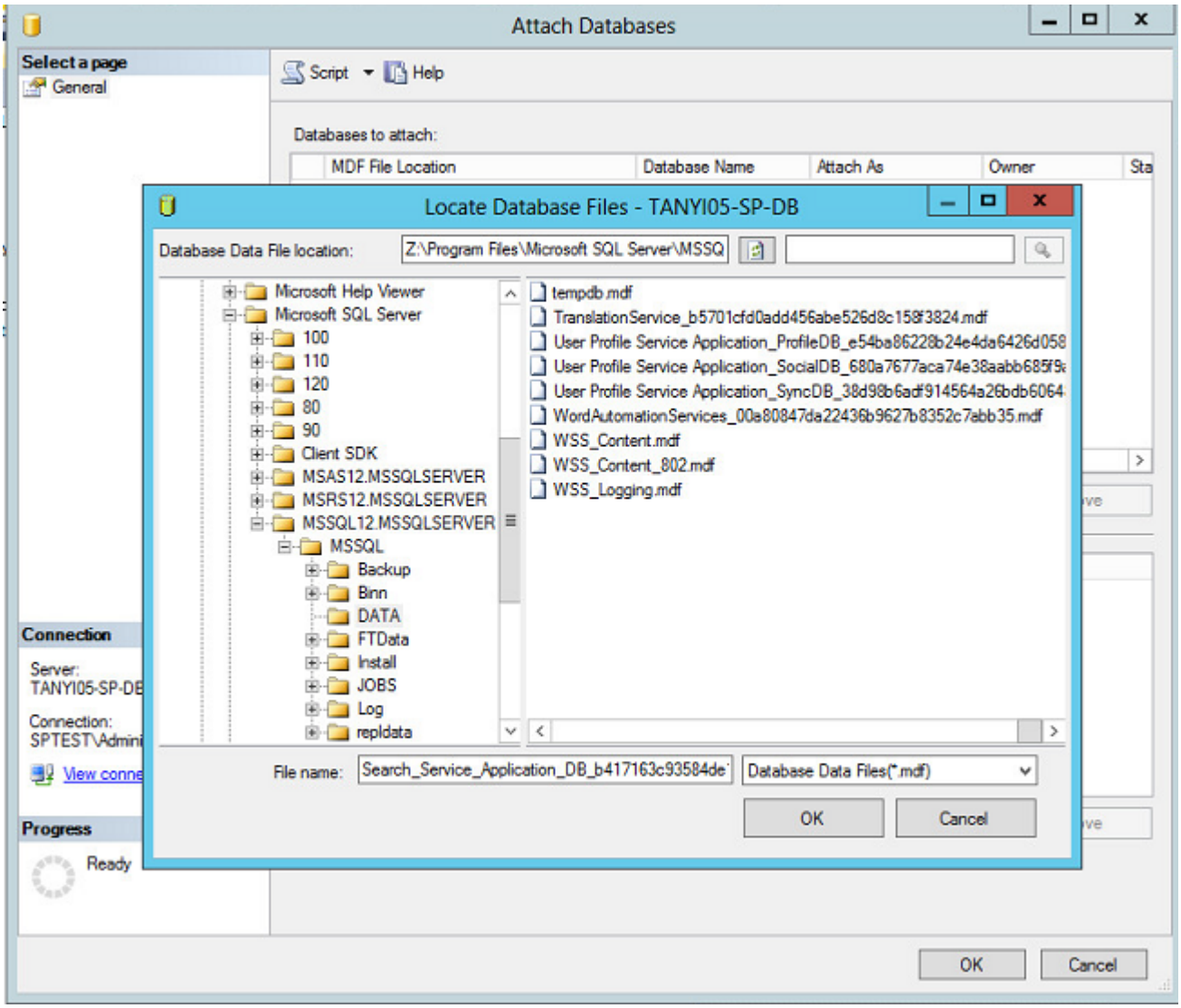
Aparece el nuevo volumen en Volúmenes montados en la interfaz de usuario.



5. Abra SQL Server Management Studio para adjuntar la base de datos de la copia de seguridad.
6. Haga clic con el botón secundario del ratón en la carpeta Databases y seleccione Attach.



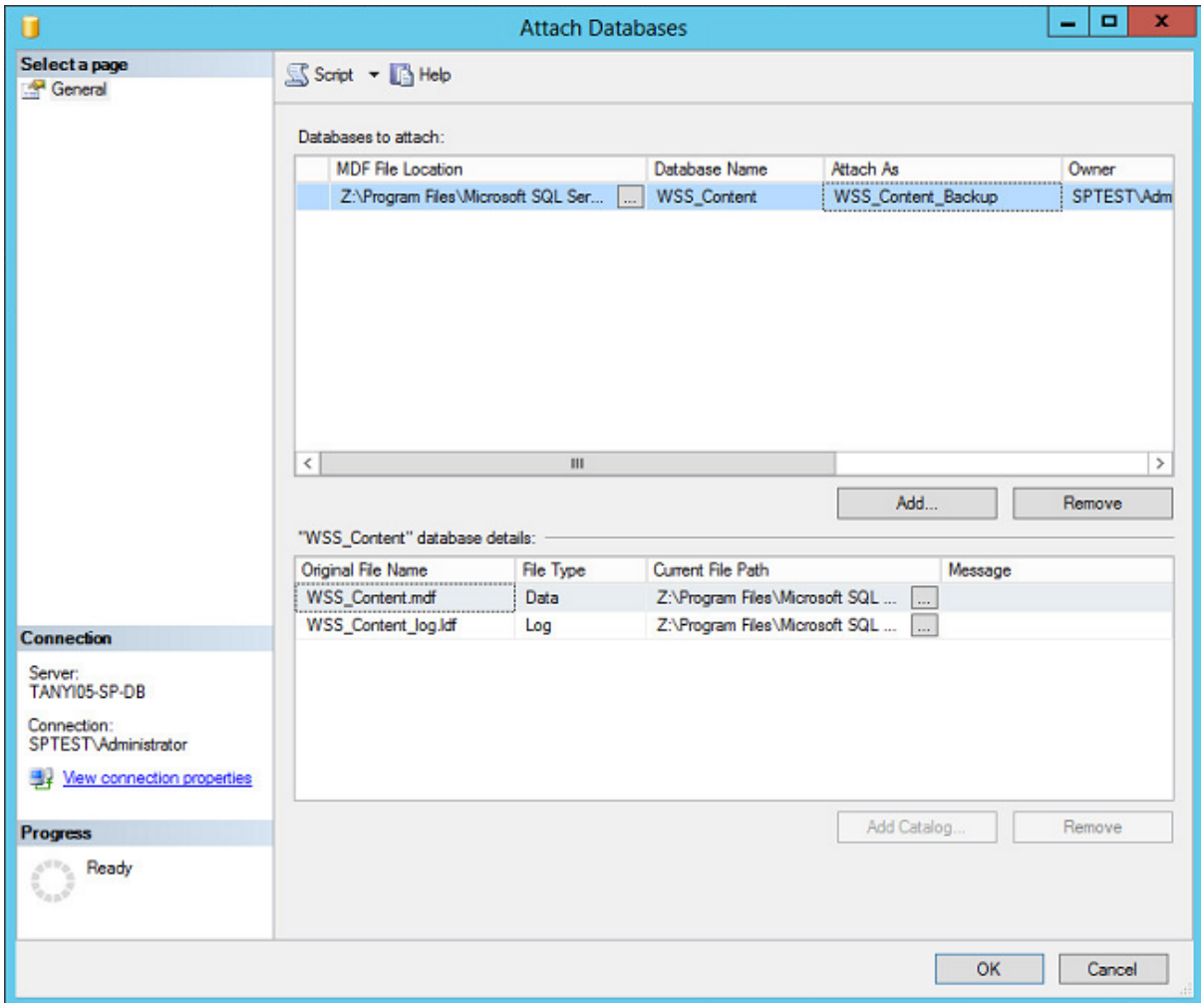
7. Haga clic en Add para seleccionar el archivo de la base de datos que se desea adjuntar.



8. Si el volumen montado es Z, seleccione la ubicación del archivo de datos de la base de datos como Z:\Archivos de programa\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA.
9. Seleccione el archivo llamado WSS_Content.mdf y haga clic en Aceptar.

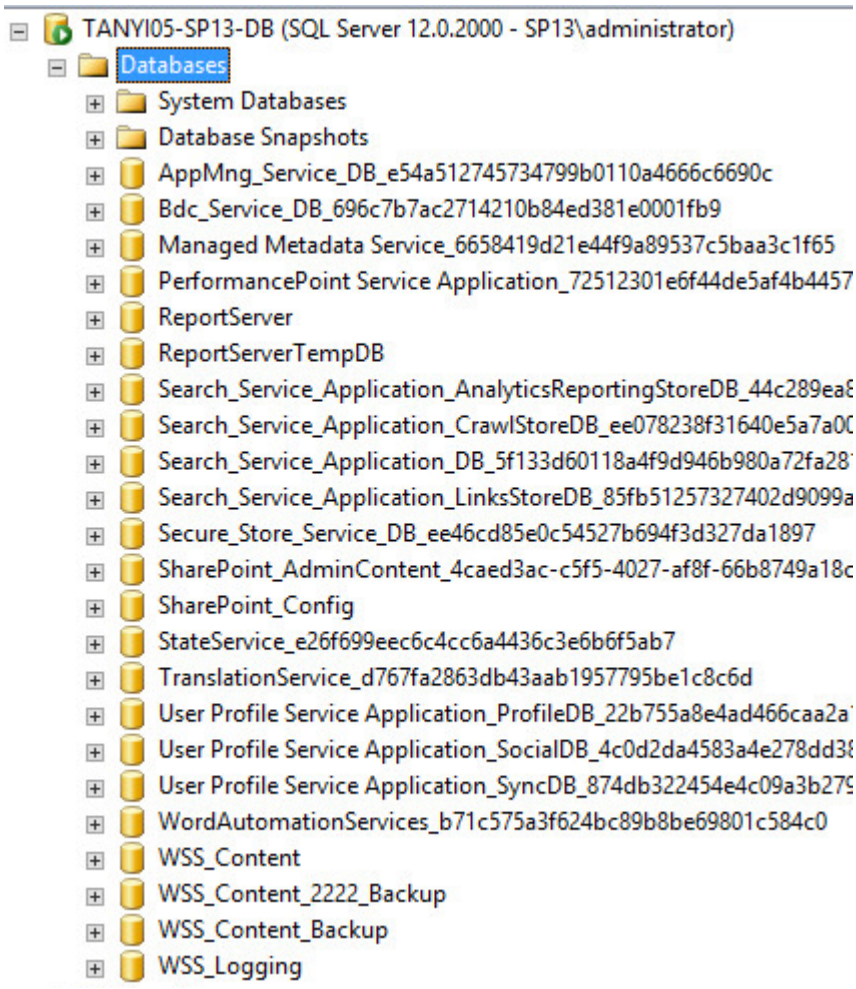
   Nota: WSS_Content.mdf es el nombre predeterminado del archivo de datos de la base de datos para la aplicación web de SharePoint. Si se desea restaurar otra base de datos que ha creado una nueva aplicación web, utilice el nombre del archivo de datos de la base de datos relacionada.
10. Haga clic en la columna Attach As para escribir el nombre de la base de datos (por ejemplo, WSS_Content_Backup) y haga clic en Aceptar.

    Nota: Antes de restaurar el contenido de una base de datos, asegúrese de que el nombre de la base de datos no existe en ninguna otra aplicación web.

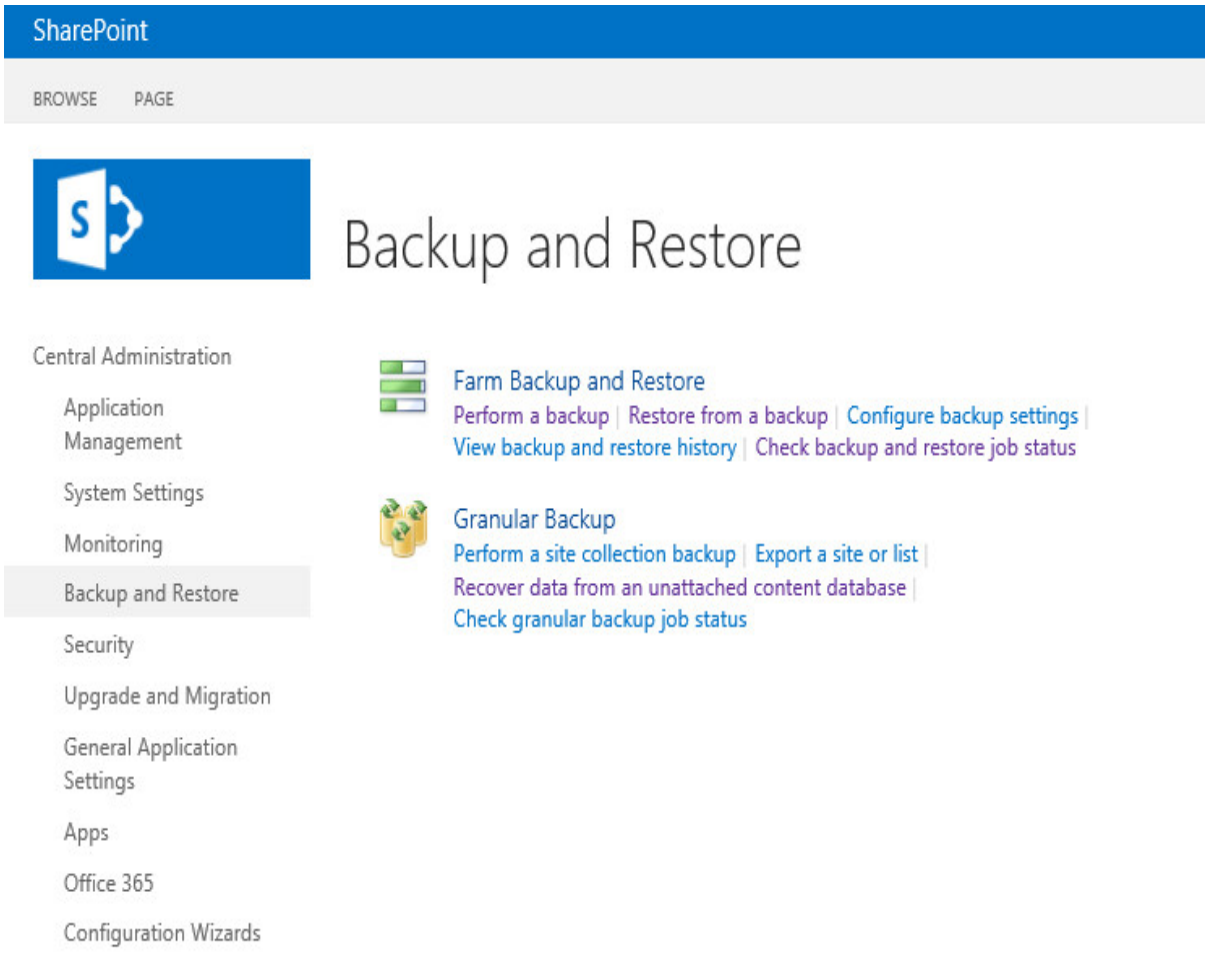


La nueva base de datos se adjunta a la carpeta Databases.

Nota: La nueva base de datos no está asociada con ninguna aplicación web.

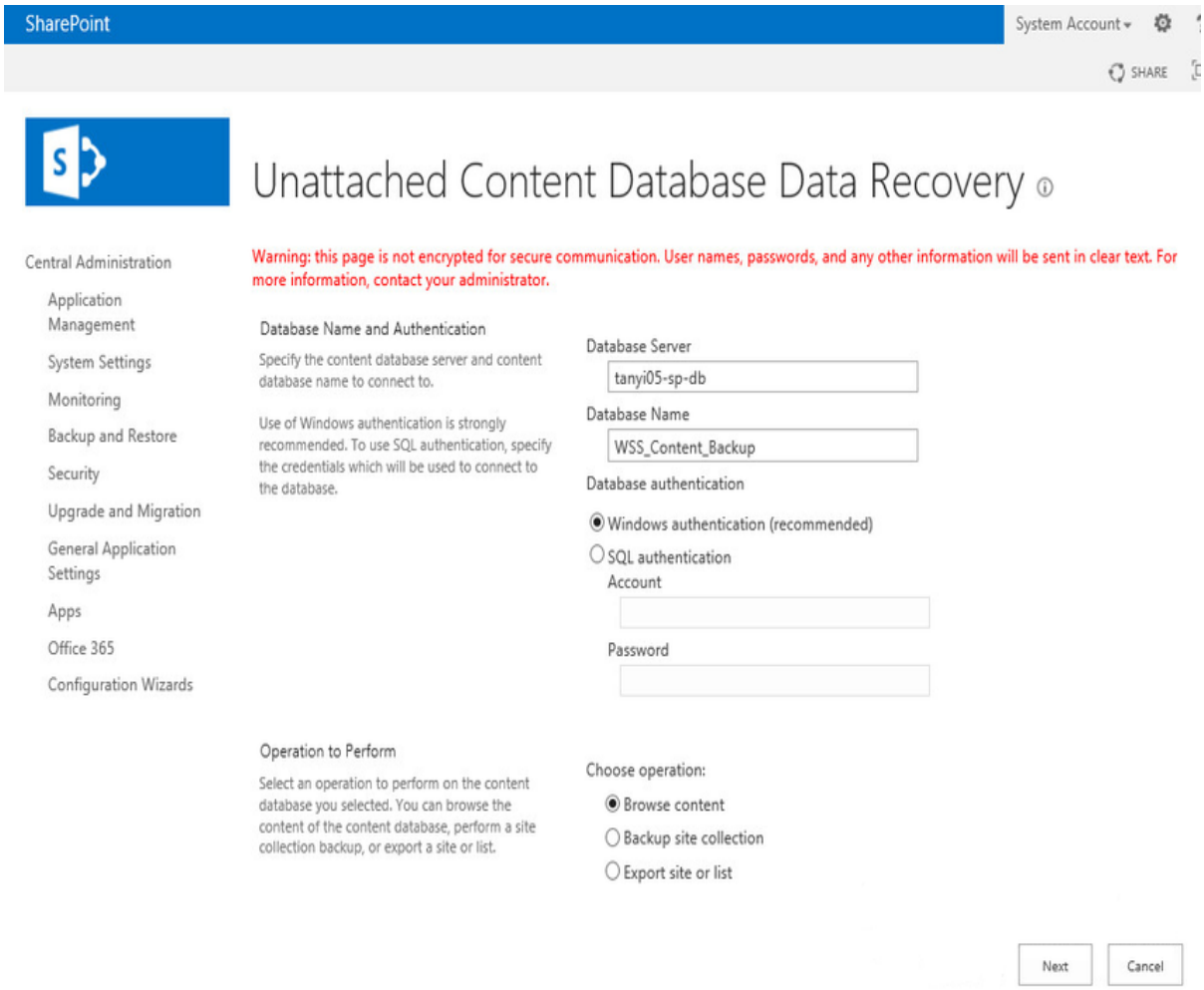


11. Inicie sesión en el equipo que está en Servidores de frontend web en las granjas de SharePoint Server.
12. Abra la Administración Central y haga clic en el encabezamiento Realizar copia de seguridad y restaurar.



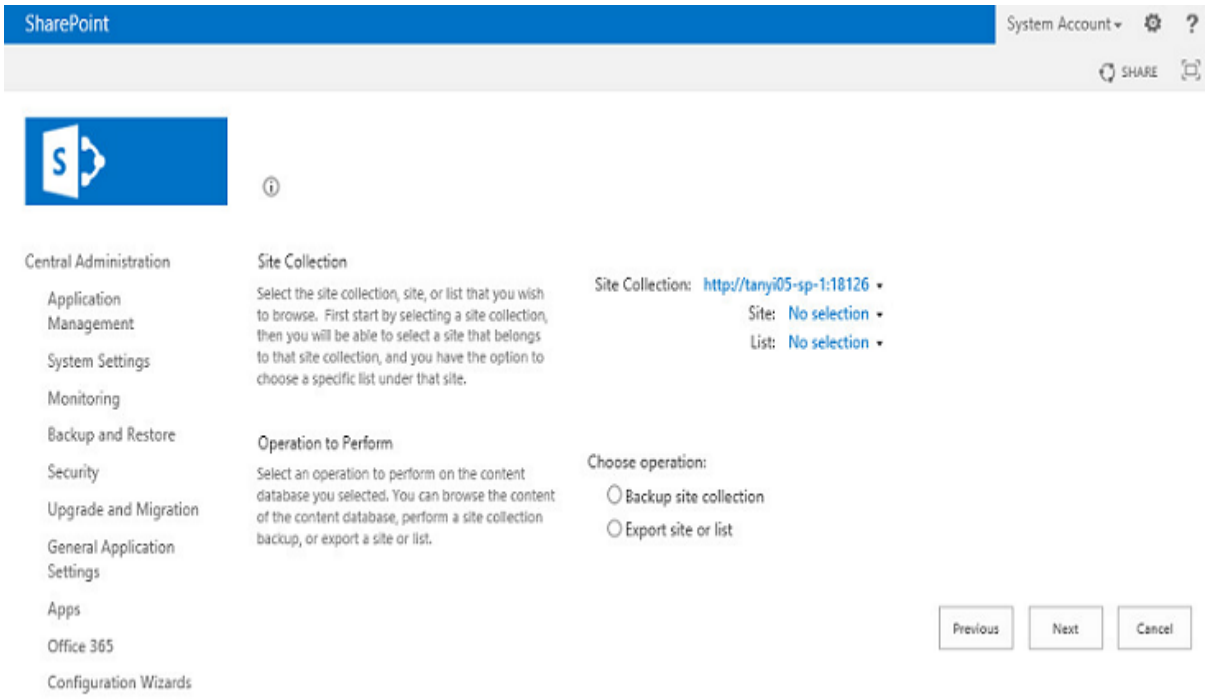
13. Haga clic en Recuperar datos en el vínculo Recuperación de datos de la base de datos de contenido no adjunto, proporcione el nombre de SQL Server y el nombre de la base de datos para la base de datos no conectada y utilice la autenticación de Windows.
14. Seleccione la opción Explorar contenido y haga clic en el botón **Siguiente**.

    Nota: El nombre de SQL Server es el nombre de los servidores de la base de datos utilizados por la granja de SharePoint Server, el nombre de la base de datos es el nombre de la base de datos recién adjuntada.



15. Seleccione si se desea realizar la copia de seguridad de la recopilación de sitios o exportar la lista y el sitio seleccionados.

    Nota: De forma predeterminada, si la base de datos es una base de datos de contenido no conectada, la dirección URL de la recopilación de sitios todavía incluirá el número de puerto de la aplicación web de la Administración central.



Se ha llevado a cabo la restauración utilizando la opción Montar la base de datos desde un punto de recuperación.

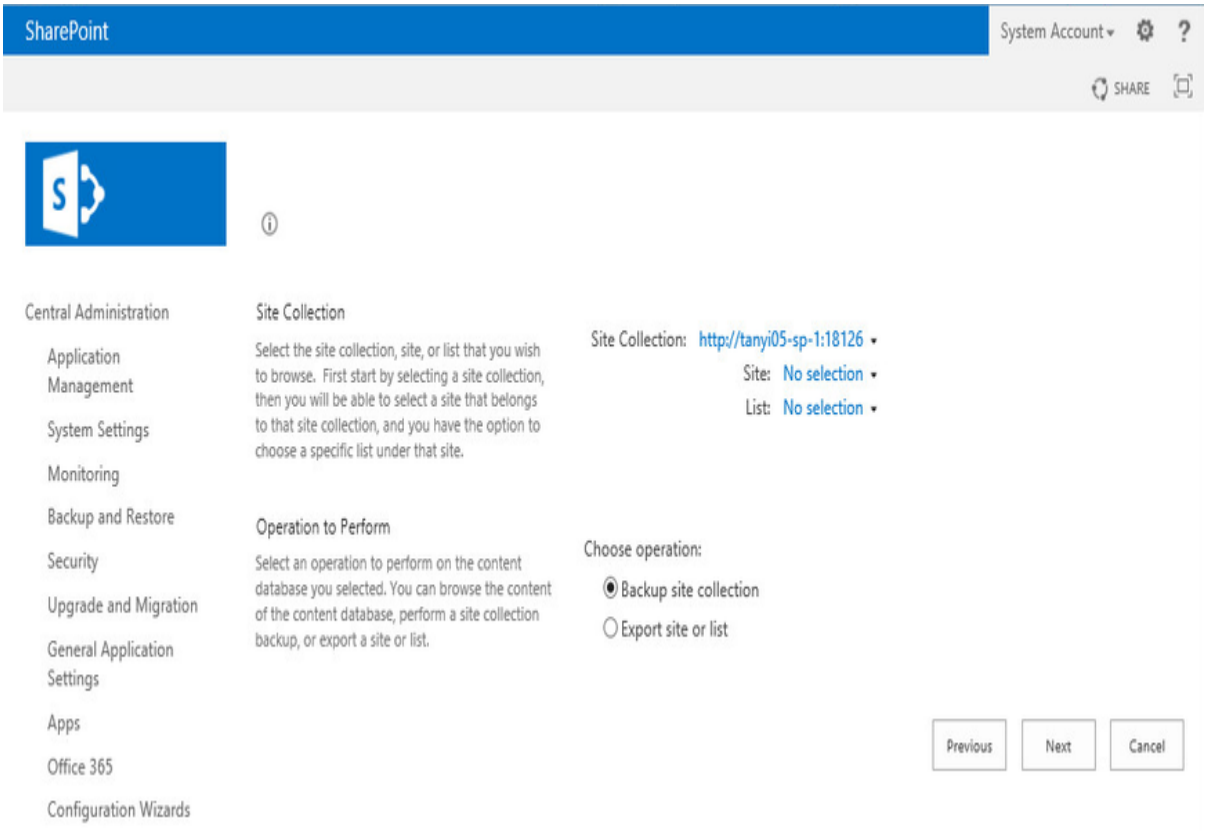
Restauración de una recopilación de sitios

Siga estos pasos:

1. Se puede recuperar el contenido de la recopilación de sitios desde una base de datos de contenido no conectada.

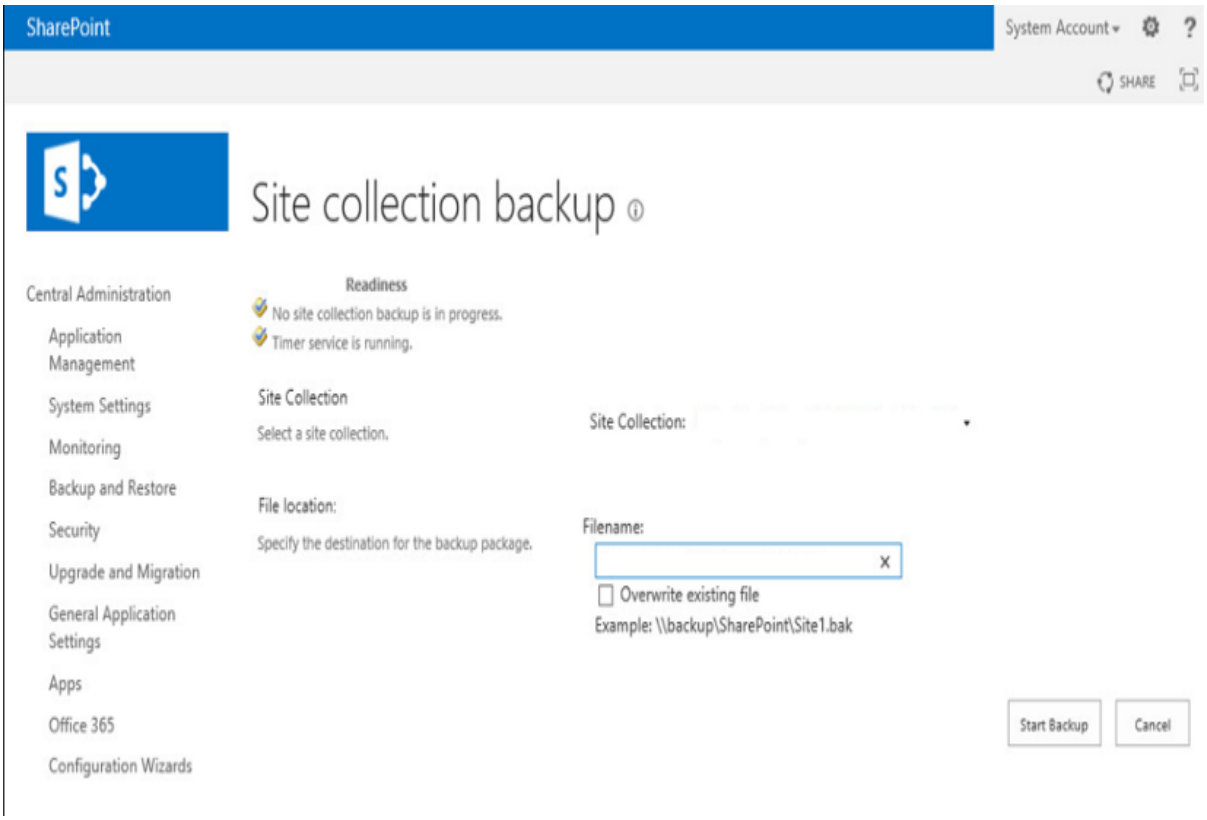
   En Administración central

   a. Seleccione la opción de recopilación de sitios de la copia de seguridad y haga clic en el botón Siguiente.



   b. Seleccione la recopilación de sitios y proporcione la ubicación del archivo para el paquete de la copia de seguridad.

   c. Seleccione Sobrescribir archivo existente.



d. Haga clic en el botón Iniciar copia de seguridad para empezar la copia de seguridad.

   Se realiza la copia de seguridad de la recopilación de sitios en un archivo.

Utilice los comandos de PowerShell

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

   ConnectAsUnattachedDatabase: Especifica que solo se han devuelto las bases de datos no conectadas en la granja.

   DatabaseName: Especifica el nombre de la base de datos de contenido.

   DatabaseServer: Especifica el nombre del servidor host para la base de datos de contenido especificada en el parámetro DatabaseName.

   Para obtener más información, consulte el artículo de Microsoft.

b. Backup-SPSite -Identity xxxx -Path xxxx

   Identity: Especifica la dirección URL o el GUID de la recopilación de sitios de la que se debe realizar la copia de seguridad.

   Path: Especifica la ruta completa del archivo de copia de seguridad (por ejemplo, C:\backup\sitecollection.bak).

   Para obtener más información, consulte el artículo de Microsoft.

2. Haga clic en Shell de administración de SharePoint para iniciar la consola.
3. Utilice los comandos de PowerShell para restaurar la recopilación de sitios.

```
Restore-SPSite -Identity xxxx -Path xxxx
```

Identity: Especifica la ubicación de la dirección URL en la que se restaura la recopilación de sitios. (Por ejemplo, http://www.contoso.com).

Path: Especifica una ruta válida de la ubicación de la copia de seguridad.(Por ejemplo, C:\backup\sitecollection.bak)

Para obtener más información, consulte el artículo de Microsoft.

Nota: Se producirá un error al restaurar una recopilación de sitios a su ubicación original. También puede realizar los pasos siguientes:

a. New-SPContentDatabase -Name xxxx -DatabaseServer xxxx -WebApplication xxxx

   Name: Especifica la nueva base de datos de contenido que se debe crear en la granja.

   DatabaseServer: Especifica el nombre del servidor host para la base de datos de contenido especificada en el parámetro Name.

   WebApplication: Adjunta la base de datos de contenido a la aplicación web especificada de SharePoint.

b. Restore-SPSite -Identity xxxx -Path xxxx -GradualDelete -DatabaseServer xxxx -DatabaseName xxxx

   Identity: Especifica la ubicación de la dirección URL en la que se restaura la recopilación de sitios. (Por ejemplo, http://www.contoso.com).

   Path: Especifica una ruta válida de la ubicación de la copia de seguridad.(Por ejemplo, C:\backup\sitecollection.bak)

   GradualDelete: Especifica que la recopilación de sitios que se sobrescribe con el parámetro Force se debe suprimir gradualmente mediante una tarea de temporizador, en lugar de suprimirse de golpe. Se reduce el impacto en el rendimiento de los productos SharePoint 2010 y SQL Server.

   DatabaseName: Especifica la base de datos de contenido de SQL Server donde se almacenarán los datos de la recopilación de sitios.

   DatabaseServer: Especifica el nombre de SQL Server que contiene la base de datos de contenido especificada por el parámetro DatabaseName.

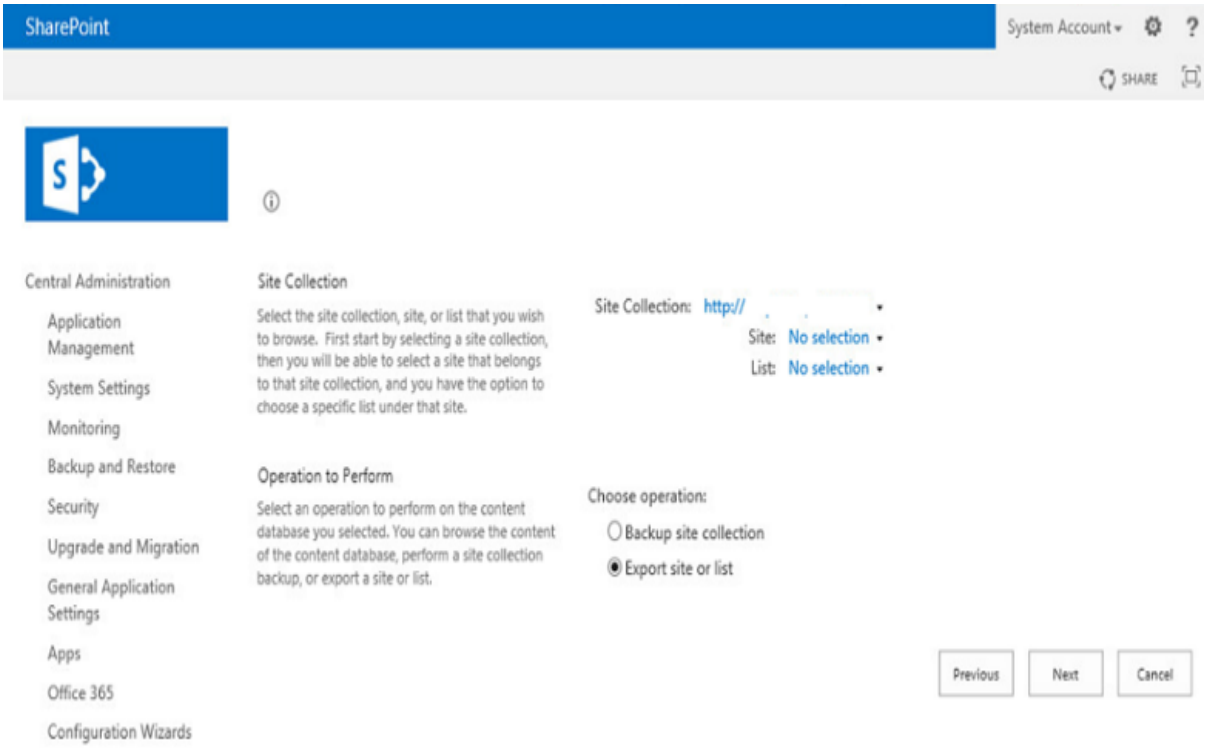
Restauración de sitios

Siga estos pasos:

1. Se puede recuperar el contenido de sitios desde una base de datos de contenido no conectada.

   Utilice la Administración central

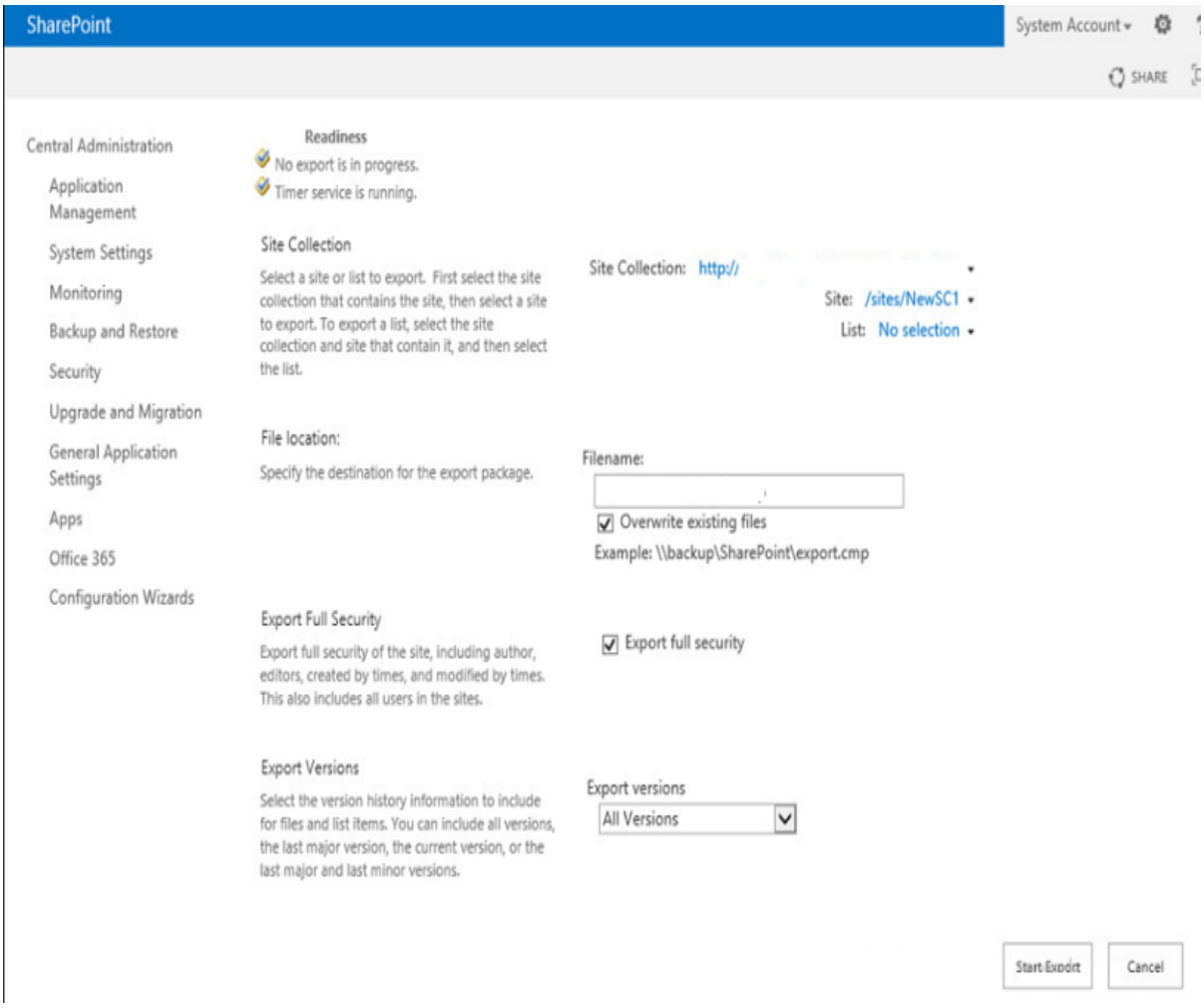
   a. Seleccione la opción de exportación de sitios o la opción de lista y haga clic en el botón Siguiente.



   b. Seleccione el sitio y proporcione la ubicación del archivo para el paquete de exportación.

      Ejemplo: El nombre del sitio que se va a restaurar es TestSite1 y la dirección URL es /TestSite1/.

   c. Seleccione las opciones de seguridad y las versiones (de forma pre-determinada la opción seleccionada es Todas las versiones).



d. Haga clic en el botón Iniciar exportación para comenzar la exportación, a continuación el sitio se exportará a un archivo.

Utilice los comandos de PowerShell

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

ConnectAsUnattachedDatabase: Especifica que solo se han devuelto las bases de datos no conectadas en la granja.

DatabaseName: Especifica el nombre de la base de datos de contenido.

DatabaseServer: Especifica el nombre del servidor host para la base de datos de contenido especificada en el parámetro DatabaseName.

Para obtener más detalles, consulte el artículo de Microsoft.

b. Establecimiento del objeto para exportar

$ExportObject = New-Object Microsoft.SharePoint.Deployment.SPExportObject

$ExportObject.Type = [Microsoft.SharePoint.Deployment.SPDeploymentObjectType]::Web

$ExportObject.Url = $SiteUrl

$SiteUrl: Especifica la ubicación de la dirección URL en la que se realizará la copia de seguridad del sitio.

c. Configuración de los valores de configuración de la exportación

$ExportSettings = New-Object Microsoft.SharePoint.Deployment.SPExportSettings

$ExportSettings.UnattachedContentDatabase = $database

$ExportSettings.SiteUrl = $CAUrl

$CAUrl: Especifica la dirección URL del sitio Administración central.

$ExportSettings.FileLocation = $ExportPath

$ExportSettings.LogFilePath = $ExportPath

$ExportPath: Especifica la ruta de acceso para guardar el archivo de la copia de seguridad (por ejemplo, C:\backup).

$ExportSettings.BaseFileName = $ExportFile

$ExportFile: Especifica el nombre de archivo del archivo de la copia de seguridad (por ejemplo, site.cmp).

$ExportSettings.IncludeVersions = [Microsoft.SharePoint.Deployment.SPIncludeVersions]::All

$ExportSettings.ExportMethod = [Microsoft.SharePoint.Deployment.SPExportMethodType]::ExportAll

$ExportSettings.IncludeVersions = [Microsoft.SharePoint.Deployment.SPIncludeVersions]::All

$ExportSettings.ExportObjects.Add($ExportObject)

$ExportSettings.Validate()

$ExportJob = New-Object Microsoft.SharePoint.Deployment.SPExport($ExportSettings)

Realiza la copia de seguridad del sitio en un archivo.

$ExportJob.Run()

Para obtener más detalles, consulte el artículo de Microsoft.

2. Haga clic en Shell de administración de SharePoint para iniciar la consola.

3. Utilice los comandos de PowerShell para restaurar el sitio a la ubicación de origen o a la nueva ubicación.

```
Import-SPWeb -Identity xxxx -Path xxxx -Inclu-
deUserSecurity:$true -UpdateVersions:xxxx
```

Identity: Especifica la dirección URL o el GUID de la Web en la que se realiza la importación. Por ejemplo, http://www.contoso.com.

Path: Especifica el nombre del archivo de importación. Por ejemplo, C:\-backup\site.cmp'.

IncludeUserSecurity: Conserva la configuración de seguridad del usuario excepto los objetos SPList que tienen definidos la herencia rota y los permisos a nivel del elemento.

UpdateVersions: Indica cómo solucionar situaciones en las que la versión de un archivo que se va a importar a un sitio ya existe en dicho sitio. Se puede seleccionar una de las siguientes opciones:

Add: Agrega el archivo como una nueva versión.

Overwrite: Sobrescribe el archivo actual y todas sus versiones (primero suprime y, a continuación, inserta).

Ignore: Omite el archivo si ya existe en el destino. No se agregará el nuevo archivo.

El valor predeterminado es Agregar.

Para obtener más detalles, consulte el artículo de Microsoft.

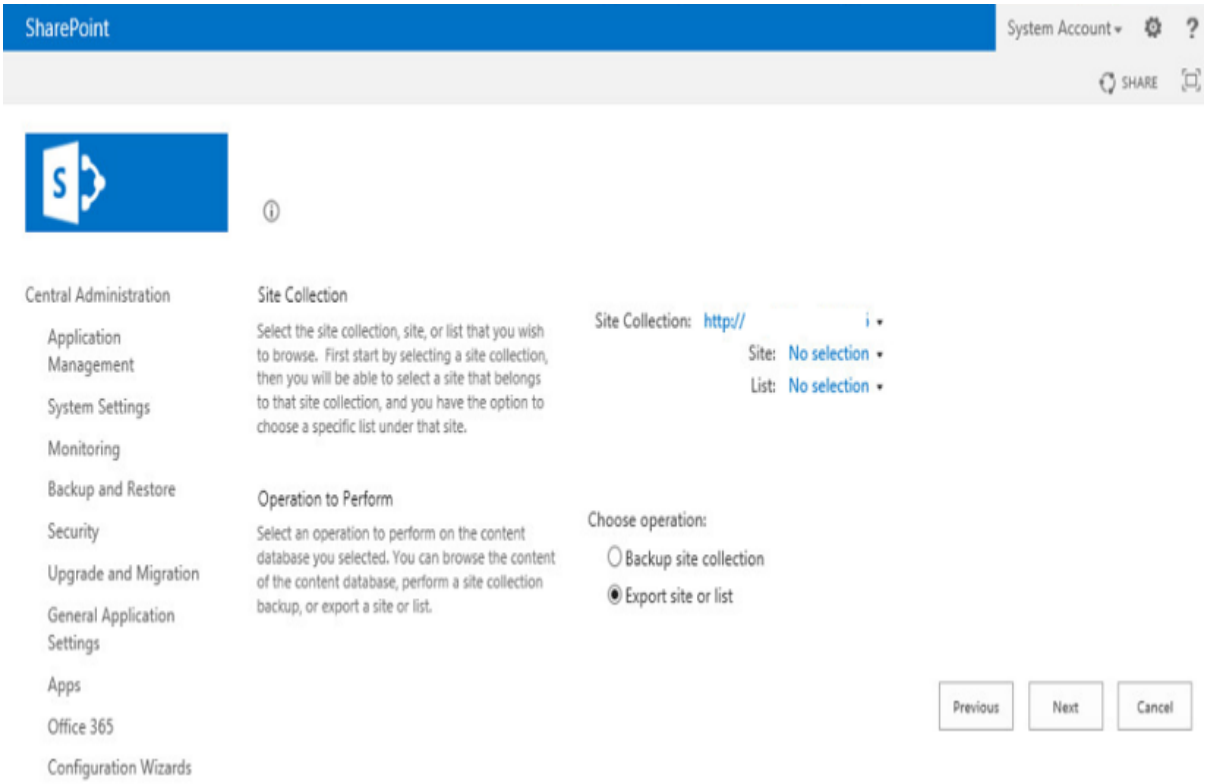
Restauración de listas o bibliotecas

Siga estos pasos:

1. Se puede recuperar el contenido de la lista o biblioteca desde una base de datos de contenido no conectada.

   Utilice la Administración central

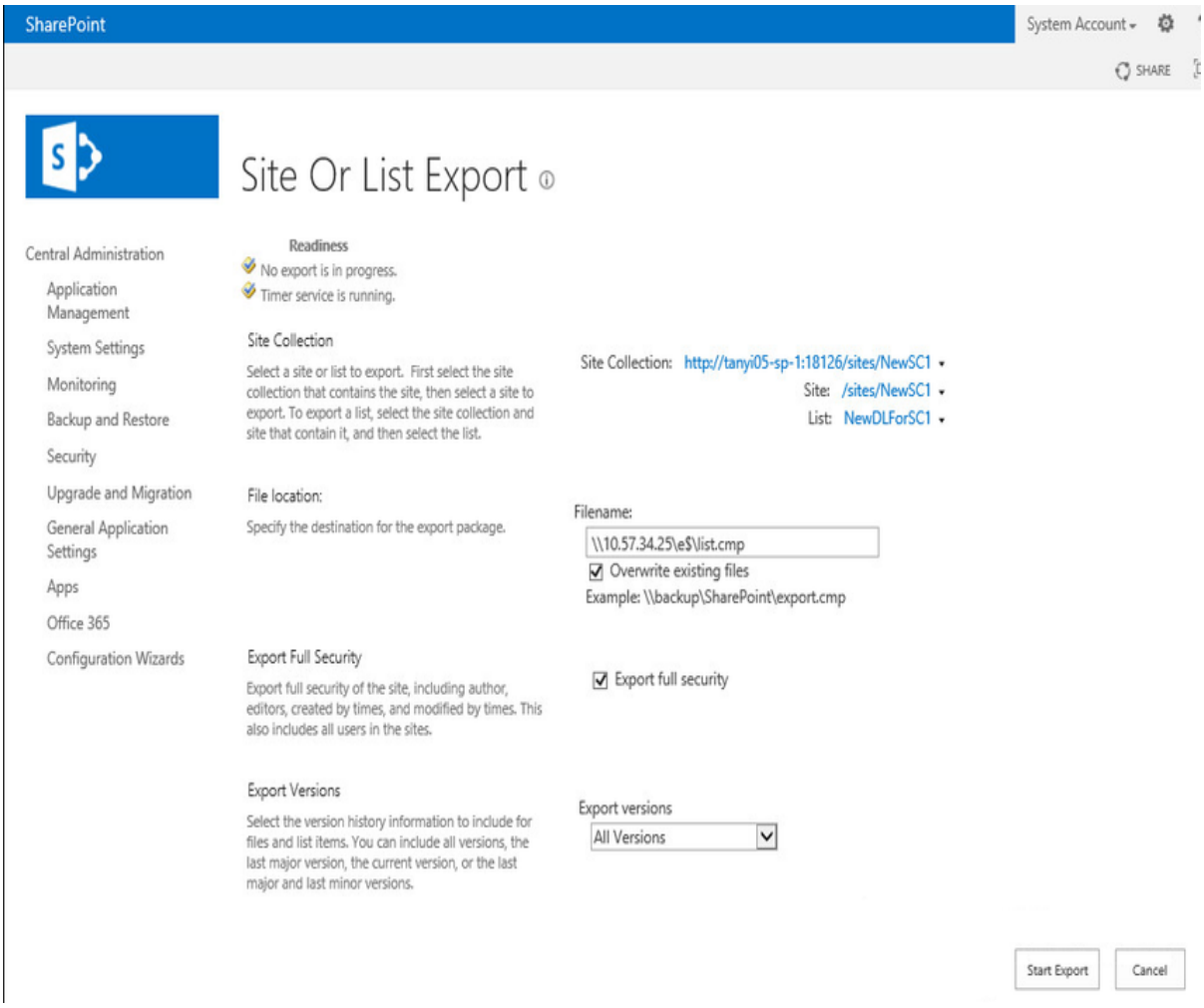
   a. Seleccione la opción de exportación de sitios o la opción de lista y haga clic en el botón **Siguiente**.



   b. Seleccione el sitio y la lista y proporcione la ubicación del archivo para el paquete de exportación.

      Ejemplo: El nombre de la lista o biblioteca que se va a restaurar es NewList1 y la dirección URL es /TestSite1/NewList1.

   c. Seleccione las opciones de seguridad y las versiones (de forma pre-determinada la opción seleccionada es Todas las versiones).



d. Haga clic en **Iniciar exportación** para iniciar la exportación.

   La lista o biblioteca se exportará a un archivo.

Utilice los comandos de PowerShell

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

   ConnectAsUnattachedDatabase: Especifica que solo se han devuelto las bases de datos no conectadas en la granja.

   DatabaseName: Especifica el nombre de la base de datos de contenido.

   DatabaseServer: Especifica el nombre del servidor host para la base de datos de contenido especificada en el parámetro DatabaseName.

   Para obtener más detalles, consulte el artículo de Microsoft.

b. Establecimiento del objeto para exportar.

   $ExportObject = New-Object Microsoft.SharePoint.Deployment.SPExportObject

$ExportObject.Type = [Microsoft.SharePoint.Deployment.SPDeploymentObjectType]::List

$ExportObject.Url = $ListUrl

$ListUrl: Especifica la ubicación de la dirección URL en la que se realizará la copia de seguridad de la lista o biblioteca. Si se trata de una lista, utilice el parámetro "/Lists/{NombreLista}". Si se trata de una biblioteca, utilice el parámetro "/{NombreBiblioteca}"

c. Configuración de los valores de configuración de la exportación

$ExportSettings = New-Object Microsoft.SharePoint.Deployment.SPExportSettings

$ExportSettings.UnattachedContentDatabase = $database

$ExportSettings.SiteUrl = $CAUrl

$CAUrl: Especifica la dirección URL del sitio Administración central.

$ExportSettings.FileLocation = $ExportPath

$ExportSettings.LogFilePath = $ExportPath

$ExportPath: Especifica la ruta de acceso para guardar el archivo de la copia de seguridad (por ejemplo, C:\backup).

$ExportSettings.BaseFileName = $ExportFile

$ExportFile: Especifica el nombre de archivo del archivo de la copia de seguridad (por ejemplo, site.cmp).

$ExportSettings.IncludeVersions = [Microsoft.SharePoint.Deployment.SPIncludeVersions]::All

$ExportSettings.ExportMethod = [Microsoft.SharePoint.Deployment.SPExportMethodType]::ExportAll

$ExportSettings.IncludeVersions = [Microsoft.SharePoint.Deployment.SPIncludeVersions]::All

$ExportSettings.ExportObjects.Add($ExportObject)

$ExportSettings.Validate()

$ExportJob = New-Object Microsoft.SharePoint.Deployment.SPExport($ExportSettings)

d. Realiza la copia de seguridad de la lista o biblioteca en un archivo.

$ExportJob.Run()

Para obtener más detalles, consulte el artículo de Microsoft.

2. Haga clic en Shell de administración de SharePoint para iniciar la consola.

3. Utilice los comandos de PowerShell para restaurar la lista o biblioteca a la ubicación de origen o a la nueva ubicación.

```
Import-SPWeb -Identity xxxx -Path xxxx -Inclu-
deUserSecurity:$true -UpdateVersions:xxxx
```

Identity: Especifica la dirección URL o el GUID de la Web en la que se realiza la importación. Por ejemplo, http://www.contoso.com.

Path: Especifica el nombre del archivo de importación. Por ejemplo, C:\-backup\list.cmp.

IncludeUserSecurity: Conserva la configuración de seguridad del usuario excepto los objetos SPList que tienen definidos la herencia rota y los permisos a nivel del elemento.

UpdateVersions: Indica cómo solucionar situaciones en las que la versión de un archivo que se va a importar a un sitio ya existe en dicho sitio. Se puede seleccionar una de las siguientes opciones:

Add: Agrega el archivo como una nueva versión.

Overwrite: Sobrescribe el archivo actual y todas sus versiones (primero suprime y, a continuación, inserta).

Ignore: Omite el archivo si ya existe en el destino. No se agregará el nuevo archivo.

El valor predeterminado es Add.

Para obtener más detalles, consulte el artículo de Microsoft.

Restauración de archivos

Siga estos pasos:

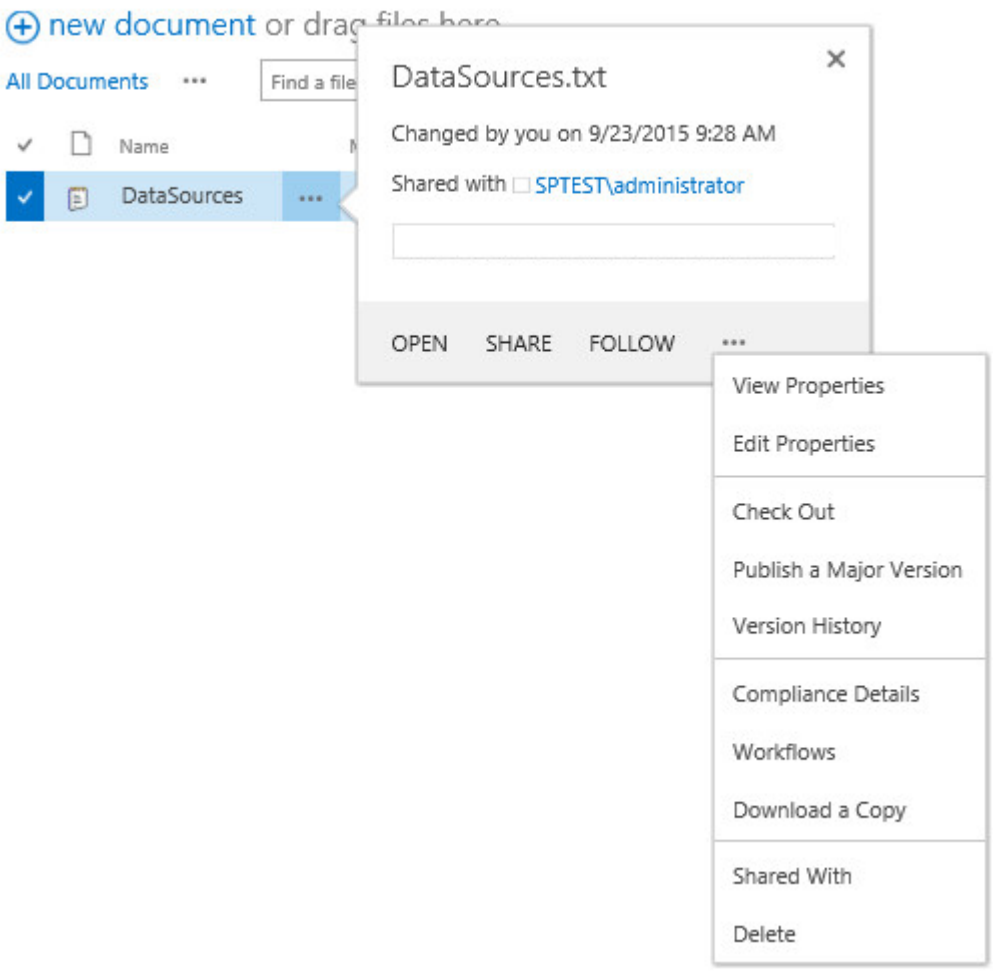
1. Restauración de la lista o biblioteca a una nueva ubicación. Para obtener más información, consulte Restauración de una lista o biblioteca.

   Por ejemplo: La lista o biblioteca de origen se llama ListaNueva1 y la dirección URL es http://contoso.com/SitioPrueba1/ListaNueva1

   - Use comandos de PowerShell para restaurar la biblioteca o lista a la nueva ubicación. Por ejemplo, http://contoso.com/SitioPrueba2

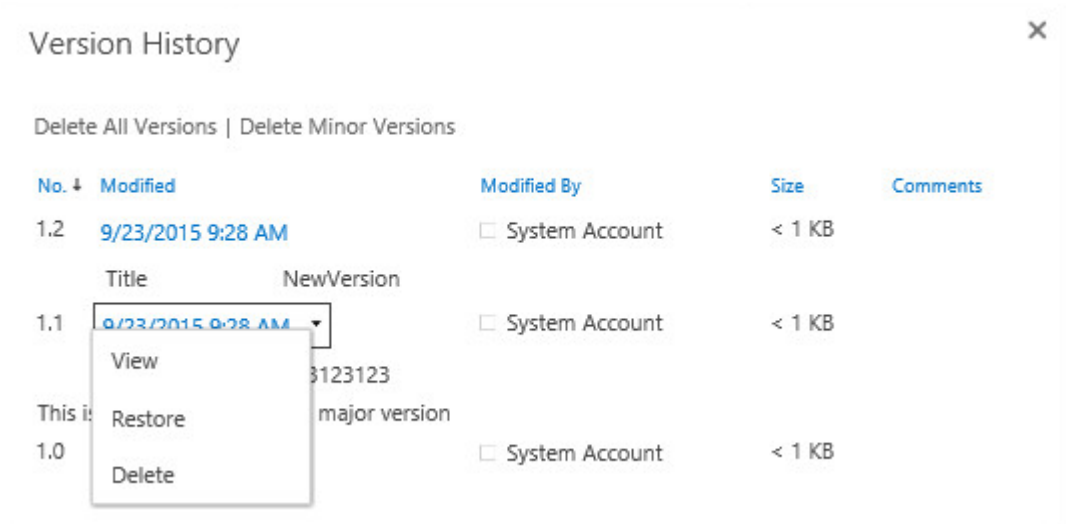
     Import-SPWeb -Identity http://contoso.com/SitioPrueba2 -Path C:\-backup\list.cmp -IncludeUserSecurity:$true -UpdateVersions:Overwrite

   - Vaya a la nueva dirección URL de la lista o biblioteca. Todos los elementos se restaurarán en http://contoso.com/SitioPrueba2/ListaNueva1.
2. Vaya a la nueva URL de la ubicación de la lista o biblioteca.
3. Compruebe el historial de versiones de archivo en la lista o biblioteca.



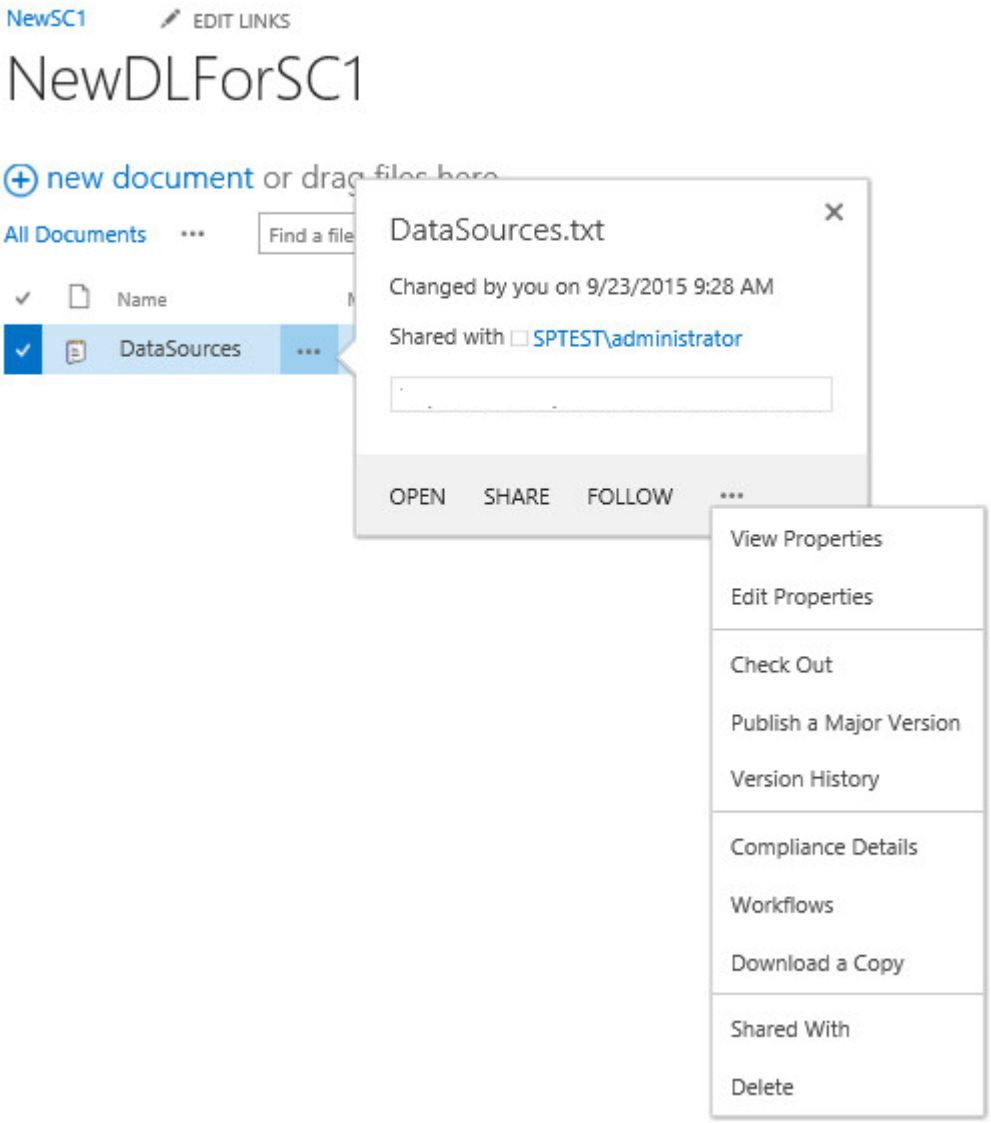
4. Seleccione la versión específica del archivo y haga clic en Restaurar.

   Por ejemplo, restaure la versión 1.1 específica del archivo.



   La versión 1.1 del archivo se restaura.

5. Haga clic en Descargar una copia para guardar el archivo con la versión específica 1.1 a una ubicación.



El archivo guardado se restaura a la lista o biblioteca de origen.

Creación de una red aislada para la recuperación de SharePoint

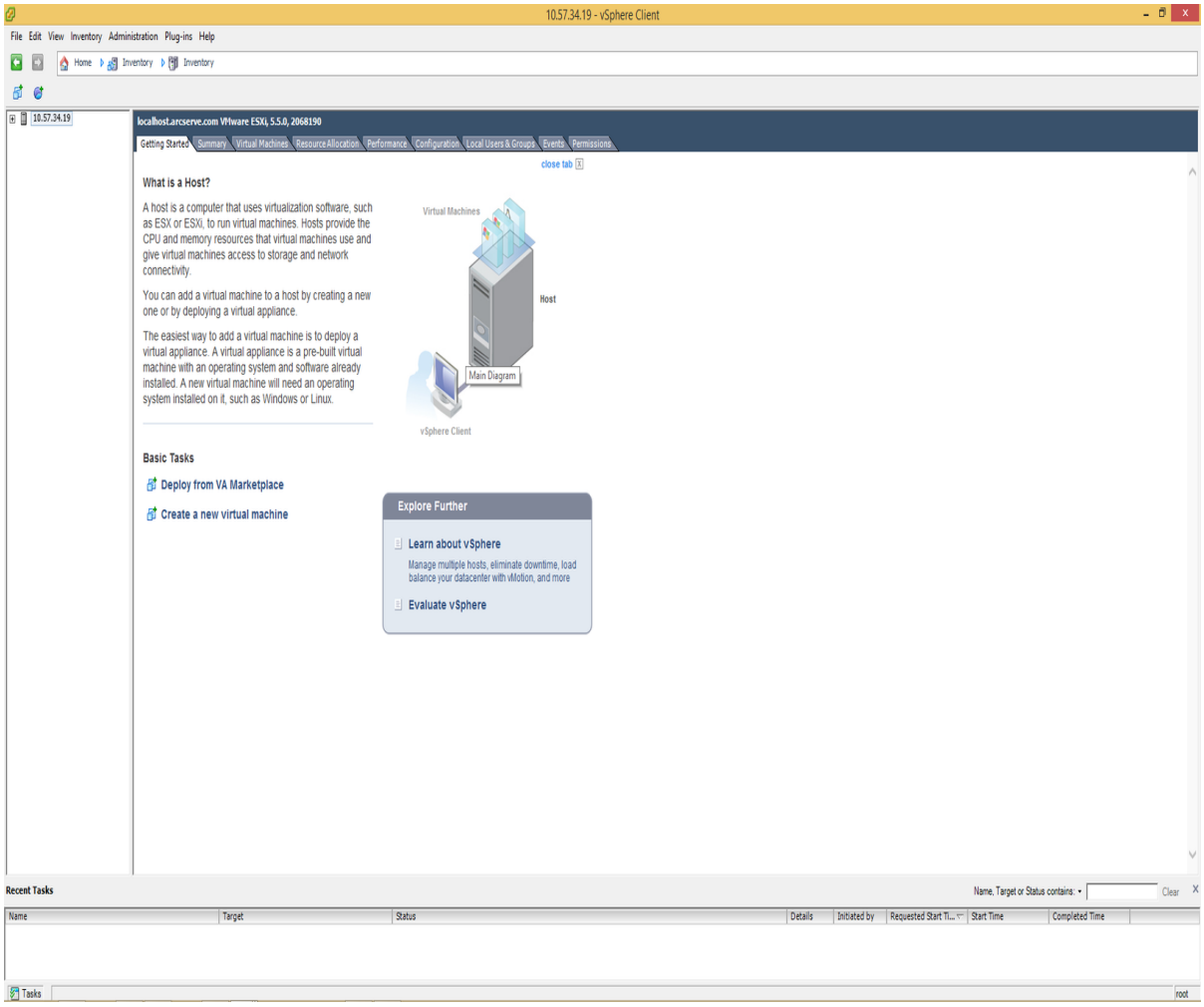
Se puede crear una red aislada para recuperar SharePoint en máquinas de Hyper-V y VMware.

- Cómo crear una red aislada para la recuperación de SharePoint en máquinas virtuales de VMware
- Cómo crear una red aislada para la recuperación de SharePoint en máquinas virtuales de Hyper-V

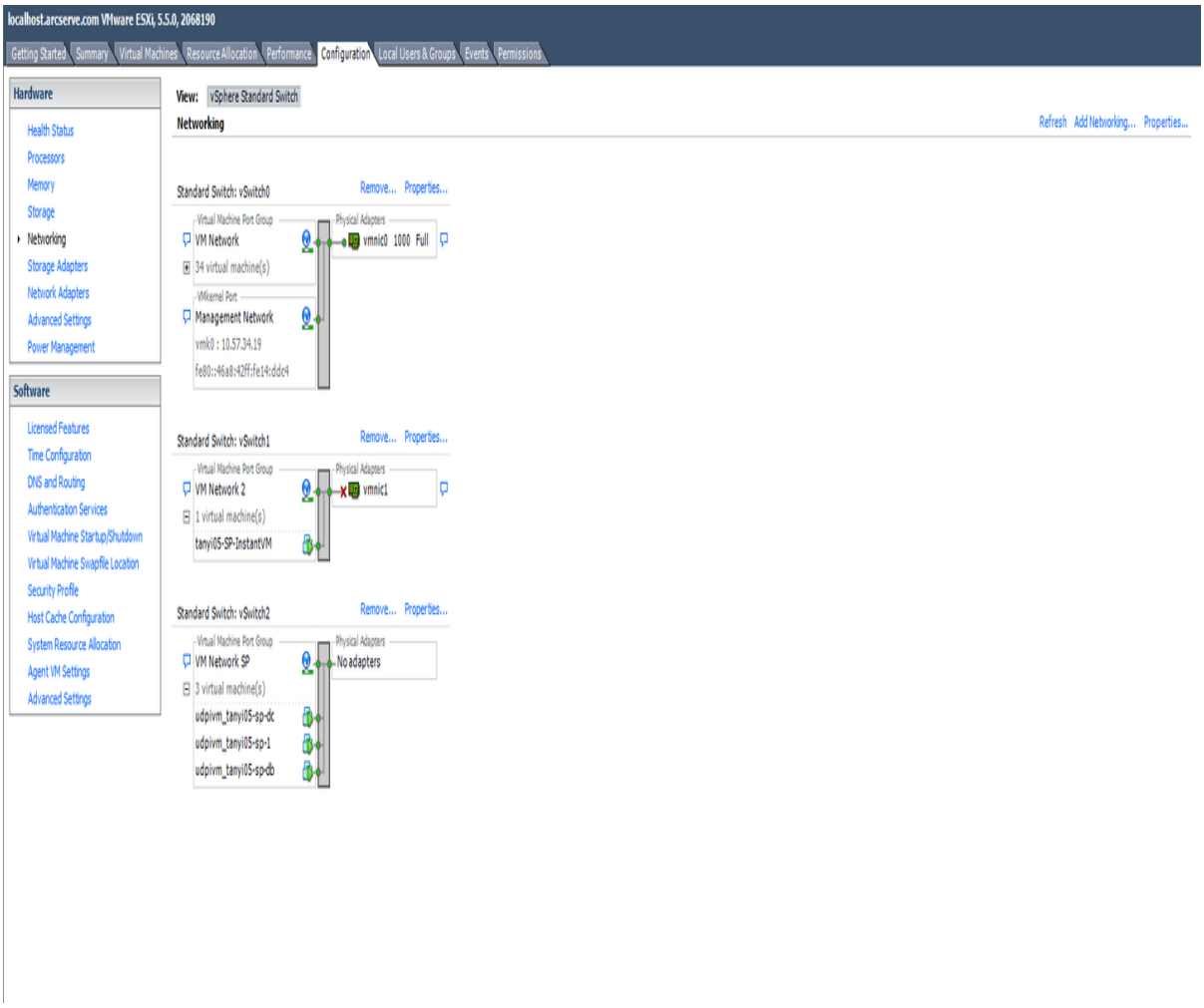
Cómo crear una red aislada para la recuperación de SharePoint en máquinas virtuales de VMware

Siga estos pasos:

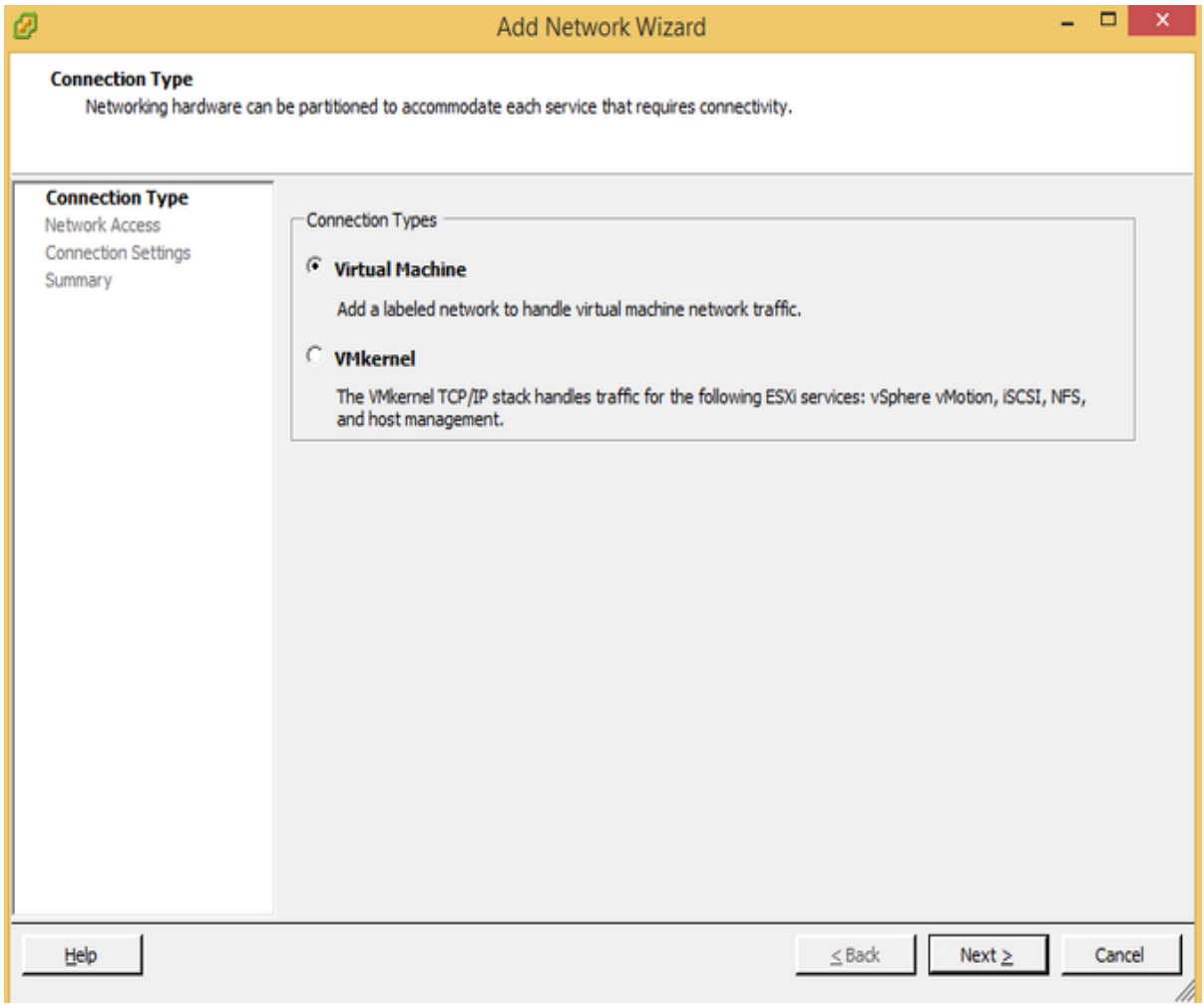
1. Inicie sesión en el servidor de VMware ESXi mediante el cliente de vSphere.



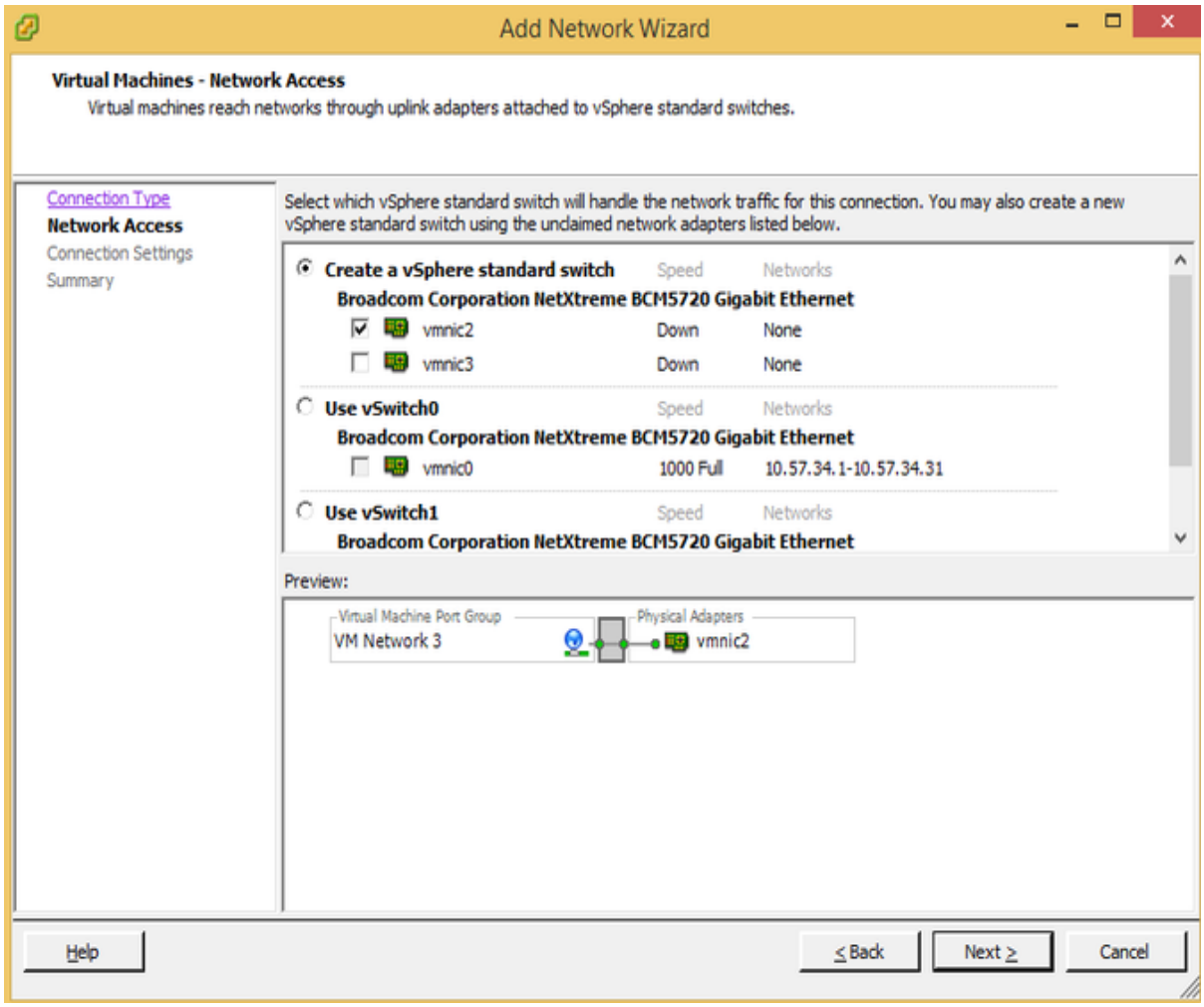
2. Haga clic en la ficha Configuración.
3. Seleccione Redes en el panel Hardware y haga clic en Agregar redes.



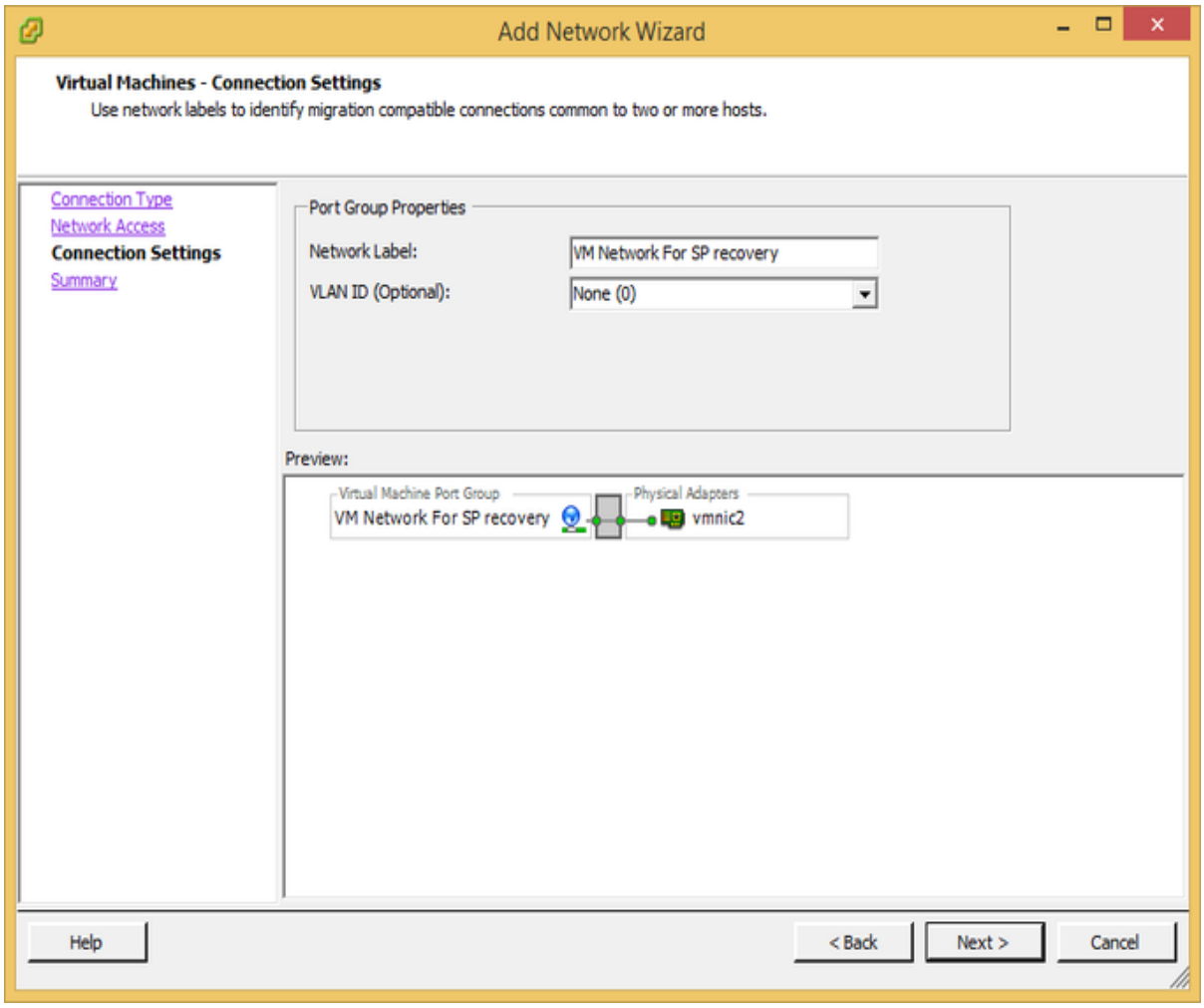
4. Asegúrese de que se selecciona la opción Máquina Virtual y haga clic en Siguiente.



5. Seleccione la NIC física que se debe utilizar para conectar el conmutador virtual con otros recursos físicos en la red y haga clic en Siguiente.

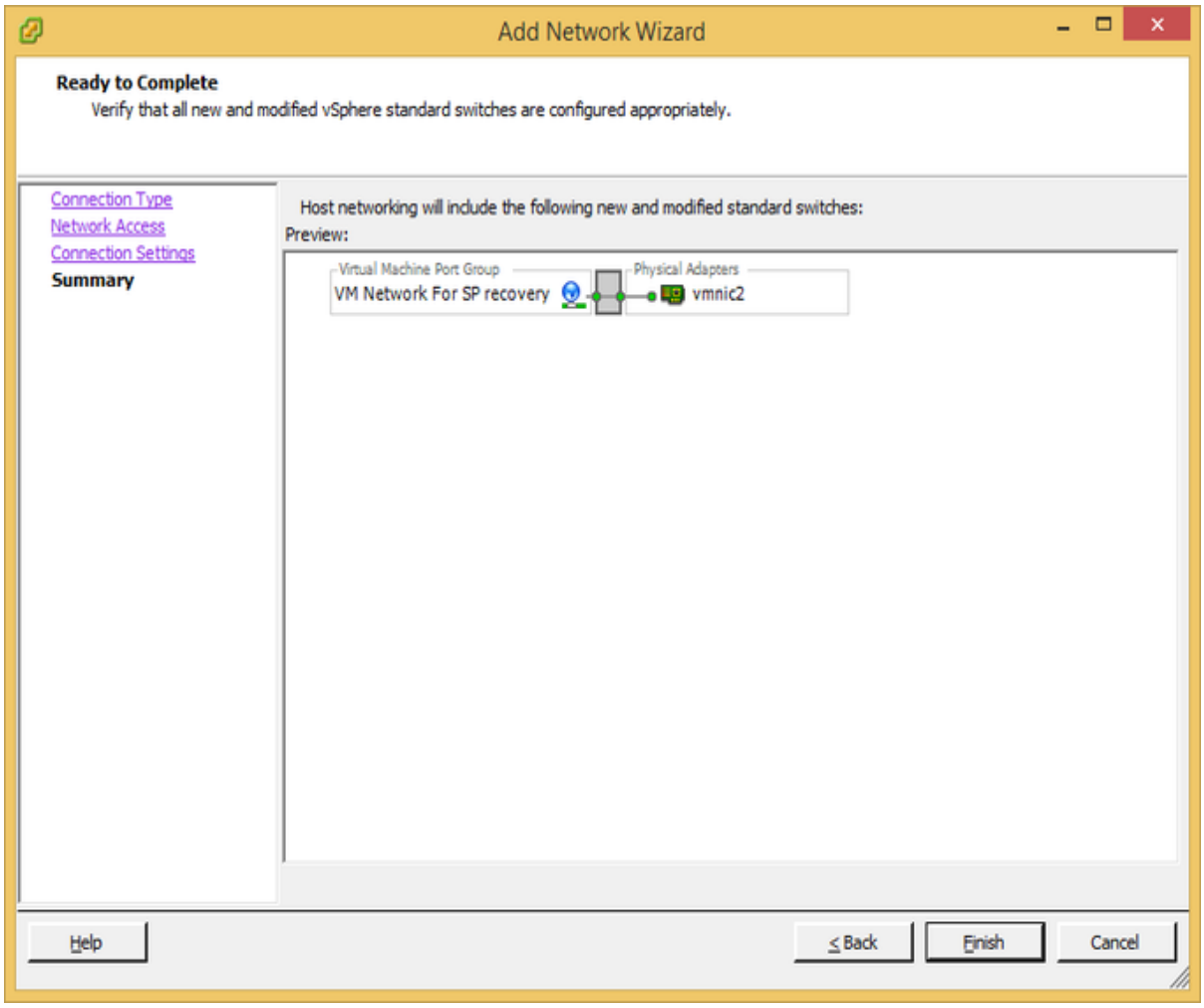


6. Asigne una etiqueta de red al conmutador virtual y un ID de VLAN si es necesario, y haga clic en **Siguiente**.



7. Compruebe que la configuración del conmutador virtual sea correcta y haga clic en **Finalizar**.

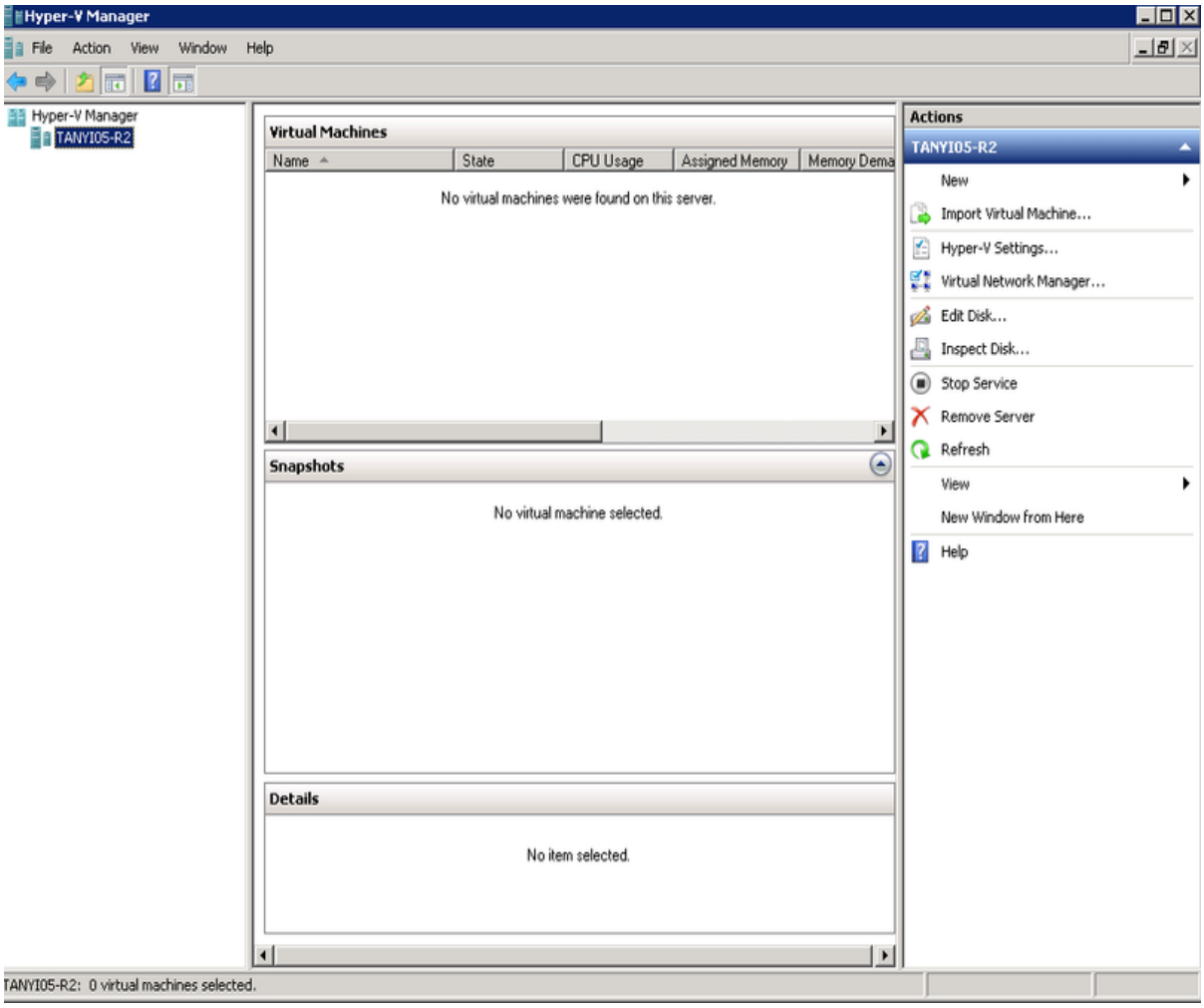
   Al volver a la ficha Configuración de redes, se puede ver que se ha agregado el nuevo conmutador virtual.


Add Network Wizard
Ready to Complete
Verify that all new and modified vSphere standard switches are configured appropriately.
Connection Type
Network Access
Connection Settings
Summary
Host networking will include the following new and modified standard switches:
Preview:
Virtual Machine Port Group
VM Network For SP recovery
Physical Adapters
vmnic2
Help
< Back
Finish
Cancel

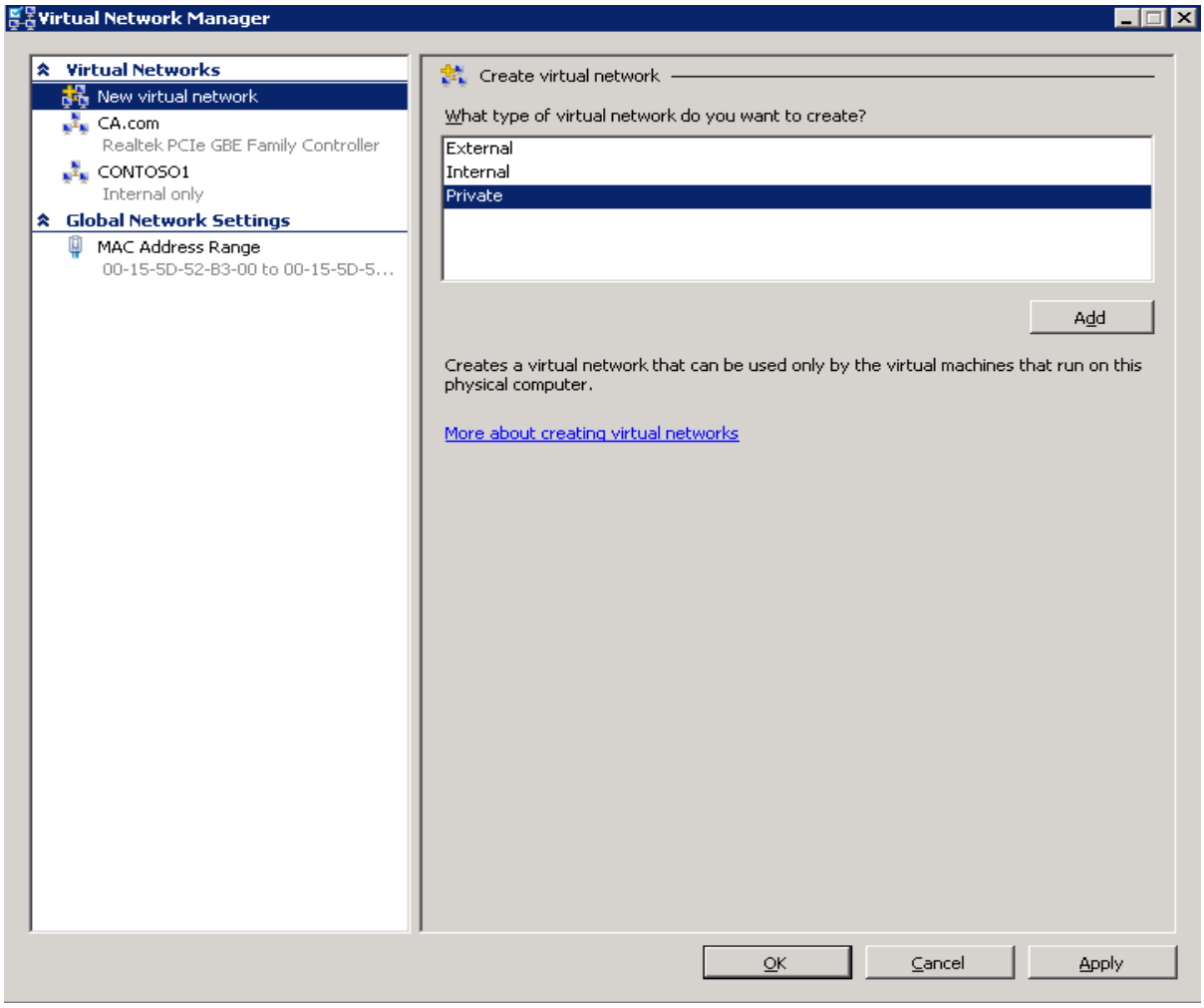
Cómo crear una red aislada para la recuperación de SharePoint en máquinas virtuales de Hyper-V

Siga estos pasos:

1. Inicie sesión en el gestor de Hyper-V.
2. Haga clic en Administrador de red virtual.

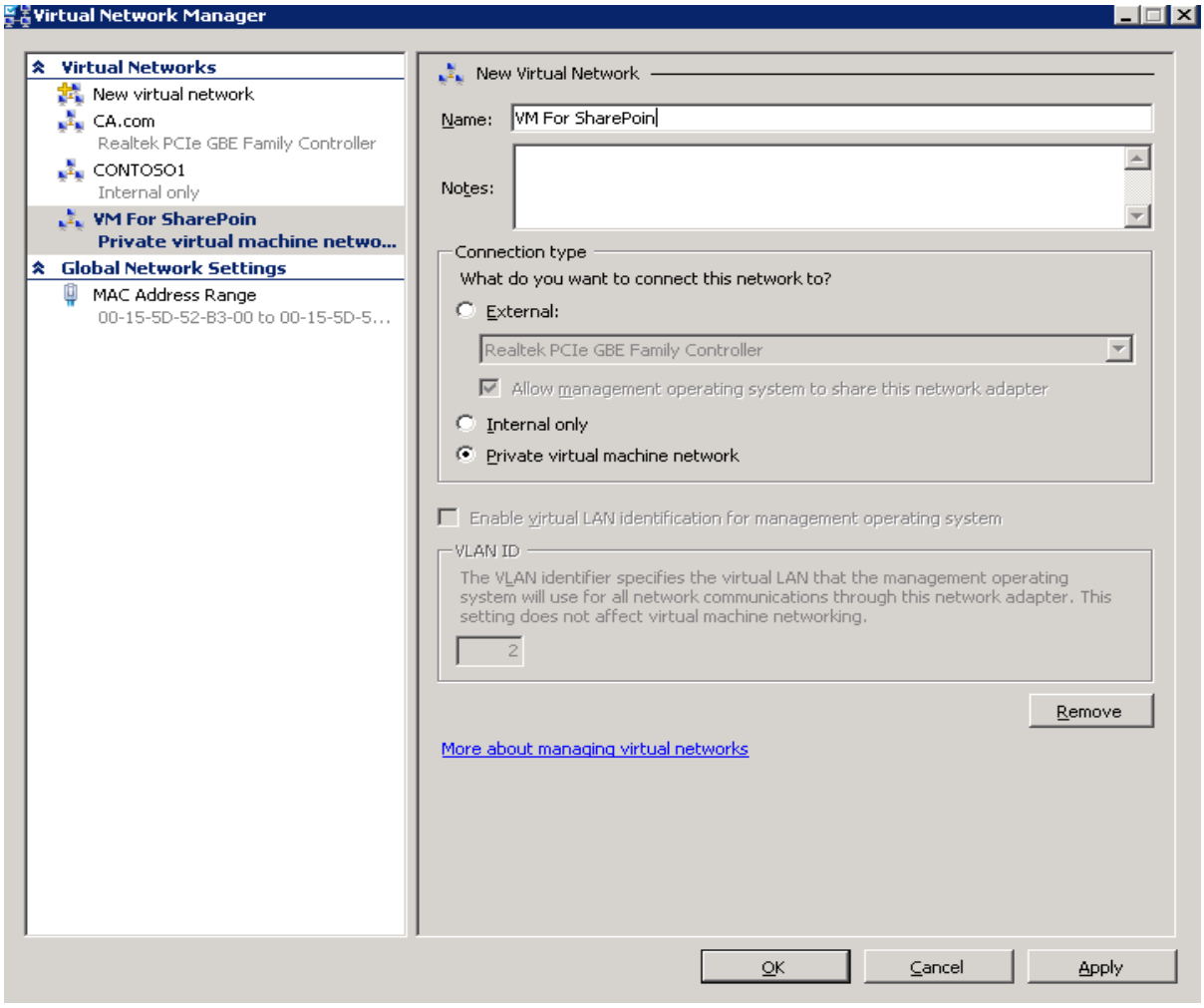


3. Haga clic en Red virtual nueva, seleccione el tipo "Privada" y haga clic en **Agregar**.



4. Escriba un nombre de la red virtual privada y haga clic en Aceptar.

   Se ha agregado la nueva red virtual.


Virtual Network Manager
Virtual Networks
New virtual network
CA.com
Realtek PCIe GBE Family Controller
CONTOSO1
Internal only
VM For SharePoin
Private virtual machine netwo...
Global Network Settings
MAC Address Range
00-15-5D-52-B3-00 to 00-15-5D-5...
New Virtual Network
Name:
VM For SharePoin
Notes:
Connection type
What do you want to connect this network to?
External:
Realtek PCIe GBE Family Controller
Allow management operating system to share this network adapter
Internal only
Private virtual machine network
Enable virtual LAN identification for management operating system
VLAN ID
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
2
Remove
More about managing virtual networks
OK
Cancel
Apply

Capítulo 6: Generación de informes de Arcserve UDP

Esta sección incluye los siguientes temas:

Funcionamiento de los informes de Arcserve UDP

La ficha **informes** proporciona acceso a diferentes tipos de informes, tales como Alertas, Tendencia de los datos, Estado de la copia de seguridad, Distribución de los datos y el Acuerdo de nivel de servicio. El panel izquierdo incluye una lista de los informes que se pueden generar. El panel central muestra los detalles del informe seleccionado y le permite configurar diversos valores de configuración del informe. El informe se genera para un grupo de nodos o servidores. Se puede filtrar también el informe para mostrar información detallada para un nodo individual.

Para obtener más información sobre los informes, consulte Informes de Arcserve UDP.

El informe de detalles incluye los siguientes elementos:

Nodos de la tarea

Muestra el nombre del nodo donde se ejecutan las tareas de los agentes de Arcserve UDP, la máquina virtual basada en host y Virtual Standby.

Nodos protegidos

Muestra el nombre del nodo del Agente y del nodo protegido por el Agente de Arcserve Unified Data Protection, Host-Based VM Backup, Virtual Standby o Arcserve Backup.

Producto

Muestra el producto que está instalado en el nodo. El nombre del producto puede ser Agente de Arcserve Unified Data Protection, Servidor de puntos de recuperación de Arcserve Unified Data Protection, máquina virtual basada en el host o Arcserve Backup.

Filtros/acciones

Muestra las opciones globales y locales de filtros y acciones relacionados con los informes. Para obtener más información, consulte Utilización de filtros y acciones.

Informes de Arcserve UDP

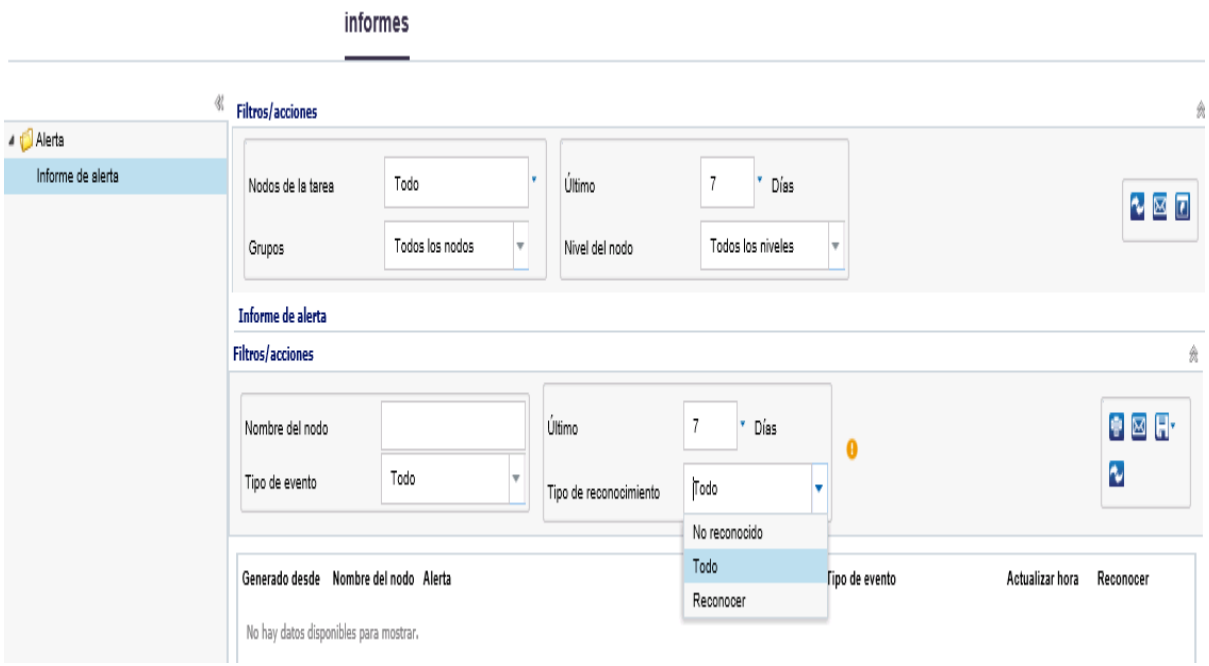
Arcserve UDP proporciona los siguientes tipos de informes:

- Informe de alerta
- Informe de tendencias en el tamaño de la copia de seguridad
- **Informe relacionado con la copia de seguridad:** Arcserve UDP ofrece tres tipos de informes relacionados con la copia de seguridad:
  - Informe del estado de las copias de seguridad del nodo
  - Informe del estado de la protección de la virtualización
  - Informe de la capacidad gestionada
- Informe de distribución de datos en medios
- **Informe del acuerdo de nivel de servicio:** El informe del acuerdo de nivel de servicio muestra los informes de cumplimiento relacionados con el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO)
  - Informe de RPO
  - Informe de RTO
- **Informe del estado de la tarea:** Arcserve UDP facilita la generación del Informe del estado de la tarea para recuperar los detalles acerca de todas las tareas realizadas en un período determinado.

Informes de alerta

Arcserve UDP muestra la información de alerta de los nodos. Además de los filtros y acciones comunes, el Informe de alerta proporciona la capacidad para ordenar el cuadro de mandos de alertas mediante el reconocimiento. De forma pre-determinada, el cuadro de mandos del informe de alerta solo muestra las alertas no reconocidas. Se puede hacer clic en el enlace **Reconocer** que se encuentra en cada alerta para eliminarla de la vista del cuadro de mandos. Si se desea ver el informe con las alarmas reconocidas, seleccione **Reconocer** en la opción **Tipo de reconocimiento** del filtro local.

Informe de alerta

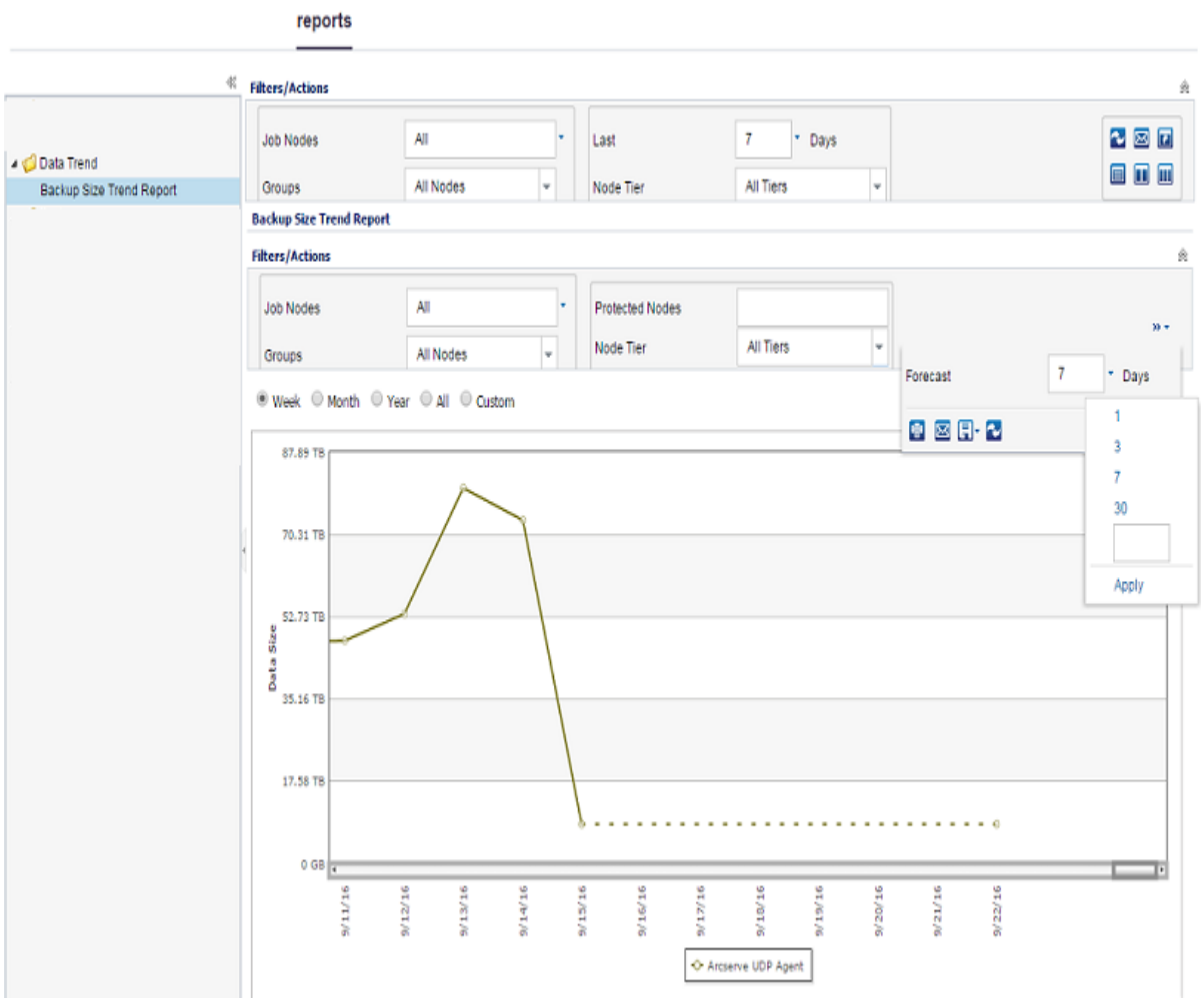


Informes de tendencias en el tamaño de la copia de seguridad

El Informe de tendencias en el tamaño de la copia de seguridad de Arcserve UDP muestra el tamaño de los datos de la copia de seguridad de Arcserve Backup y del Agente de Arcserve Unified Data Protection en una vista histórica y, a continuación, proyecta la tendencia de crecimiento para que el usuario pueda prepararse ante los futuros requisitos de espacio de almacenamiento. Este informe incluye información sobre los nodos que se ejecutan en sistemas operativos Windows y Linux compatibles y permite bajar de nivel para obtener información más detallada para un nodo individual.

Además de los filtros y acciones comunes, el informe de tendencias del tamaño de la copia de seguridad proporciona la capacidad para consultar los resultados en función del número de **Días**. De forma predeterminada, no se puede aplicar el filtro para el **último** día. En su lugar, se puede utilizar el filtro del modo **Vista** (semana/mes/año/personalizado).

Informe de tendencias en el tamaño de la copia de seguridad


reports
Data Trend
Backup Size Trend Report
Filters/Actions
Job Nodes
All
Last
7
Days
Groups
All Nodes
Node Tier
All Tiers
Backup Size Trend Report
Filters/Actions
Job Nodes
All
Protected Nodes
Groups
All Nodes
Node Tier
All Tiers
Forecast
7
Days
Week
Month
Year
All
Custom
1
3
7
30
Apply
87.89 TB
70.31 TB
52.73 TB
35.16 TB
17.58 TB
0 GB
Data Size
9/11/16
9/12/16
9/13/16
9/14/16
9/15/16
9/16/16
9/17/16
9/18/16
9/19/16
9/20/16
9/21/16
9/22/16
Arcserve UDP Agent

Informes del estado de las copias de seguridad del nodo

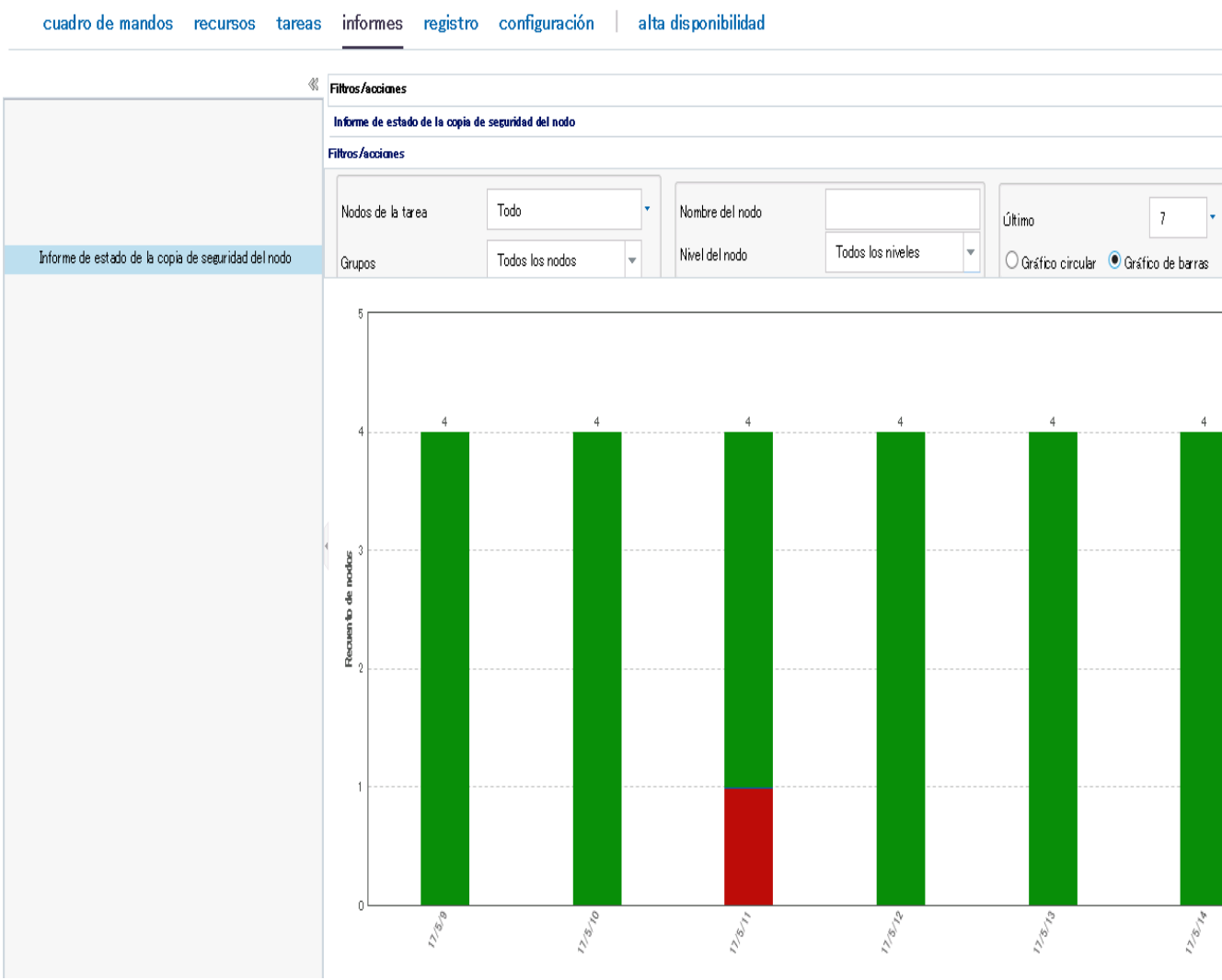
Arcserve UDP muestra el estado de la copia de seguridad más reciente de todos los nodos durante el período de tiempo específico. Este informe le permite ver información detallada sobre los nodos basándose en categorías como el tipo seleccionado de grupos y nivel de nodo.

Además de los filtros y acciones comunes, el informe del estado de las copias de seguridad del nodo proporciona la capacidad para consultar los resultados en función del número de **Días**. En el gráfico de barras, el número del nodo es visible por encima de cada barra.

El informe muestra el estado de tarea siguiente:

- **Correcto:** Proporciona una lista de tareas que se han realizado correctamente.
- **Erróneo:** Proporciona una lista de tareas que han producido un error.
- **Incompleto:** Proporciona una lista de tareas que han finalizado con el estado incompleto.
- **Cancelado:** Proporciona una lista de tareas que se han cancelado.
- **Perdido**: Proporciona una lista de tareas que no se han intentado.
- **Sin copia de seguridad:** Proporciona una lista de los nodos que no tienen ningún plan asignado o de los nodos que tienen un plan asignado pero que todavía están esperando para poder ejecutar las copias de seguridad.

Informe del estado de las copias de seguridad del nodo:

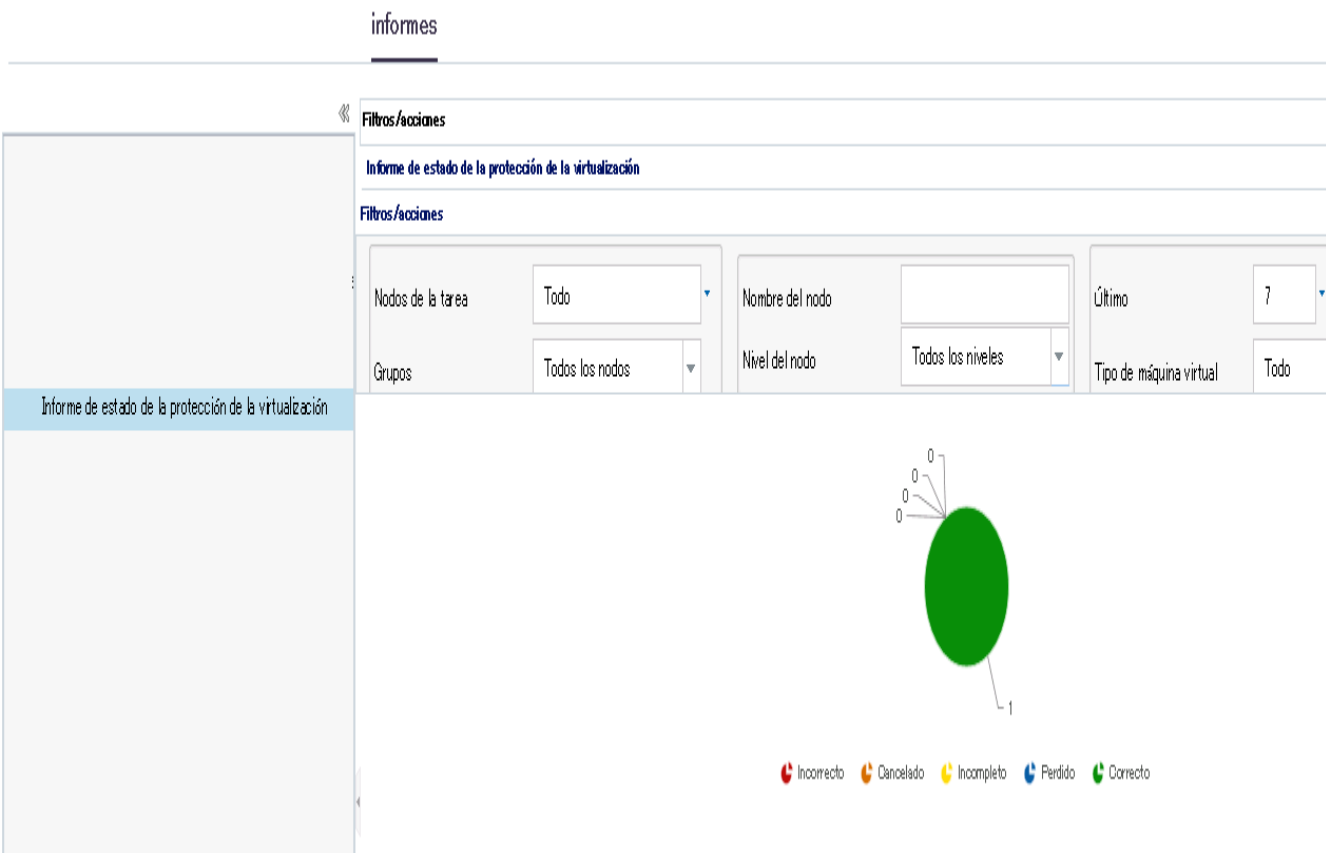

cuadro de mandos
recursos
tareas
informes
registro
configuración
alta disponibilidad
Filtros/acciones
Informe de estado de la copia de seguridad del nodo
Filtros/acciones
Informe de estado de la copia de seguridad del nodo
Nodos de la tarea
Todo
Grupos
Todos los nodos
Nombre del nodo
Nivel del nodo
Todos los niveles
Último
7
Gráfico circular
Gráfico de barras
Recuento de nodos
5
4
3
2
1
0
4
4
4
4
4
4
17/5/9
17/5/10
17/5/11
17/5/12
17/5/13
17/5/14

Informes del estado de la protección de la virtualización

Se muestra el último estado de la copia de seguridad de las máquinas virtuales protegidas por Host-based VM Backup, Virtual Standby o Arcserve Backup. Este informe le permite ver información durante un período de tiempo especificado y obtener detalles para mostrar más información detallada acerca de cada categoría seleccionada.

Además de los filtros y acciones comunes, el informe del estado de la protección de la virtualización proporciona la capacidad para consultar los resultados en función del número de **Días** y la capacidad para consultar los informes como gráficos circulares o como tablas.

Informe del estado de la protección de la virtualización



Informes de la capacidad gestionada

Muestran el tamaño de los datos sin formato de la última copia de seguridad completa correcta para cada nodo protegido por Arcserve Backup, el Agente de Arcserve Unified Data Protection y Host-Based VM Backup.

Para obtener más detalles sobre los filtros y acciones, consulte los filtros y acciones comunes.

Notas:

- La introducción de un valor en el filtro **Último día** no modifica el resultado del filtro global. Cuando se aplica el filtro, se muestran los valores más recientes independientemente del número de días que se proporcione.
- Los datos relacionados con la copia de seguridad del nodo en el almacén de datos suprimido pueden aparecer como el informe de la capacidad gestionada a menos que la copia de seguridad se ejecute en el destino más reciente de la copia de seguridad. Por ejemplo, si se ha modificado el plan para ejecutar copias de seguridad en el almacén de datos DS2 y se ha suprimido el almacén de datos DS1, entonces a menos que se ejecute la copia de seguridad en DS2, los datos suprimidos de DS1 todavía pueden aparecer en el informe.
- En el área de cuadrícula del informe, las tres siguientes columnas se aplican solo a los nodos de máquina virtual protegidos por la copia de seguridad sin agente basada en host:

  Espacio utilizado de los volúmenes (máquina virtual)

  Indica la suma del espacio utilizado de todos los volúmenes dentro del sistema operativo invitado de la máquina virtual.

  Para Windows: Hace referencia a la suma del espacio utilizado de todos los volúmenes NTFS.

  Para la máquina virtual de Linux: Hace referencia a la suma del espacio utilizado de todos los volúmenes.

  Para la máquina virtual de Linux, solo la máquina virtual de VMware es compatible para esta columna. En este caso, es necesario actualizar el nodo de la máquina virtual con credenciales raíz. Tanto si es una máquina virtual de Linux de VMware sin credenciales como si es una máquina virtual de Linux de Hyper-V, esta columna estará vacía.

  Para la compatibilidad con la máquina virtual de Linux, el equipo de CentOS o VMware Red Hat y las máquinas virtuales de Linux de Hyper-V tienen limitaciones. Para obtener más detalles, consulte la sección

Problemas conocidos de las Notas de la versión de Arcserve UDP v6 Actualización 1.

Tamaño de lectura de la copia de seguridad sintética

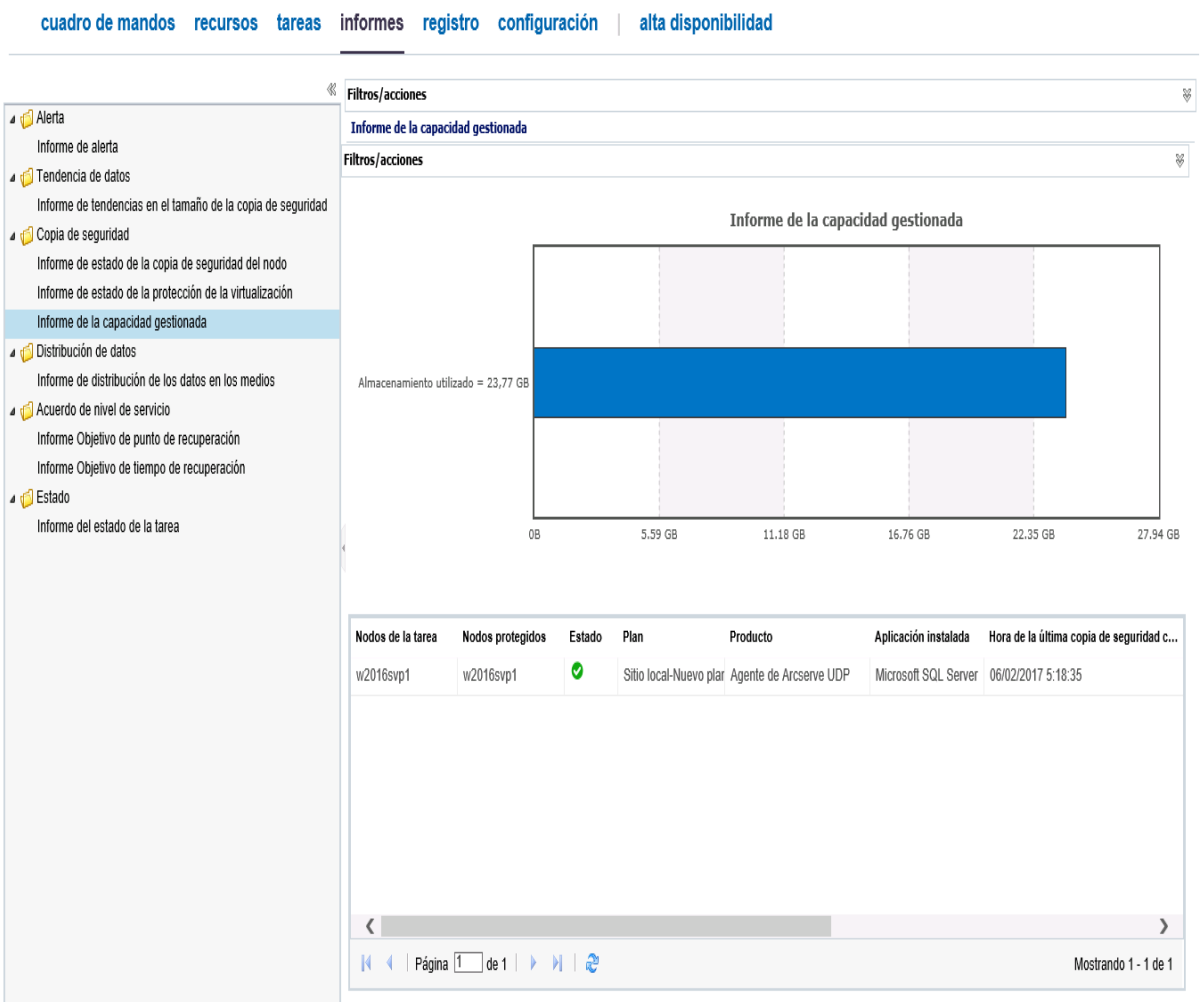
Indica el tamaño total leído durante la copia de seguridad.

Tamaño de aprovisionamiento del disco virtual

Indica la suma del tamaño de aprovisionamiento de todos los discos virtuales de la máquina virtual.

- Por lo general, la columna Tamaño de los datos sin formato indica el tamaño de los datos escritos en el destino de la copia de seguridad. En el caso de las copias de seguridad sin agente basadas en host, puede ser, o no, igual al tamaño de lectura de la copia de seguridad sintética, ya que Arcserve UDP no escribe bloques de datos con solo ceros en el destino de la copia de seguridad. En otras palabras, los bloques de datos de solo ceros se omiten durante la copia de seguridad. Además, para los nodos de máquina virtual protegidos por la copia de seguridad sin agente basada en host, se pueden personalizar los datos que se muestran para Tamaño de los datos sin formato mediante la configuración de varios valores de registro. Para obtener más información sobre cómo configurar los valores de registro y los comportamientos asociados, consulte Funcionamiento del tamaño de los datos sin formato en el Informe de la capacidad gestionada para la copia de seguridad de máquina virtual sin agente basada en el host.

Informe de la capacidad gestionada

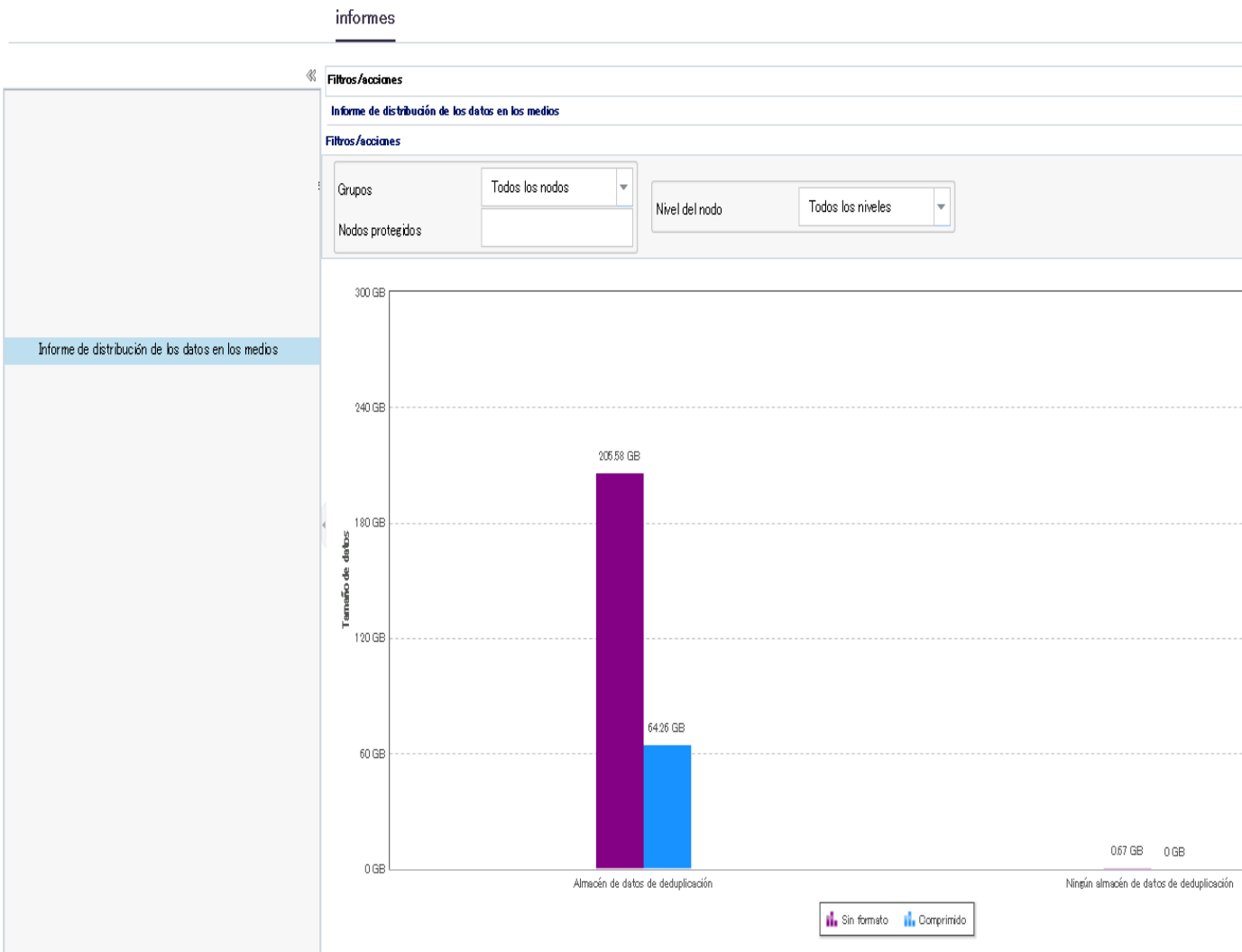

cuadro de mandos
recursos
tareas
informes
registro
configuración
alta disponibilidad
Alerta
Informe de alerta
Tendencia de datos
Informe de tendencias en el tamaño de la copia de seguridad
Copia de seguridad
Informe de estado de la copia de seguridad del nodo
Informe de estado de la protección de la virtualización
Informe de la capacidad gestionada
Distribución de datos
Informe de distribución de los datos en los medios
Acuerdo de nivel de servicio
Informe Objetivo de punto de recuperación
Informe Objetivo de tiempo de recuperación
Estado
Informe del estado de la tarea
Filtros/acciones
Informe de la capacidad gestionada
Filtros/acciones
Informe de la capacidad gestionada
Almacenamiento utilizado = 23,77 GB
0B
5.59 GB
11.18 GB
16.76 GB
22.35 GB
27.94 GB
Nodos de la tarea
Nodos protegidos
Estado
Plan
Producto
Aplicación instalada
Hora de la última copia de seguridad c...
w2016svp1
w2016svp1
Sitio local-Nuevo plar
Agente de Arcserve UDP
Microsoft SQL Server
06/02/2017 5:18:35
Página 1 de 1
Mostrando 1 - 1 de 1

Informes de distribución de los datos en los medios

Muestra el tamaño de los datos de la copia de seguridad reales (sin formato) y comprimidos para los diferentes tipos de destino (deduplicación o de no deduplicación y un destino local). Este informe permite ver todos los nodos, incluidos los nodos del Agente de Arcserve Backup y Arcserve UDP. Para ver la información sobre los datos de Arcserve Backup, active la opción **Programación de la sincronización de datos de Arcserve Backup** en la ficha **configuración**. Para ver la información más reciente, haga clic en **Ejecutar ahora** en la ficha configuración.

Para obtener más detalles sobre los filtros y acciones, consulte los filtros y acciones comunes.

Informe de distribución de datos en medios



Nota: La distribución de datos en un informe de medios depende de los datos de los puntos de recuperación disponibles en el destino de la copia de seguridad. Se

puede utilizar la opción **Actualización** para iniciar una sincronización a petición y obtener el estado más reciente en los informes.

Informes de RPO

El Informe Objetivo de punto de recuperación (RPO) es el informe de cumplimiento que muestra el modo en que se distribuyen los puntos de recuperación en el entorno de la copia de seguridad. El informe ayuda al usuario a evaluar cuáles son el punto más antiguo y el punto más reciente en el tiempo a los que puede volver el nodo en el caso de un desastre. Puesto que el informe de RPO está relacionado con el destino de la copia de seguridad, el informe se rellena con datos cuando ya hay algunas copias de seguridad listas. El informe se rellena a partir de una actualización a petición o de acuerdo a una programación.

Nota: El informe se rellena directamente desde el Cuadro de mandos de Arcserve UDP. Al hacer clic dentro de la gráfica de barras de RPO en un mes en el Cuadro de mandos, se mostrará la pantalla de informe de RPO para ese mes específico en la página de RPO.

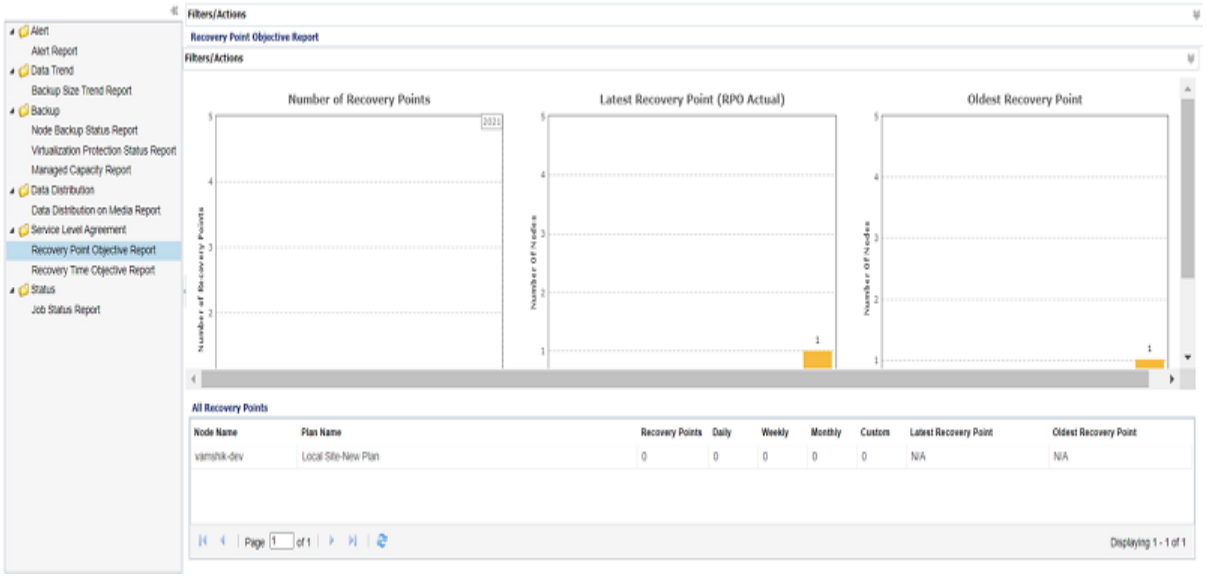
La gráfica de barras de RPO proporciona la siguiente información:

- Distribución mensual de los puntos de recuperación en el destino de la copia de seguridad
- Antigüedad del punto de recuperación más reciente disponible para cada nodo
- Antigüedad del punto de recuperación más antiguo disponible para cada nodo
- Números proporcionados en la parte superior de cada barra.
- *Tipo de destino* permite seleccionar el tipo de destino. Por ejemplo, un destino de la nube, el servidor de puntos de recuperación y el recurso compartido local.
- *Nombre de destino* permite seleccionar un destino de la lista de destinos que aparece como resultado de la opción que se ha seleccionado como tipo de destino.
- Al hacer clic en una barra específica de cualquiera de los siguientes tres gráficos muestra resultados específicos: *Número de puntos de recuperación* para cada mes, *Antigüedad del punto de recuperación más reciente* y *Antigüedad del punto de recuperación más antiguo*.

En la gráfica de barras de RPO, la sección Todos los puntos de recuperación muestra información como Nombre de nodo, Nombre del plan, Puntos de recuperación, Diario, Semanal, Mensual, Personalizado, Último punto de recuperación y Punto de recuperación anterior.

Además de los filtros y acciones comunes, los informes de RPO proporcionan la única opción de **Actualización** en el filtro local.

Informe de RPO



Nota: El informe depende de los datos de los puntos de recuperación disponibles en el destino de la copia de seguridad. Se puede utilizar la opción **Actualización** para iniciar una sincronización a petición y obtener el estado más reciente en los informes.

Informes de RTO

El Informe Objetivo de tiempo de recuperación (RTO) es el informe de cumplimiento que muestra si el objetivo de tiempo de recuperación se ha cumplido para todos los tipos de tarea de recuperación ejecutados. El informe de RTO muestra los tipos de estado siguientes:

- **RTO cumplido:** La tarea de recuperación ha cumplido el objetivo definido.
- **RTO no cumplido:** La tarea de recuperación no ha cumplido el objetivo definido.
- **RTO no definido**: El objetivo no se ha definido para la tarea de recuperación.
- **RTO no probado:** Se ha definido el objetivo de tiempo de recuperación pero aún no se ha probado la tarea.

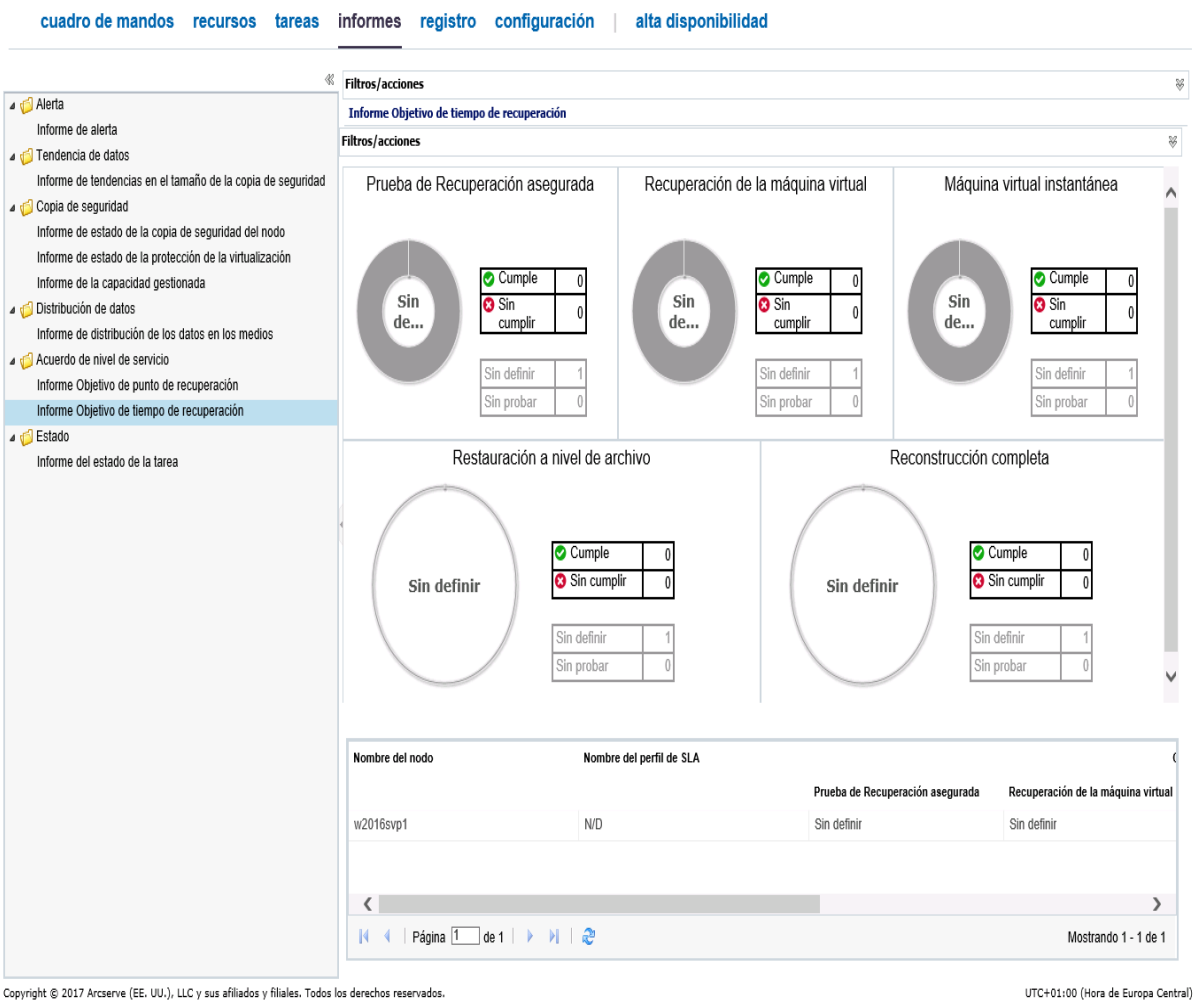
Se pueden definir objetivos de tiempo de recuperación para todas las tareas de recuperación. Para obtener más información, consulte Creación de un perfil de acuerdo de nivel de servicio.

Además de los filtros y acciones comunes, los informes de RPO proporcionan las opciones únicas **Perfil de SLA** y Estado del RTO en el filtro local.

Nota: El informe de RTO no admite las tareas de reconstrucción completa que se ejecutan para las tareas de copia de seguridad configuradas en el destino local.

Cuadro de mandos del informe de RTO

Consideraciones sobre el informe de RTO	Descripción
Parámetros considerados para generar el gráfico de RTO	• Cumplido • No cumplido • Sin probar
Fórmula para definir el porcentaje del estado de RTO (%)	Nodos asignados del perfil del SLA/Total*100
Codificación de color utilizada en el gráfico	• Cumplido = Verde • No cumplido = Rojo • No probado = Gris

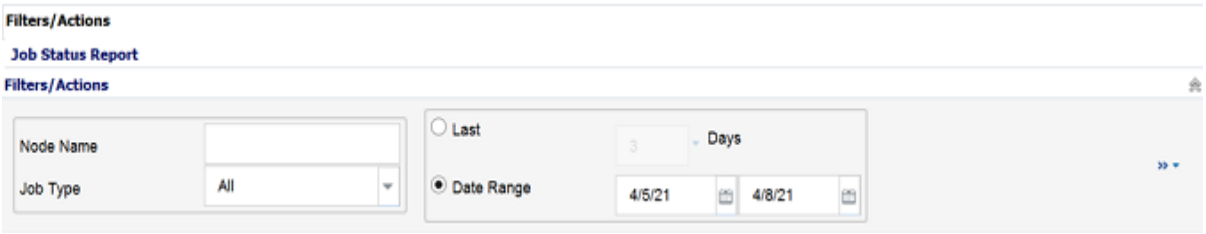

cuadro de mandos
recursos
tareas
informes
registro
configuración
alta disponibilidad
Alerta
Informe de alerta
Tendencia de datos
Informe de tendencias en el tamaño de la copia de seguridad
Copia de seguridad
Informe de estado de la copia de seguridad del nodo
Informe de estado de la protección de la virtualización
Informe de la capacidad gestionada
Distribución de datos
Informe de distribución de los datos en los medios
Acuerdo de nivel de servicio
Informe Objetivo de punto de recuperación
Informe Objetivo de tiempo de recuperación
Estado
Informe del estado de la tarea
Filtros/acciones
Informe Objetivo de tiempo de recuperación
Filtros/acciones
Prueba de Recuperación asegurada
Recuperación de la máquina virtual
Máquina virtual instantánea
Restauración a nivel de archivo
Reconstrucción completa
Sin definir
Cumple
Sin cumplir
Sin definir
Sin probar
Nombre del nodo
Nombre del perfil de SLA
Prueba de Recuperación asegurada
Recuperación de la máquina virtual
w2016svp1
N/D
Página 1 de 1
Mostrando 1 - 1 de 1
Copyright © 2017 Arcserve (EE. UU.), LLC y sus afiliados y filiales. Todos los derechos reservados.
UTC+01:00 (Hora de Europa Central)

Informes del estado de la tarea

El Informe del estado de la tarea permite generar el estado global de todos los tipos de tarea que se ejecutan en la Consola. Este informe puede ser útil con fines de auditoría. Además de las acciones y de los filtros comunes, el Informe del estado de la tarea permite visualizar los resultados en función del tipo de tarea, del ID de la tarea, del estado de la tarea y del nombre del plan (activo o suprimido). Además, para la duración se muestra el formato de hora en hora-s:minutos:segundos.

Se puede ver el informe del estado de la tarea mediante los filtros locales. La opción Filtros/Acciones contiene lo siguiente:

- **Nombre de nodo:** Filtra el informe del estado de la tarea en función del nombre de nodo.
- **Tipo de tarea:** Filtra el informe del estado de la tarea en función del tipo de tarea.
- **Último:** Muestra el informe del estado de la tarea correspondiente al último número de días.
- **Intervalo de fechas:** Muestra el informe del estado de la tarea durante el intervalo de fechas especificado.



Nota: Se puede seleccionar entre el filtro Último o el filtro Intervalo de fechas según sea necesario. De forma predeterminada, se selecciona el filtro Último y se muestra el estado del informe de la tarea de los últimos 7 días.

En el registro, se puede hacer clic en el ID de tarea para ver los detalles. También se puede ver el estado de la tarea de cada tarea.

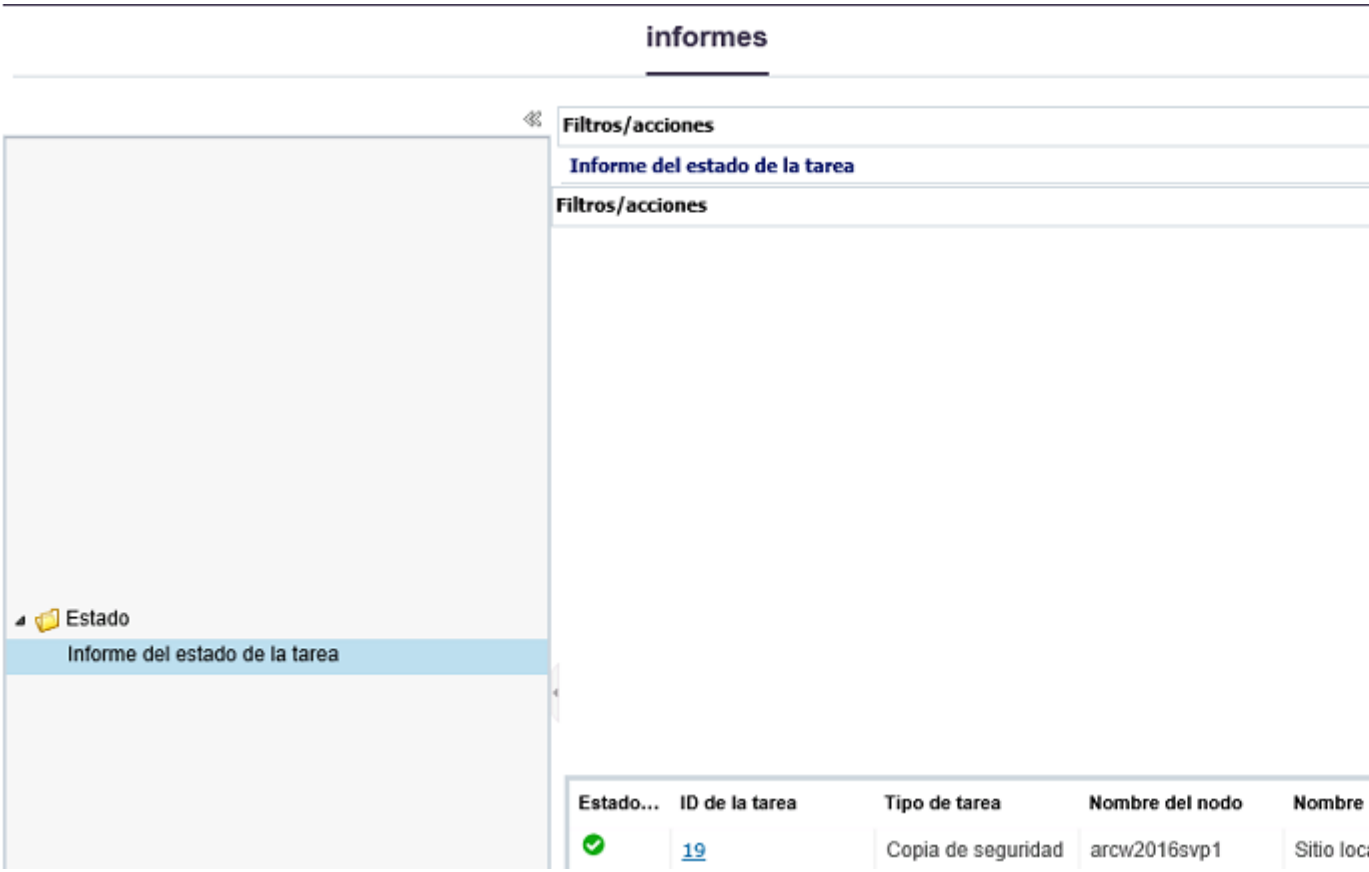
Se pueden ver los valores reales en el origen y en el destino para los tipos de tareas. El informe muestra el estado de tarea siguiente:

- **Correcto:** Proporciona una lista de tareas que se han realizado correctamente.
- **Erróneo:** Proporciona una lista de tareas que han producido un error.

- **Incompleto**: Proporciona una lista de tareas que han finalizado con el estado incompleto.
- **Cancelado:** Proporciona una lista de tareas que se han cancelado.
- **Perdido**: Proporciona una lista de tareas que no se han intentado.

Nota: La duración predeterminada de la retención para recuperar el estado de la tarea es de 180 días. Se puede modificar esta configuración para personalizar los días de retención predeterminados para el borrado definitivo.

Informe del estado de la tarea



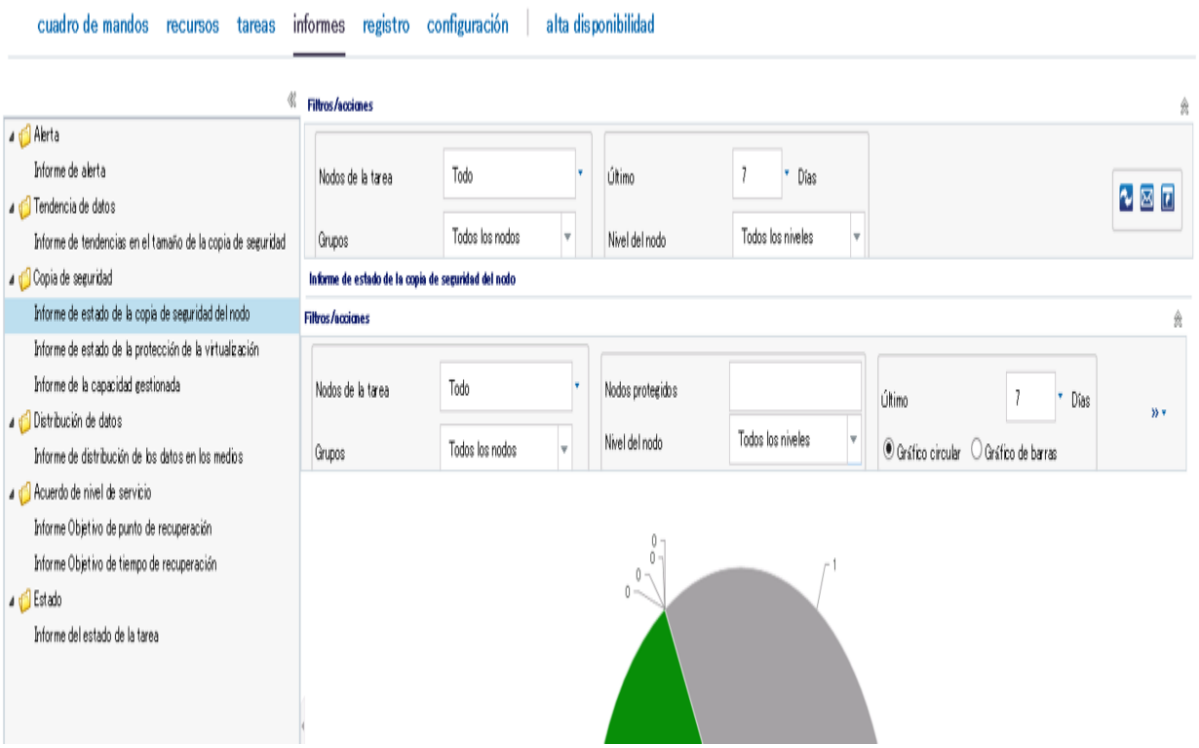
Nota: Cuando hay varias tareas en ejecución, se genera el informe Estado de la tarea. Sin embargo, al hacer clic en el gráfico circular, es posible que los datos detallados mostrados sean incoherentes. Para corregir esta incoherencia, actualice el informe.

Utilización de filtros y acciones

Todas las páginas del informe contienen dos opciones de Filtros/acciones. La primera opción es la opción global que aparece en la parte superior de la página del informe. La otra opción es la opción local que aparece por debajo del nombre del informe en la página del informe y proporciona soluciones relacionadas con un informe en particular.

Como requisito previo, instale Microsoft .NET Framework (versión 3.5) en el equipo en el que se ha instalado la Consola para que la función de exportación de los gráficos de informe pueda exportar las imágenes de un informe correctamente.

Nota: Adobe Flash ya no es necesario y la instalación de .NET Framework como requisito previo permite ver los gráficos.



Filtros

Las opciones globales y locales contienen filtros donde se pueden introducir datos para establecer las opciones de visualización del informe. Las opciones disponibles para los filtros globales son similares para todos los informes. Las opciones disponibles para los filtros locales varían para informes diferentes.

Acciones

Para los informes que utilizan la opción global:

- **Actualizar:** permite actualizar la información relacionada con la página.
- **Programar informes para enviar a través de correo electrónico:** permite crear una programación para que los informes se envíen mediante el correo electrónico. Para obtener más información, consulte la sección Programación de correos electrónicos.

  Nota: Un correo electrónico de programación exporta un máximo de 5000 registros.
- **Restablecer:** permite cambiar todos los parámetros del filtro a los valores predeterminados.
- **La vista de informes solo muestra un informe:** permite ver un informe en un panel único.
- **La vista de informes muestra varios informes en dos columnas:** permite dividir el panel de visualización del informe en dos columnas para ver varios informes.
- **La vista de informes muestra varios informes en tres columnas:** permite dividir el panel de visualización del informe en tres columnas para ver varios informes.

  Para los informes que utilizan la opción local:
- **Imprimir:** haga clic en el icono para imprimir el informe.

  Nota: Con la impresión solo se puede acceder a los primeros 50 nodos o alertas de la lista completa de datos.
- **Actualizar:** haga clic para actualizar la información relacionada del informe.
- **Correo electrónico:** se puede enviar por correo electrónico el informe. Para obtener más información, consulte Enviar informe mediante correo electrónico.

  Nota: Un correo electrónico exporta un máximo de 10000 registros.
- **Guardar:** se puede utilizar la opción para exportar un informe. Seleccione uno de los formatos disponibles como **CSV**, **PDF** y **HTML**, y, a continuación, haga clic en **Abrir** o en una de las opciones de **Guardar** del cuadro de diálogo mostrado en la parte inferior de la página para exportar el informe.

  Nota: Al utilizar Guardar, solo se puede acceder a los primeros 10000 nodos o alertas de la lista completa de datos.

Cómo trabajar con los informes de Arcserve UDP

Esta sección incluye los siguientes temas:

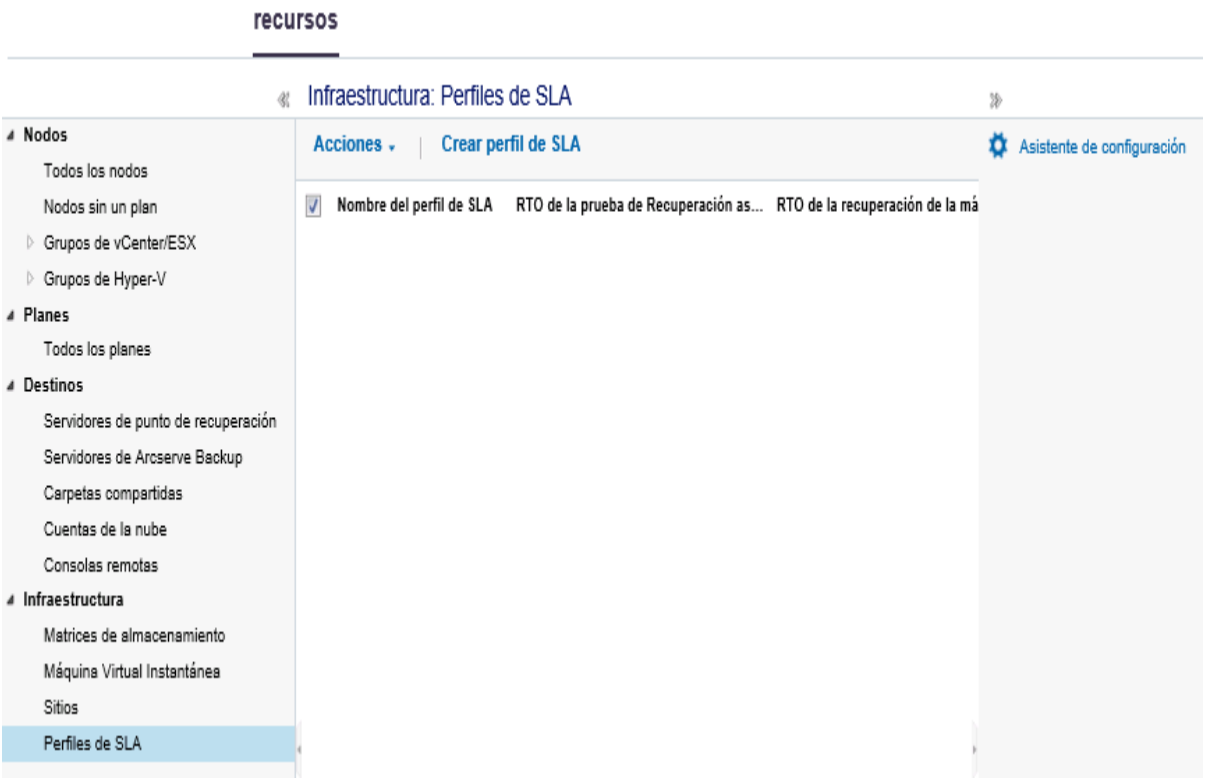
1. Creación de un perfil de acuerdo de nivel de servicio
2. Programación de correos electrónicos
3. Envío de informes por correo electrónico
4. Generación de un informe
5. Personalización de los días de retención para un informe de estado de una tarea
6. Tamaño de los datos sin formato en el informe de la capacidad gestionada para la copia de seguridad de la máquina virtual sin agente basada en el host
7. Visualización de los valores reales en el origen y en el destino para los tipos de tareas

Creación de un perfil de acuerdo de nivel de servicio

Se debe crear un perfil de acuerdo de nivel de servicio para generar los informes de RTO.

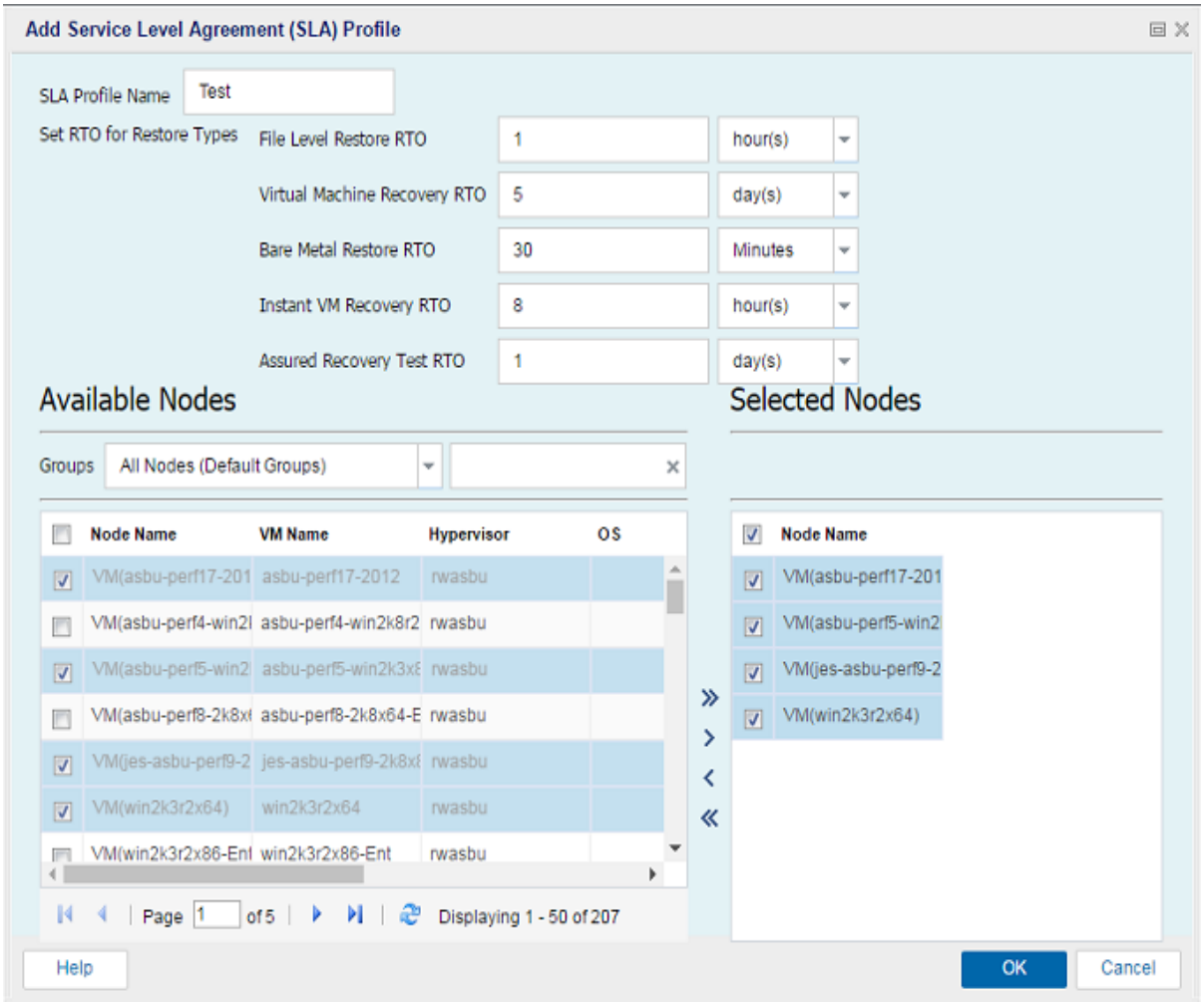
Siga estos pasos:

1. Vaya al panel izquierdo de la ficha **recursos** y haga clic en **Infraestructura** > **Perfil de acuerdo de nivel de servicio**.



2. Haga clic en **Crear un perfil de acuerdo de nivel de servicio** en el panel central.

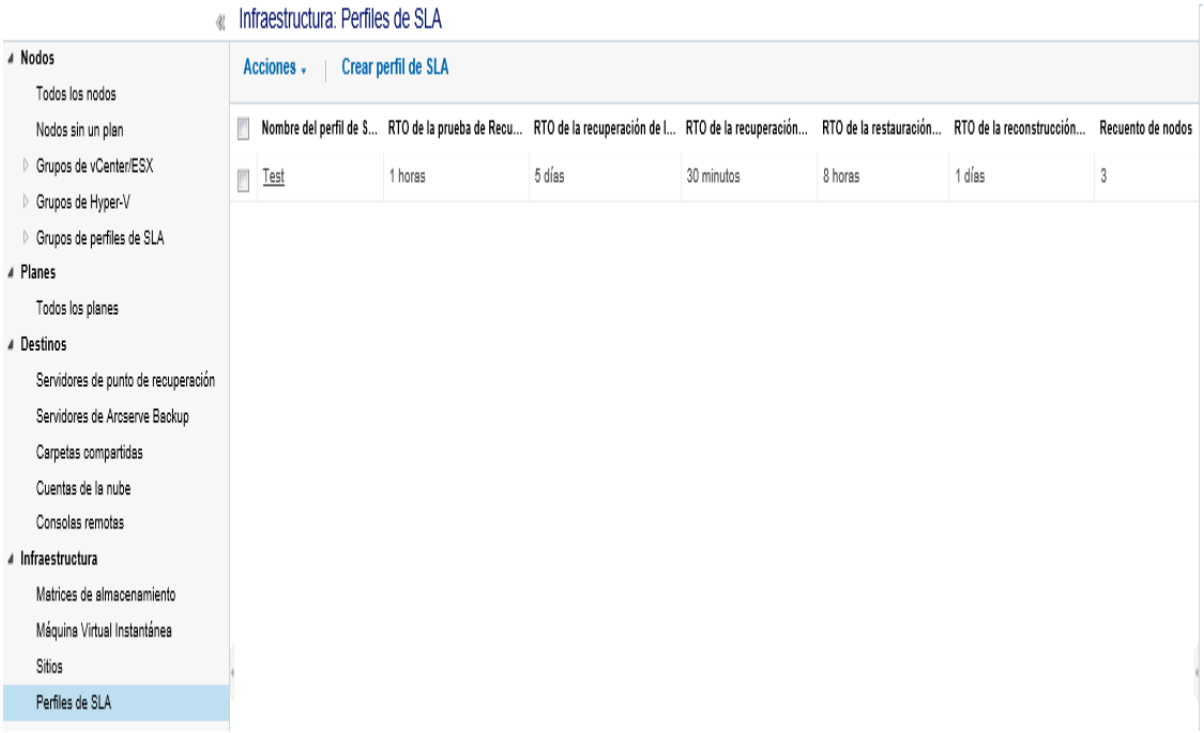
   Se abre **Agregar perfil de acuerdo de nivel de servicio**.



3. En el panel Agregar perfil de acuerdo de nivel de servicio, realice los pasos siguientes:
   a. Introduzca un **Nombre del perfil de acuerdo de nivel de servicio.**
   b. Introduzca el tipo de tiempo y la duración de tiempo para las opciones deseadas en **Establecer RTO para el tipo de restauración**.

      Nota: Para todas las opciones, se puede seleccionar el tiempo en días, horas y minutos.
   c. En la sección **Nodos disponibles**, seleccione las casillas de verificación de los nodos de los que desea generar informes y vaya a la sección **Nodos seleccionados**.
   d. Seleccione uno o más nodos en **Nodos seleccionados** y haga clic en **Aceptar**.

   Se crea el perfil de acuerdo de nivel de servicio y se agrega en Nombre del perfil de acuerdo de nivel de servicio.



4. Para modificar o suprimir el perfil de acuerdo de nivel de servicio existente, seleccione la casilla de verificación del perfil deseado y haga clic en **Acciones**.



Consulte el informe de **RTO** mediante la ficha **informes** para conocer el estado de la tarea para todos los perfiles de acuerdo de nivel de servicio definidos.

Programación de correos electrónicos

Arcserve Unified Data Protection permite programar el envío de los informes por correo electrónico a destinatarios específicos.

Nota: Antes de crear una programación para enviar un correo electrónico, configure los valores de configuración del correo electrónico. Para obtener más información sobre cómo configurar, consulte la sección Configuración de la configuración del correo electrónico y alertas.

Se puede crear una programación y editar la programación.

Creación de la programación

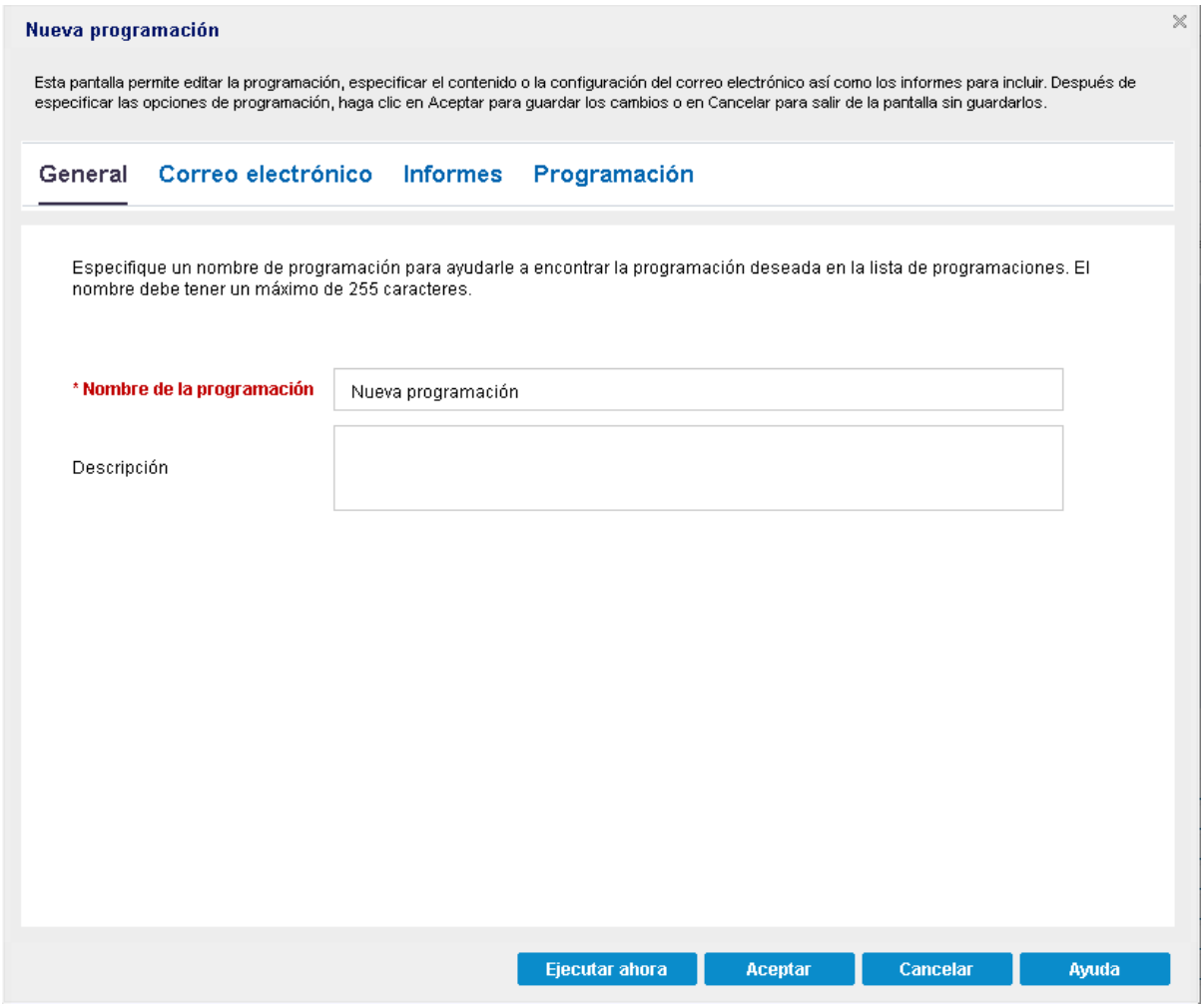
Se puede agregar una programación nueva para el informe de correos electrónicos. Estos correos electrónicos de informe se actualizan, generan y envían automáticamente de la forma programada. Se puede personalizar la programación de los mensajes de correo electrónico de informe. La aplicación permite definir el contenido del correo electrónico, los informes para adjuntar, el destinatario de los informes y la fecha y hora para enviar el informe. Los informes seleccionados muestran información detallada en el formato de tabla dentro del correo electrónico.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection.
2. Haga clic en **informes** en la barra de exploración.
3. En la esquina superior derecha de cualquier informe, haga clic en la sección **Filtros/acciones** global.
4. En la lista expandida, seleccione el icono de correo electrónico para abrir el cuadro de diálogo **Programar informes para enviar a través de correo electrónico**.

   Se muestra el cuadro de diálogo **Programar correos electrónicos**.
5. Haga clic en **Nuevo** en el cuadro de diálogo **Programar correos electrónicos**.

   Se muestra el cuadro de diálogo **Nueva programación**.



Se muestran las siguientes fichas:

- **General:** especifique un nombre y descripción (opcional) para la nueva programación.
- **Correo electrónico:** especifique la configuración del correo, el contenido y los archivos adjuntos para la programación de correo electrónico.
- **Informes:** seleccione los informes específicos que se desea incluir en el correo electrónico.
- **Programación:** especifique una programación para el correo electrónico.

6. Rellene los campos obligatorios en cada ficha.
7. Haga clic en **Aceptar** para guardar la programación.

   La programación nueva se agrega al cuadro de diálogo **Programar correos electrónicos**.

   Nota: No haga clic en **Aceptar** si se desea ver el informe inmediatamente.

8. (Opcional) Para ver el informe inmediatamente, haga clic en **Ejecutar ahora**.

   El informe se envía a los destinatarios.

Edición de la programación

Al utilizar Arcserve UDP se podrá actualizar una programación que se ha agregado mediante la Creación de la programación.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection.
2. Haga clic en la ficha **informes**.
3. Haga clic en la sección **Filtros/acciones** global.
4. En la lista expandida, seleccione el icono de correo electrónico para abrir el cuadro de diálogo **Programar correos electrónicos**.
5. Haga clic en **Editar** en el cuadro de diálogo **Programar correos electrónicos**.

   El cuadro de diálogo **Editar programación** se muestra.
6. Actualice los detalles de la programación y haga clic en **Aceptar**.

   La programación actualizada se muestra en el cuadro de diálogo **Programar correos electrónicos**.

   Nota: No haga clic en **Aceptar** si se desea ver el informe inmediatamente.
7. (Opcional) Para ver el informe actualizado inmediatamente, haga clic en **Ejecutar ahora**.

   El informe se envía a los destinatarios.

Enviar informe mediante correo electrónico

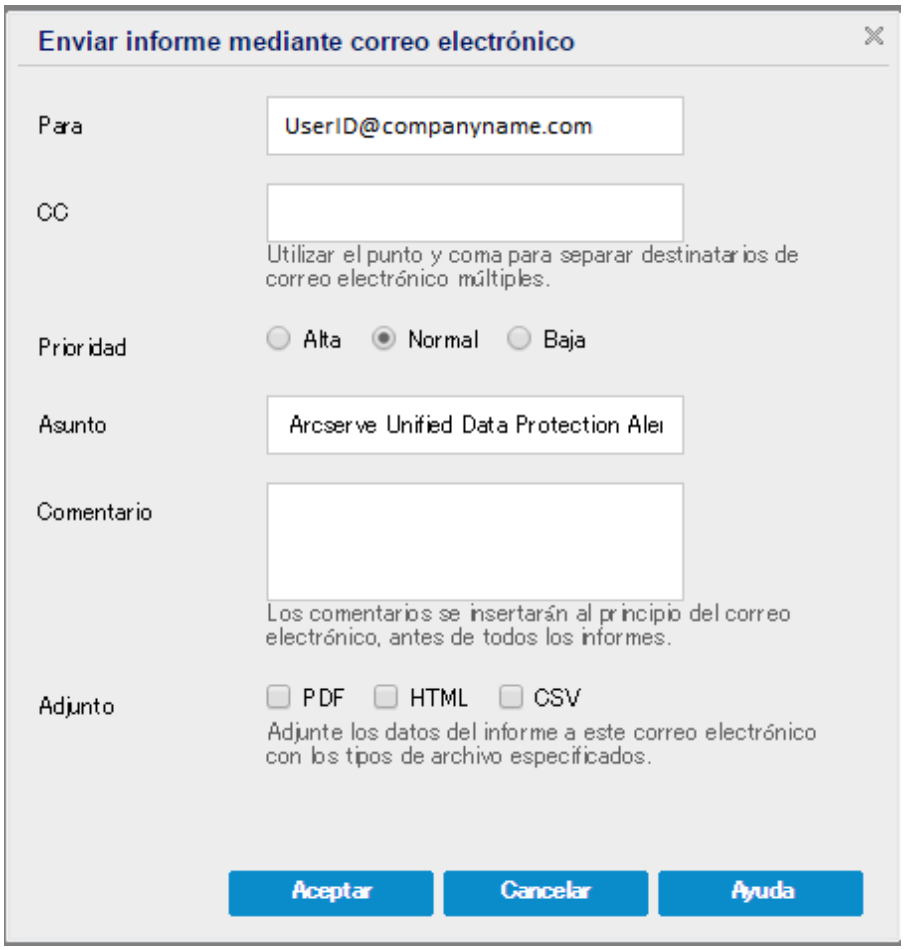
Arcserve Unified Data Protection permite enviar informes individuales a destinatarios específicos. Al enviar el informe por correo electrónico, el contenido es el mismo que el impreso y todos los esquemas gráficos se envían como imágenes incrustadas.

Nota: Antes de utilizar la opción **Enviar informe por correo electrónico**, configure los valores de **Configuración del correo electrónico**. Para obtener más información sobre cómo configurar, consulte la sección Configuración de la configuración del correo electrónico y alertas.

Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection.
2. Haga clic en **informes** en la barra de exploración y seleccione uno de los informes.
3. Haga clic en la sección **Filtros/acciones** local, disponible debajo del nombre del informe seleccionado.
4. En la lista expandida, seleccione el icono de correo electrónico para abrir el cuadro de diálogo **Enviar informe mediante correo electrónico**.

   Nota: Si no se ha completado la configuración del correo electrónico, aparecerá un cuadro de diálogo **Advertencia** que informa de que los valores de configuración de los correos electrónicos no se han especificado. Para obtener más información sobre cómo configurar, consulte la sección Configuración de la configuración del correo electrónico y alertas.



5. Rellene los siguientes campos:
   - **Para**: Especifica el destinatario del correo electrónico.

     Nota: El valor predeterminado de este campo es la dirección de correo electrónico especificada en el módulo Configuración del correo electrónico.
   - **CC**: Especifica otros destinatarios (separados por punto y coma) a los que se desea enviar por correo electrónico el informe.
   - **Prioridad**: Especifica la prioridad del correo electrónico. El valor predeterminado de este campo es Normal.
   - **Asunto:** Especifica el asunto del correo electrónico. El valor predeterminado de este campo es el informe que seleccione.
   - **Comentario:** Especifica cualquier información que se desea compartir (opcional).
   - **Archivo adjunto**: Seleccione los formatos para adjuntar los datos del informe.
6. Haga clic en **Aceptar**.

   El correo electrónico se enviará de forma correcta.

Generación de un informe

Se pueden generar informes predeterminados en la ficha **informes.** Se pueden generar los informes en formato CSV, PDF y HTML.

Siga estos pasos:

1. Vaya a la ficha **informes** y seleccione un informe en el panel izquierdo.
2. Haga clic en la lista desplegable **Filtros/acciones** local.
3. Especifique o seleccione los detalles de las opciones del menú desplegable **Filtros/acciones**.
4. En la lista desplegable del botón **Guardar**, haga clic en **CSV**, **PDF** o **HTML**.

   Nota: Las imágenes de gran tamaño o más datos en una página del informe pueden ocultar algunas de las opciones, incluyendo el botón Guardar. Para ver estas opciones, haga clic en el botón Ampliar.



El informe se genera en el formato seleccionado.

Personalización de los días de retención para un informe de estado de una tarea

Los días de retención predeterminados para recuperar un informe sobre el estado de una tarea son 180 días. Se puede modificar el número de días de retención disponibles en la configuración mencionada en ConsoleConfiguration.xml desde la ubicación siguiente:

Archivos de programa\Arcserve\Unified Data Protection\Management\ConfigurationConsoleConfiguration.xml.

Si es necesario, se puede modificar el número de días de retención de la configuración.

```
<PurgeConf>
<!-- retentionDays, defalut value is 180 (180 days).
The unit is day.
Number of days to retent data for console database.-->
<retentionDays>180</retentionDays>
<!-- purgeHourOfDay, defalut value is 0 (0:00 a.m.).
Execute purge job on this time point every day.-->
<purgeHourOfDay>0</purgeHourOfDay>
</PurgeConf>
```

Tamaño de los datos sin formato en el informe de la capacidad gestionada para la copia de seguridad de la máquina virtual sin agente basada en el host

En el nivel de proxy o de máquina virtual, se pueden configurar los siguientes registros:

En el nivel de proxy para todas las máquinas virtuales protegidas por el proxy actual:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

"CountNtfsVolumeSize"=dword:00000001

"ReportZeroIfHavingNonNtfsVolume"=dword:00000001

"BackupZeroBlock"=dword:00000001

En el nivel de máquina virtual para una máquina virtual específica:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\{VM UUID}]

"CountNtfsVolumeSize"=dword:00000001

"ReportZeroIfHavingNonNtfsVolume"=dword:00000001

"BackupZeroBlock"=dword:00000001

Nota: El registro del nivel de máquina virtual prevalece sobre el del nivel de proxy.

Se observan los siguientes comportamientos:

Clave de registro	Valor predeterminado	Posibles valores	Finalidad	Información adicional
GetVMGuestVolumeUsedSize	0	0 o 1	Especifica si se debe contar el espacio utilizado de todos los volúmenes de una máquina vir-	

			tual. 0: Cuenta el tamaño del archivo VMDK de la máquina virtual como el tamaño de los datos sin formato de la máquina virtual. 1: Solo cuenta el espacio utilizado de los volúmenes. **Nota:** Para los clientes de Windows, solo se tienen en cuenta los volúmenes NTFS. Para los clientes de Linux se tienen en cuenta todos los volúmenes.	
ReportZeroIfHavingNonNtfsVolume	0	0 o 1	Especifica el comportamiento de la columna del tamaño de los datos sin	1. Se ignora cuando GetVMGuestVolumeUsedSize=0 2. Solo se aplica a la máquina virtual de Windows

			formato del informe de la capacidad gestionada cuando existen volúmenes que no son NTFS en las máquinas virtuales. 0: El tamaño de los volúmenes que no son NTFS no se considera como parte de la columna del tamaño de los datos sin formato. 1: El tamaño global de los datos sin formato se muestra como 0 cuando existen volúmenes que no son NTFS en la máquina virtual	
BackupZeroBlock	0	0 o 1	Especifica si se deben escribir los bloques de datos de solo ceros en el destino de la copia de seguridad.	1. Se ignora cuando GetVMGuestVolumeUsedSize=1 2. Si se cambia, el valor solo surte efecto después de una copia de seguridad completa

			1: Escribe bloques de datos de solo ceros en el destino de la copia de seguridad. 0: Ignora los bloques de datos de solo ceros como parte de la copia de seguridad.	

Ejemplo

Una máquina virtual tiene un disco virtual de aprovisionamiento fino con el tamaño aprovisionado de 1000 GB. El tamaño del archivo VMDK del disco virtual es de 800 GB, de los cuales 200 GB son bloques de datos de solo ceros. En el sistema operativo invitado de esta máquina virtual hay 2 volúmenes NTFS cuyo espacio utilizado es de 100 y 200 GB respectivamente, así como un volumen FAT32 con 1 GB de espacio utilizado.

Nombres de la clave	Valores predeterminados	Valores personalizados	Configuración personalizada	Valores personalizados
GetVMGuestVolumeUsedSize	0	0	1	1
ReportZeroIfHavingNonNtfsVolume	N/D	N/D	1	1
BackupZeroBlock	0	1	N/D	N/D
Se esperaba DataSizeRaw	600 GB (excluyendo bloques de datos de solo ceros)	800 GB (incluidos los bloques de datos de solo ceros)	300 GB	0

Visualización de los valores reales en el origen y en el destino para los tipos de tareas

La tabla siguiente describe los valores reales en el origen y en el destino que se muestran para todos los tipos de tarea para ayudarle a entender el informe de estado de la tarea:

Tipo de tarea	Valor real en el origen	Valor real en el destino	Comentarios
Copia de seguridad de FS en el almacén de datos (deduplicación/sin deduplicación) - Nodos de Windows y Linux	No está disponible (N/D)	Se muestra como se esperaba	
Copia de seguridad de FS en el recurso compartido de red	N/D	Se muestra como se esperaba	
Restauración de FS desde el recurso compartido de red	N/D	N/D	
Tareas de copia de seguridad de CIFS - Almacén de datos sin deduplicación	N/D	Se muestra como se esperaba	
Tareas de restauración CIFS – Almacén de datos sin no deduplicación	Se muestra como se esperaba	N/D	
Restauración de FS desde el almacén de datos (deduplicación/sin deduplicación)	Se muestra como se esperaba	N/D	
Copia de archivos desde el almacén de datos (deduplicación/sin deduplicación), copia de archivos desde la replicación	Se muestra como se esperaba	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Archivo de archivado desde el almacén de datos (deduplicación/sin deduplicación), archivo de archivado desde la replicación	Se muestra como se esperaba	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.

Copia de archivos/archivo de archivado en un recurso compartido de la red	N/D	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Copia de archivos/restauración del archivo de archivado	N/D	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Archivo de archivado - Suprimir	N/D		**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Tarea de catálogo de FS (basada en el agente/sin agente)	Se muestra como se esperaba	N/D	
Copia de puntos de recuperación desde el almacén de datos (deduplicación, sin deduplicación)	Se muestra como se esperaba	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Copia de puntos de recuperación desde un recurso compartido de la red, recurso local	N/D	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Restauración de la copia de puntos de recuperación en un recurso compartido de red, recurso local	N/D	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Tareas de la máquina virtual instantánea	Se muestra como se esperaba	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Tareas de recuperación asegurada	Se muestra como se espe-	N/D	

	raba		
Reconstrucción completa desde el almacén de datos (deduplicación/sin deduplicación)	Se muestra como se esperaba	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Tareas de Virtual Standby	Se muestra como se esperaba	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Tareas de copia en cinta	Se muestra como se esperaba	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Tareas de replicación, tareas de replicación entre sitios	Se muestra como se esperaba	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Tareas de replicación de MSP	Se muestra como se esperaba	Se muestra como se esperaba	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Servidor de puntos de recuperación Jumpstart desde el recurso compartido de red	Se muestra como se esperaba	N/D	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.
Servidor de puntos de recuperación Jumpstart (almacén de datos de deduplicación/sin deduplicación)	Se muestra como se esperaba	Se muestra como se esperaba	**Nota:** Aquí las columnas Datos protegidos y Almacenamiento utilizado también se muestran como N/D.

Capítulo 7: Gestión de High Availability

Esta sección incluye los siguientes temas:

Cómo funciona High Availability

Si utiliza Unified Data Protection, podrá controlar y gestionar las funciones de Arcserve High Availability desde la ficha **High Availability.** Para gestionar estas funciones, se debe iniciar sesión primero en el servicio de control. Cuando se hace clic en la ficha **High Availability** por primera vez, se abre el cuadro de diálogo **Agregar servicio de control.** Este cuadro de diálogo no aparecerá después.

Gestión de los servicios de control de High Availability

Siga estos pasos:

1. Haga clic en la ficha **High Availability**.

   Se abre el cuadro de diálogo **Agregar servicio de control**.

2. Introduzca los detalles del servicio de control como la dirección IP, el nombre de cuenta, la contraseña, el protocolo y el número de puerto.

3. Haga clic en **Aceptar**.

   El servicio de control especificado se agrega debajo del encabezado Servicios de control y escenarios en el panel izquierdo. Para modificar o suprimir un servicio de control, seleccione Servicio de control y haga clic con el botón secundario del ratón para ver las opciones. Se puede seleccionar también el servicio de control en el panel central y hacer clic en el menú **Acciones**para modificar o suprimir un servicio de control. O haga clic con el botón secundario del ratón en el servicio de control en el panel de navegación.

   Nota: Expanda el servicio de control para ver escenarios, grupos y otros detalles.

Gestión de licencias de High Availability

Siga estos pasos:

1. Haga clic en la ficha **High Availability**.
2. En el panel izquierdo, haga clic en **Servicios de control y escenarios**.

   Se muestra la página **Escenarios y servicios de control**.
3. Seleccione el servicio de control y haga clic en **Registrar**.

   Se abre el cuadro de diálogo **Registro**.
4. Introduzca la clave de registro.
5. Haga clic en **Aceptar**.

   La licencia se registra.

Gestión de escenarios

Arcserve Unified Data Protection permite gestionar los escenarios de HA existentes y se pueden crear escenarios de todo el sistema. Se pueden crear también grupos de escenarios para organizar los escenarios. Las secciones siguientes describen cómo gestionar los escenarios de HA:

- Gestión del grupo de escenarios
- Cómo crear escenarios Todo el sistema
- Gestión de escenarios
- Edición de escenarios
- Gestión de los hosts de los escenarios
- Operaciones en escenarios
- Reconstrucción completa y replicación inversa
- Control de los escenarios

Gestión del grupo de escenarios

Arcserve Unified Data Protection permite gestionar grupos en un servicio de control. Se pueden agregar, renombrar, suprimir, marcar y publicar comentarios para un grupo.

Siga estos pasos:

1. Seleccione un servicio de control gestionado en el panel izquierdo.

   Todos los grupos del servicio de control se muestran en el panel central.

2. Haga clic en el menú desplegable **Acciones** y, a continuación, haga clic en uno de los siguientes:

   Agregar grupo de escenarios

   Crea un grupo.

   Seleccione un grupo para realizar las acciones siguientes:

   Renombrar grupo de escenarios

   Renombra el grupo.

   Eliminar grupo de escenarios

   Suprime el grupo. No se puede eliminar un grupo si se tienen escenarios dentro del grupo.

   Indicador y comentario

   Marca el grupo con indicadores de diversos colores y le permite agregar comentarios al indicador. Utilice los indicadores para personalizar e identificar fácilmente su grupo.

3. Opcionalmente, haga clic con el botón secundario del ratón en un grupo del panel izquierdo para agregar, suprimir o renombrar un grupo del servicio de control seleccionado.

   El grupo se agrega o se actualiza basándose en la selección.

Cómo crear escenarios Todo el sistema

Siga estos pasos:

1. En el panel izquierdo, haga clic en **Escenarios y servicios de control** y, a continuación, haga clic en un servicio de control gestionado.

   Todos los grupos de escenarios del servicio de control se enumeran.

2. Haga clic en un grupo de escenarios.

   La página **Escenarios** se muestra en el panel central.

3. En el panel central, haga clic en **Crear escenario**.

   Nota: Opcionalmente, en el panel izquierdo, se puede hacer clic con el botón secundario del ratón y, a continuación, hacer clic en **Crear escenario**.

   Se abre el asistente **Crear sistema completo** y se abre el cuadro de diálogo **Seleccionar servidor y tipo de producto**.

4. Introduzca el nombre del escenario, seleccione el tipo de producto y especifique si se desea realizar pruebas de AR.

5. Haga clic en **Siguiente**.

   Aparecerá el cuadro de diálogo **Host máster y réplica**.

6. Introduzca los detalles del máster y de la réplica.

7. Haga clic en **Siguiente**.

   Los motores se verifican en los hosts si se ha seleccionado la opción **Verificar motor en los hosts**. Se pueden instalar también motores en los hosts o desinstalar los motores de los hosts.

8. Haga clic en **Siguiente** después de verificar los motores.

   Aparecerá el cuadro de diálogo **Configuración de volumen**.

9. Seleccione los volúmenes que se desea proteger.

   Nota: Cuando se selecciona la opción **Permitir la exclusión de directorios y archivos**, los archivos pagefile.sys, hyberfil.sys, la información de volumen del sistema, el reutilizador y los archivos y las carpetas reciclados se filtran de manera predeterminada.

10. Haga clic en **Siguiente**.

    Se abre el cuadro de diálogo **Selección de agrupación de recursos**. Se puede seleccionar la agrupación de recursos donde se encuentra la máquina virtual después de la conmutación o durante las pruebas de AR.

11. Haga clic en **Siguiente**.

Se abrirá el cuadro de diálogo **Selección de almacenamiento**.

12. Seleccione el almacén de datos para almacenar la máquina virtual. Opcionalmente, seleccione **Adjudicar y confirmar espacio a petición (mediante un disco dinámico)**. La máquina virtual generada utiliza el aprovisionamiento fino para el disco virtual si se selecciona esta opción.
13. Haga clic en **Siguiente**.

    Se abrirá el cuadro de diálogo **Propiedades del escenario**.
14. Expanda las propiedades, modifíquelas según sea necesario y, a continuación, haga clic en **Siguiente**. Para obtener más información, consulte la Guía del administrador de Arcserve RHA.

    Aparecerá el cuadro de diálogo **Propiedades del servidor máster y réplica**.
15. Revise las propiedades del máster y de la réplica y, a continuación, utilice **Haga clic para editar asignaciones físicas de red**.

    Aparece el cuadro de diálogo **Asignación de adaptador de redes de High Availability**.

    Nota: Si solo hay un adaptador de red virtual en los servidores máster y de réplica, estos se asignan automáticamente.
16. Realice los pasos siguientes:
    a. En **Adaptador de redes de réplica**, haga clic para elegir el adaptador para asignar al adaptador enumerado en la columna Adaptador de redes máster.
    b. En **Aplicar informac. adaptador máster** (valor predeterminado), elija esta opción si Adaptador máster está en el modo Protocolo de configuración dinámica de host.
    c. En **Personalizar información del adaptador**, seleccione para activar los valores de configuración de la dirección IP, puertas de enlace, servidores DNS y servidores WINS. Agregue o elimine la dirección IP, las puertas de enlace, los servidores DNS y los servidores WINS según sea necesario.
17. Haga clic en Aceptar para cerrar el cuadro de diálogo **Asignación de adaptador de redes** y, a continuación, haga clic en **Siguiente** para continuar.

    Se abrirá el cuadro de diálogo **Propiedades de conmutación**.
18. Expanda la propiedad **Redireccionamiento del tráfico de red** y otras propiedades para verificar los valores y, a continuación, haga clic en **Siguiente**.

    Aparecerá el cuadro de diálogo **Inicio de la conmutación y de la replicación inversa**.

19. Especifique el tipo de restauración. Para los escenarios de todo el sistema, la replicación inversa es manual.
20. Haga clic en **Siguiente**.

    Espere mientras el proceso de verificación del escenario se completa y se abre el cuadro de diálogo **Verificación del escenario**.

    Si el proceso Verificación del escenario enumera algún error, deberá solucionarlos con tal de continuar. Si aparecen advertencias, también debería resolverlas para continuar el proceso correctamente. Después de realizar cambios, haga clic en **Reintentar** para repetir la verificación.
21. Haga clic en **Siguiente**.

    Se abrirá el cuadro de diálogo **Ejecutar escenario**.
22. Haga clic en **Finalizar** para guardar los valores de configuración actuales y ejecutar el escenario más tarde.

    Opcionalmente, para ejecutar el escenario instantáneamente, seleccione **Ejecutar ahora después de hacer clic en el botón Finalizar** y, a continuación, haga clic en **Finalizar**.

    Para los escenarios de todo el sistema, elija **Sincronización de volúmenes**.

    Se crea el escenario.

Gestión de escenarios

Cuando se selecciona un servicio de control gestionado en el panel izquierdo, todos los escenarios del servicio de control se muestran en el panel central. Los escenarios se enumeran con su tipo, estado, producto y modo. También se enumeran las estadísticas de RPO/RTO, el uso del spool del master y el progreso de la sincronización. Se pueden realizar diversas operaciones como suprimir, renombrar, marcar o comentar seleccionando un escenario.

Siga estos pasos:

1. En el panel izquierdo, haga clic en **Escenarios y servicios de control** y, a continuación, haga clic en un servicio de control gestionado.

   Todos los grupos de escenarios del servicio de control se muestran en el panel central.

2. En el panel izquierdo haga clic en un grupo de escenarios.

   Los escenarios del grupo de escenarios se muestran en el panel central.

3. Seleccione un escenario.

4. Haga clic en el menú desplegable **Acciones** y, a continuación, haga clic en uno de los siguientes:

   Renombrar escenario

   Renombra el escenario.

   Eliminar escenario

   Suprime el escenario.

   No se puede eliminar un grupo si se tienen escenarios dentro del grupo.

5. Opcionalmente, en el panel izquierdo, haga clic con el botón secundario del ratón en un escenario para suprimir o renombrar el escenario.

   El nodo se ha actualizado.

Edición de escenarios

Arcserve Unified Data Protection permite editar las propiedades de un escenario cuando el escenario está en el estado detenido. Se puede insertar, renombrar o suprimir host o modificar la topología de un escenario.

Siga estos pasos:

1. En el panel izquierdo, haga clic en **Escenarios y servicios de control** y, a continuación, haga clic en un servicio de control gestionado.

   Todos los grupos de escenarios del servicio de control se muestran en el panel central.

2. Del panel izquierdo, haga clic en un grupo de escenarios y, a continuación, haga clic en un escenario.

   Se muestra la página <grupo de escenarios>:<escenario>.

3. Seleccione un host en el escenario.

4. Haga clic en la ficha **Propiedades** y seleccione una de las siguientes opciones en la lista desplegable.

   Propiedades del escenario

   Actualiza las propiedades de los escenarios.

   Propiedades de alta disponibilidad

   Actualiza las propiedades de alta disponibilidad.

   Propiedades del host

   Actualiza las propiedades del host.

   Directorios raíz

   Actualiza los directorios raíz.

   Nota: Esto solo es aplicable para escenarios de todo el sistema.

5. Haga clic en **Guardar** en el menú desplegable **Acción**.

   Las propiedades del escenario se han actualizado.

   Edite la configuración de la plataforma virtual de un escenario de todo el sistema detenido:

   Siga estos pasos:

1. Seleccione un host de réplica en el escenario:

2. Haga clic en la ficha **Propiedades** y en **Propiedades del host** en la lista desplegable.

3. Expanda **Máquina virtual** y haga clic en **Haga clic aquí para editar la configuración de la plataforma virtual...**.

   Aparecerá el cuadro de diálogo del asistente **Configuración de la plataforma virtual**.

4. Seleccione el **Tipo de plataforma virtual** y la dirección IP o nombre de host relacionados.
5. Seleccione la agrupación de recursos para ESX y vCenter o el servidor de host para Citrix Xen.
6. Seleccione el almacenamiento. Para Hyper-V, explore los directorios y seleccione la ubicación de la máquina virtual en el servidor Hyper-V.
7. Haga clic en **Finalizar**.

Edite la asignación del adaptador de redes para la Alta disponibilidad o para la Recuperación asegurada:

Siga estos pasos:

1. Seleccione el host de réplica en el escenario:
2. Haga clic en la ficha **Propiedades** y seleccione **Propiedades del host** en la lista desplegable.
3. Expanda **Máquina virtual** y **Configuración de la plataforma virtual**.
4. Haga clic en **Haga clic aquí para editar las asignaciones físicas de red...** para la propiedad **Asignación de adaptador de redes de High Availability** o para la propiedad **Asignación de adaptador de redes de recuperación asegurada**.

   Aparece el cuadro de diálogo **Asignación de adaptador de redes de High Availability**.

5. Seleccione los adaptadores de redes de réplica para asignar el adaptador de redes máster.

   Se puede personalizar la información del adaptador del adaptador de réplica incluyendo la dirección IP, la puerta de enlace, los servidores DNS y los servidores WINS.

6. Haga clic en **Aceptar**.

   Las asignaciones se modifican y se guardan.

Gestión de los hosts de los escenarios

Se pueden insertar, suprimir y renombrar los hosts de un escenario.

Siga estos pasos:

1. En el panel izquierdo, haga clic en **Escenarios y servicios de control** y, a continuación, haga clic en un servicio de control gestionado.

   Todos los grupos de escenarios del servicio de control se muestran en el panel central.

2. Del panel izquierdo, haga clic en un grupo de escenarios y, a continuación, haga clic en un escenario.

   Se muestra la página <grupo de escenarios>:<escenario>.

3. Seleccione un host en el escenario.

4. Haga clic en el menú desplegable **Editar** y, a continuación, haga clic en una de las siguientes opciones:

   Insertar host

   Inserta un host secundario al host seleccionado en el escenario.

   Eliminar host

   Suprime el host seleccionado del escenario.

   Renombrar host

   Renombra el host seleccionado en el escenario.

   Guardar

   Guarda todas las modificaciones realizadas en las propiedades del escenario.

   Actualizar

   Actualiza todas las modificaciones.

   Las propiedades del escenario se modifican.

Operaciones en escenarios

Se pueden ejecutar diversas operaciones en los escenarios.

Siga estos pasos:

1. En el panel izquierdo, haga clic en **Escenarios y servicios de control** y, a continuación, haga clic en un servicio de control gestionado.

   Todos los grupos de escenarios del servicio de control se muestran en el panel central.

2. Del panel izquierdo, haga clic en un grupo de escenarios y, a continuación, haga clic en un escenario.

   Se muestra la página <grupo de escenarios>:<escenario>.

3. Haga clic en el menú desplegable **Acciones** y, a continuación, haga clic en una de las siguientes opciones:

   Ejecutar

   Después de crear un escenario, debe ejecutarlo para iniciar el proceso de replicación. Normalmente, antes de que los cambios de los datos del servidor master se puedan a replicar en el réplica, se deben sincronizar el master y el réplica. Por lo tanto, el primer paso para iniciar una replicación es sincronizar los servidores master y réplica. Después de sincronizar los servidores, se inicia automáticamente una replicación en línea, que actualiza ininterrumpidamente el servidor réplica con todos los cambios que se producen en el master.

   Ejecutar (Modo de evaluación)

   El modo de evaluación permite valorar el uso de la banda ancha exacto y evaluar de manera comparativa la relación de compresión que se necesita para la replicación, sin reproducir datos realmente. Al ejecutar este comando, no se produce ninguna replicación pero las estadísticas se reúnen. Cuando se detiene el proceso de evaluación, se genera un informe.

   Detener

   Para poder configurar o cambiar las propiedades de un escenario en ejecución, este se debe detener. Se pueden detener los escenarios que se encuentran en ejecución o en el modo de evaluación.

   Sincronizar

   La sincronización es un proceso para que los datos del servidor master y del servidor réplica sean coherentes. Activa el proceso de sincronización, tanto si la replicación está en ejecución como si no.

Informe de diferencias

Un Informe de diferencias compara las diferencias entre el master y el réplica en un momento determinado. La comparación se realiza utilizando los mismos algoritmos que se utilizan en el proceso de sincronización, pero no se transfieren datos. Se genera un informe de diferencias para cada réplica y se envía al gestor al final del proceso. Este informe se puede generar en cualquier momento.

Realización de la conmutación

La conmutación (o conmutación por error) es el proceso de cambiar roles entre el servidor master y el réplica. Esto significa que se convierte al servidor master en el servidor en espera y al servidor de réplica en el servidor activo.

Recuperar servidor activo

Cuando el proceso de conmutación no se ha finalizado correctamente, se puede seleccionar manualmente el servidor que actuará como servidor activo mediante un proceso llamado Recuperar servidor activo.

Suspender comprobación de monitorización

Suspende la comprobación de monitorización que verifica que el servidor activo está operacional. Se puede suspender/reanudar manualmente la comprobación de monitorización para un escenario de HA en ejecución.

Prueba de integración de réplicas

La opción de recuperación asegurada permite realizar una prueba totalmente transparente de la posibilidad de recuperación de los datos del servidor réplica. El servidor réplica que se prueba es el que toma el control del servidor de producción si este estuviera fuera de servicio. La opción de recuperación asegurada es una verdadera prueba del servidor real, las aplicaciones y las acciones que se necesitan en caso de que el servidor de réplica tenga que conmutarse, convertirse en el servidor activo y llevar a cabo sus funciones.

Iniciar/detener máquina virtual

Utilice esta operación para iniciar o detener una máquina virtual de su último estado del sistema o de un marcador. Se puede iniciar o detener una máquina virtual después de crear un escenario y sincronizar el máster y la réplica. Utilice esta función cuando el escenario no esté ejecutándose. Esta función está disponible para la recuperación de desastres de todo el sistema y escenarios de alta disponibilidad. Iniciar/detener es un elemento del menú de alternancia.

Suspender la replicación

Suspende las actualizaciones de la replicación en el host de réplica con el fin de efectuar el mantenimiento del sistema o algún otro tipo de proceso que no modifique los datos replicados existentes. Los cambios continúan registrándose con fines de actualización en el réplica suspendido, pero no se transfieren realmente hasta que se reanuda la replicación. No es posible suspender la replicación durante la sincronización.

Suprimir todos los recursos de la máquina virtual

Cuando se ejecuta un escenario Todo el sistema, se crean algunos recursos temporales como archivos de disco, instantáneas y otros archivos. Esta operación permite suprimir estos recursos y está disponible cuando el escenario no está en ejecución.

Restauración de datos

Recupera los datos perdidos o dañados del servidor master desde cualquier réplica a través de la activación de un proceso de sincronización en sentido inverso.

Configurar marcador de rebobinado

Un marcador es un punto de control que se configura manualmente para marcar un estado al cual se puede volver. Esta configuración manual se llama configuración de los marcadores de rebobinado. Se recomienda establecer un marcador justo antes de cualquier actividad que pueda causar inestabilidad en los datos. Los marcadores se establecen en tiempo real, no para eventos pasados.

La operación seleccionada se realiza.

Reconstrucción completa y replicación inversa

Arcserve Unified Data Protection permite procesar la reconstrucción completa y la replicación inversa para los escenarios completos del sistema.

Siga estos pasos:

1. Prepare un equipo de reconstrucción completa iniciando el equipo desde el CD de reconstrucción completa de
2. Seleccione el escenario de todo el sistema y haga clic en **Restaurar** en el menú desplegable **Acciones**.

   Aparecerá el **Asistente de restauración de datos**.
3. Siga las instrucciones en las pantallas del asistente para crear y ejecutar el escenario de recuperación.

   Nota: En la página **Asignación de volumen**, si los volúmenes se asignan automáticamente para el origen y el destino, la asignación de volumen personalizada se desactiva. Para activar la asignación de volumen personalizada, haga clic en **Borrar** para eliminar la asignación anterior. Haga clic con el botón secundario del ratón en el volumen seleccionado y seleccione **Personalizar asignación de volumen** para abrir el cuadro de diálogo **Cambiar el tamaño del volumen** y cambiar el tamaño como sea necesario.

Para ejecutar la replicación inversa, siga estos pasos:

1. Prepare un equipo de reconstrucción completa iniciando el equipo desde el CD de reconstrucción completa de
2. Seleccione el escenario de todo el sistema que ha realizado la conmutación o la conmutación por error y haga clic en **Ejecutar** en el menú desplegable **Acciones**.

   Aparecerá el **Asistente de restauración de datos**.
3. Siga las instrucciones en las pantallas del asistente para crear y ejecutar el escenario de recuperación.

   Los datos se restauran en el equipo de reconstrucción completa. Si ha seleccionado la conmutación automática, se iniciará el proceso de conmutación y el equipo de reconstrucción completa estará listo. Si se ha seleccionado la conmutación manual, deberá iniciar manualmente el proceso de conmutación.

Control de los escenarios

Arcserve Unified Data Protection permite controlar escenarios de alta disponibilidad o de recuperación de desastres proporcionando distintas estadísticas e informes.

Siga estos pasos:

1. En el panel central, seleccione un escenario.

   El estado del escenario en ejecución se muestra con detalles como los datos enviados, los archivos enviados, los datos recibidos, los archivos recibidos, etc.

2. Haga clic en la ficha **Estadísticas** para ver más detalles. La ficha tiene las dos categorías siguientes:

   Estadísticas en ejecución

   Se muestran los datos de estadística detallados cuando el escenario se está ejecutando.

   Registro del historial

   Muestra informes para la sincronización, informes de diferencias e informes para la prueba de recuperación asegurada.

3. Haga clic en la ficha **Eventos** para ver todos los eventos de un escenario seleccionado. Para copiar o suprimir los eventos, seleccione los eventos, haga clic con el botón secundario del ratón y, a continuación, seleccione **Mostrar eventos** para abrir el cuadro de diálogo de que muestra eventos para copiar o suprimir los eventos. Utilice las teclas Maýus + Ctrl para seleccionar varios eventos.

   Nota: Los eventos se actualizan automáticamente. Los cinco eventos importantes recientes se muestran en el panel cuando se selecciona un escenario.

4. Seleccione el grupo de escenarios en el panel izquierdo. Todos los escenarios del grupo se muestran en el panel central. Se puede comprobar RPO/RTO, el uso del spool del master y el progreso de la sincronización en esta lista.

5. Los detalles en el panel derecho muestra la información del escenario como el nombre del escenario, el estado del escenario y el progreso de la sincronización.

   Nota: En el panel derecho, el uso de spool (% de spool) indica el uso de spool del master en el escenario.

Instalación remota

Arcserve Unified Data Protection permite implementar el motor de desde un servicio de control gestionado hasta los hosts remotos. Se puede gestionar también la instalación y verificación en la lista de host.

Siga estos pasos:

1. En el panel izquierdo, haga clic en **Instalación remota**.

   La página **Instalación remota** se muestra en el panel central.

2. En la lista desplegable **Servicio de control**, seleccione un servicio de control que se desea utilizar para implementar el motor.

   Los hosts existentes donde el motor se ha instalado o verificado anteriormente se muestran en el panel central.

3. En el menú desplegable **Acción**, haga clic en **Agregar hosts**.

   Se abre el cuadro de diálogo **Host para instalar el motor**.

4. Introduzca el nombre de host o la dirección IP del host y haga clic en **Agregar**.

   El host se agrega a la lista.

5. Haga clic en **Aceptar**.

   Se abrirá el cuadro de diálogo **Agregar hosts**.

6. Seleccione una de las opciones siguientes:

   Editar hosts

   Abre el cuadro de diálogo **Host para instalar el motor** para permitirle agregar hosts o gestionar los hosts existentes.

   Cambiar configuración de la instalación

   Abre el cuadro de diálogo **Edición de la configuración de la instalación.** Se pueden especificar los siguientes detalles:

   Cuenta de la instalación

   Cuenta de servicio

   Puerto

   Utilice los valores de configuración anteriores al reinstalar o actualizar

   Actualiza o reinstala un motor de RHA existente.

7. Haga clic en **Aceptar**.

8. El host se muestra en la página **Instalación remota**.

   La columna **Estado** muestra el estado de la instalación.

Nota: Mueva el ratón en el estado para obtener los detalles si se produce un error en la instalación.

Acciones de la instalación remota

Se pueden realizar diversas operaciones en los hosts agregados.

Siga estos pasos:

1. En el panel central, seleccione un host.
2. Haga clic en la lista desplegable **Acciones** y, a continuación, seleccione uno de los siguientes elementos:

Agregar host

Se abre el cuadro de diálogo **Host para instalar el motor**. Consulte Instalación remota para obtener más detalles.

Instalar/actualizar

Instala o actualiza el motor de alta disponibilidad en el host seleccionado.

Desinstalar

Desinstala el motor de alta disponibilidad del host seleccionado.

Editar configuración

Abre el cuadro de diálogo **Edición de la configuración de la instalación**.

Comprobar el estado del host

Verifica la existencia del host.

Eliminar host

Elimina el host de la lista.

Visualización de registros

Abre el cuadro de diálogo **Registros de instalación remota** y muestra los registros de todos los hosts remotos. Haga clic para actualizar para poder ver los últimos registros.

La operación se completa correctamente.

Informes de alta disponibilidad

Arcserve Unified Data Protection proporciona distintos informes para controlar el estado de la alta disponibilidad. Se pueden aplicar filtros para generar diversos tipos de informes según sea necesario.

Siga estos pasos:

1. Haga clic en la ficha **Escenarios y servicios de control**.
2. En el panel izquierdo, haga clic en **Informes**.
3. La página **Informes** se muestra en el panel central.
4. En el panel central, seleccione un servicio de control en la lista desplegable **Servicio de control**.
5. Introduzca detalles y aplique filtros según sea necesario.

   Se generará el informe de HA.

Capítulo 8: Uso de la utilidad VSphereConfig

Esta sección incluye los siguientes temas:

Activación o desactivación de la etiqueta VSPhereBackupNFC mediante el símbolo del sistema

Importante: Active la etiqueta VSphereBackupNFC en un adaptador de kernel específico para la copia de seguridad (en lugar de una red de copia de seguridad específica) cuando una máquina virtual de origen aloje el hipervisor de ESXi y la copia de seguridad utilice VDDK7 o versiones posteriores.

Arcserve UDP permite activar o desactivar la etiqueta *VSphereBackupNFC* mediante el símbolo del sistema. La herramienta de la línea de comandos (*AFVSphereConfigTool.exe*) permite activar o desactivar la etiqueta VSphereBackupNFC en un adaptador de kernel específico.

Esta sección proporciona información sobre cómo activar o desactivar la etiqueta *VSPhereBackupNFC* mediante el símbolo del sistema.

Siga estos pasos:

1. Abra el símbolo del sistema y vaya a <Engine>\BIN>.

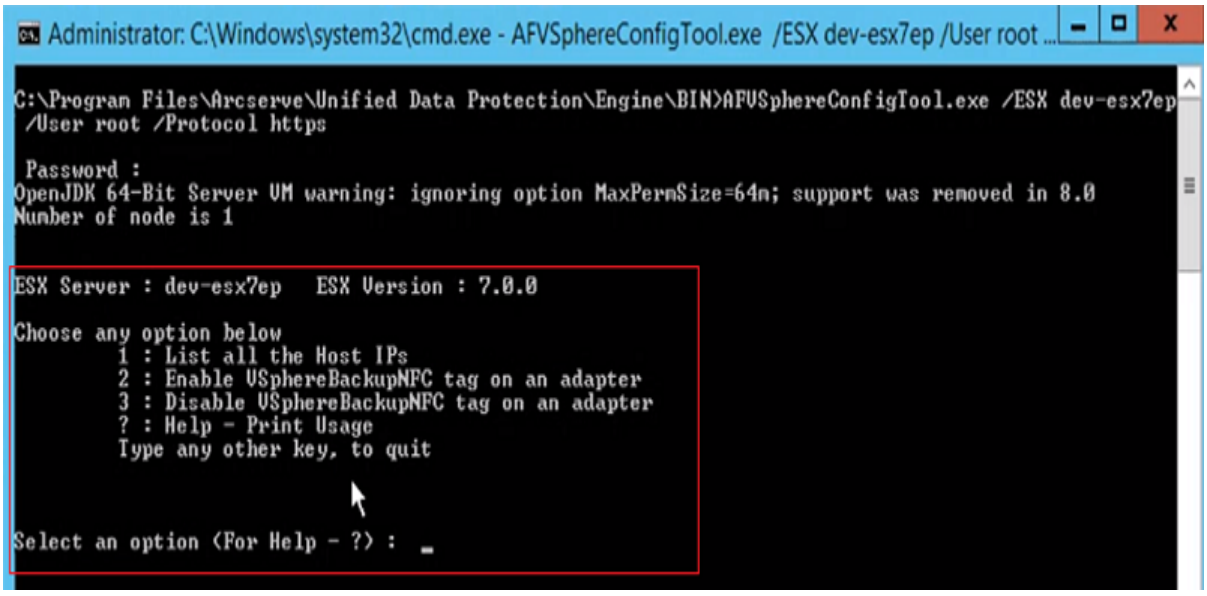
   Ejemplo: C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN>

2. Conéctese al servidor ESX mediante la herramienta de la línea de comandos (*AFVSphereConfigTool.exe*) y, a continuación, especifique una contraseña cuando se le solicite.

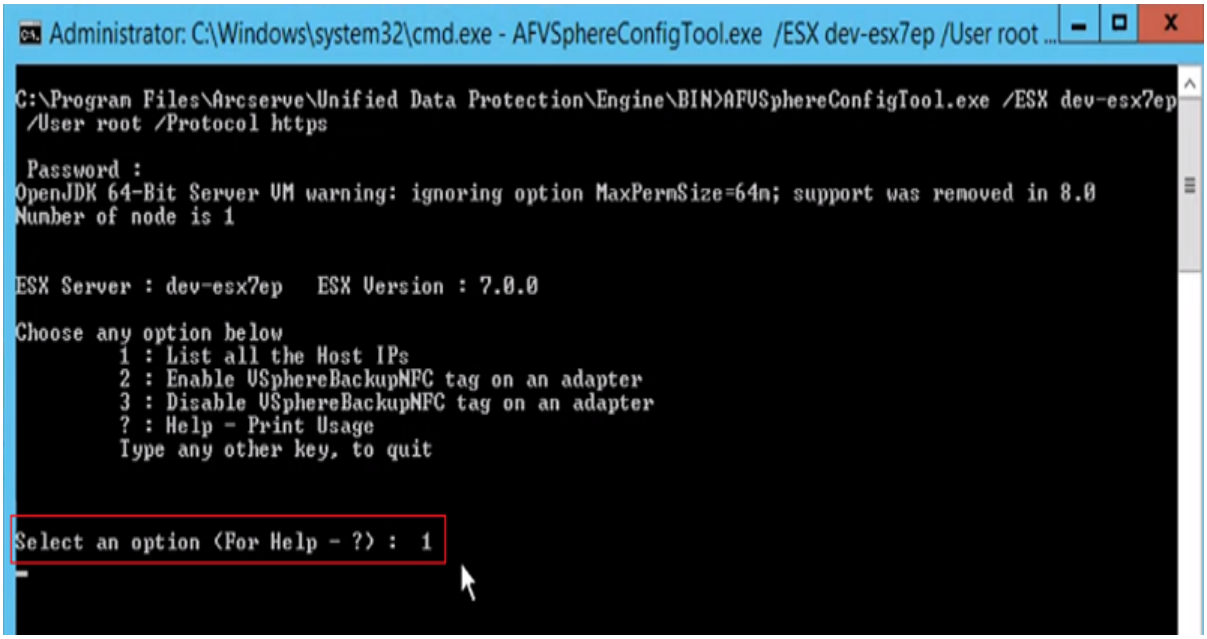
   AFVSphereConfigTool.exe /ESX dev-esx7ep /user root /protocol https

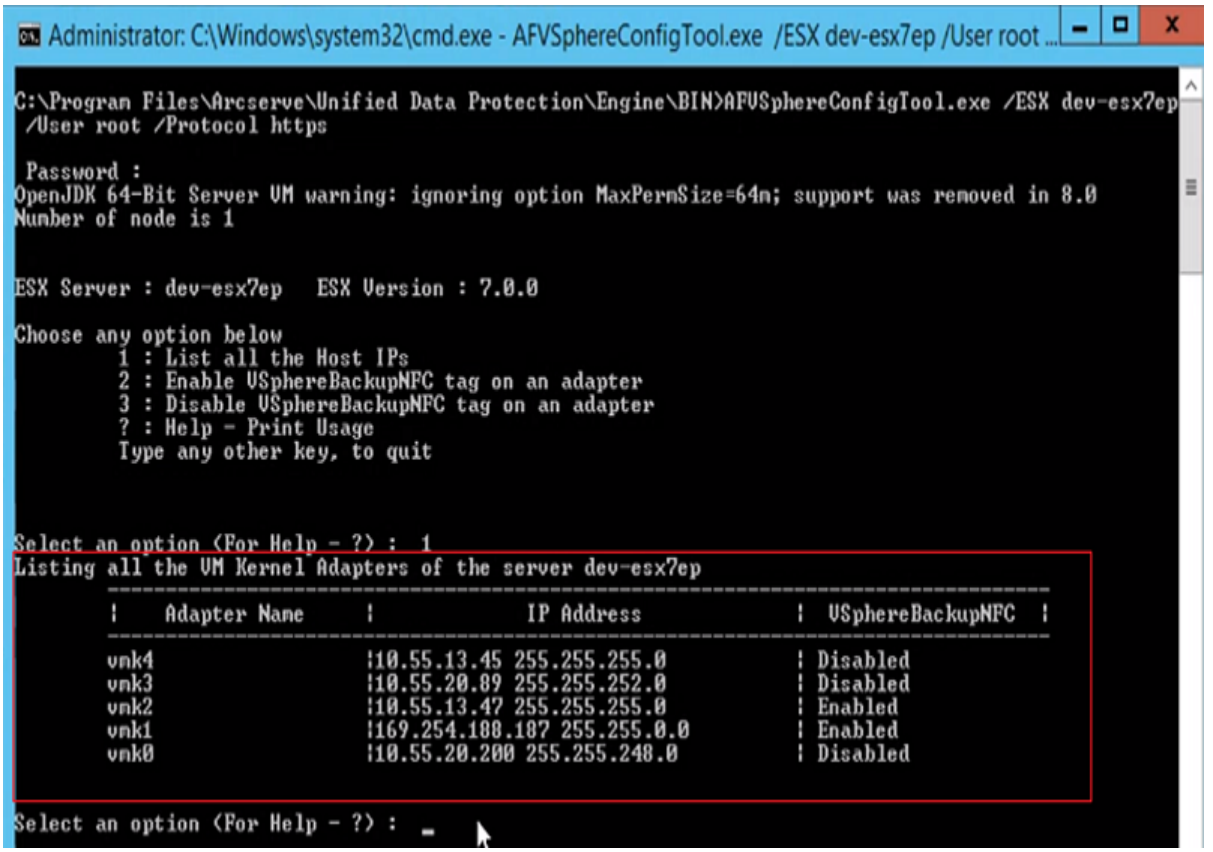
   El servidor ESX seleccionado (dev-esx7ep) ahora está conectado.



3. Después de conectarse correctamente al servidor ESX, cuando se le solicite que seleccione una opción, haga lo siguiente:
   - Para enumerar todos los adaptadores de kernel de la máquina virtual del servidor ESX, especifique el número de opción. Por ejemplo, escriba 1 para la opción.

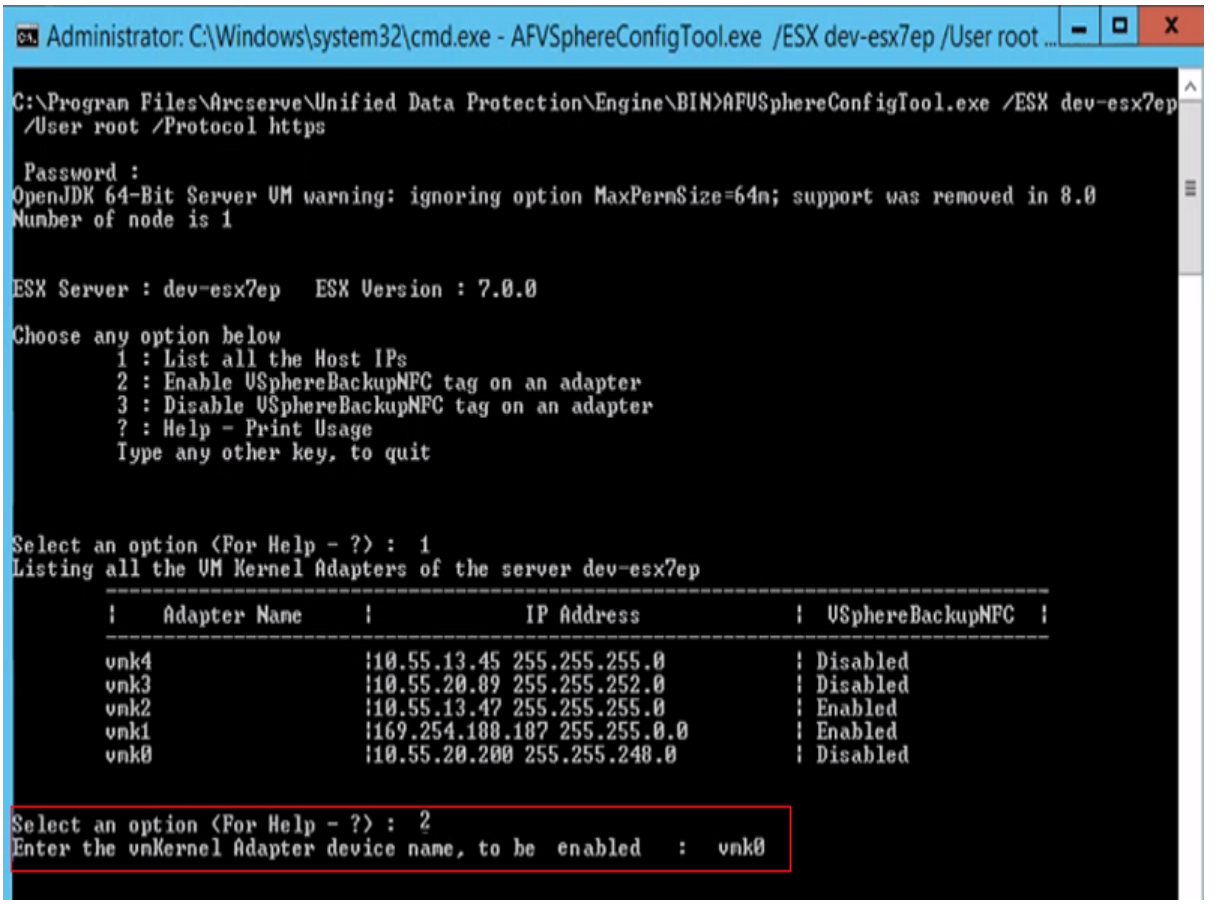


Se muestra una lista de todos los adaptadores de kernel de la máquina virtual.

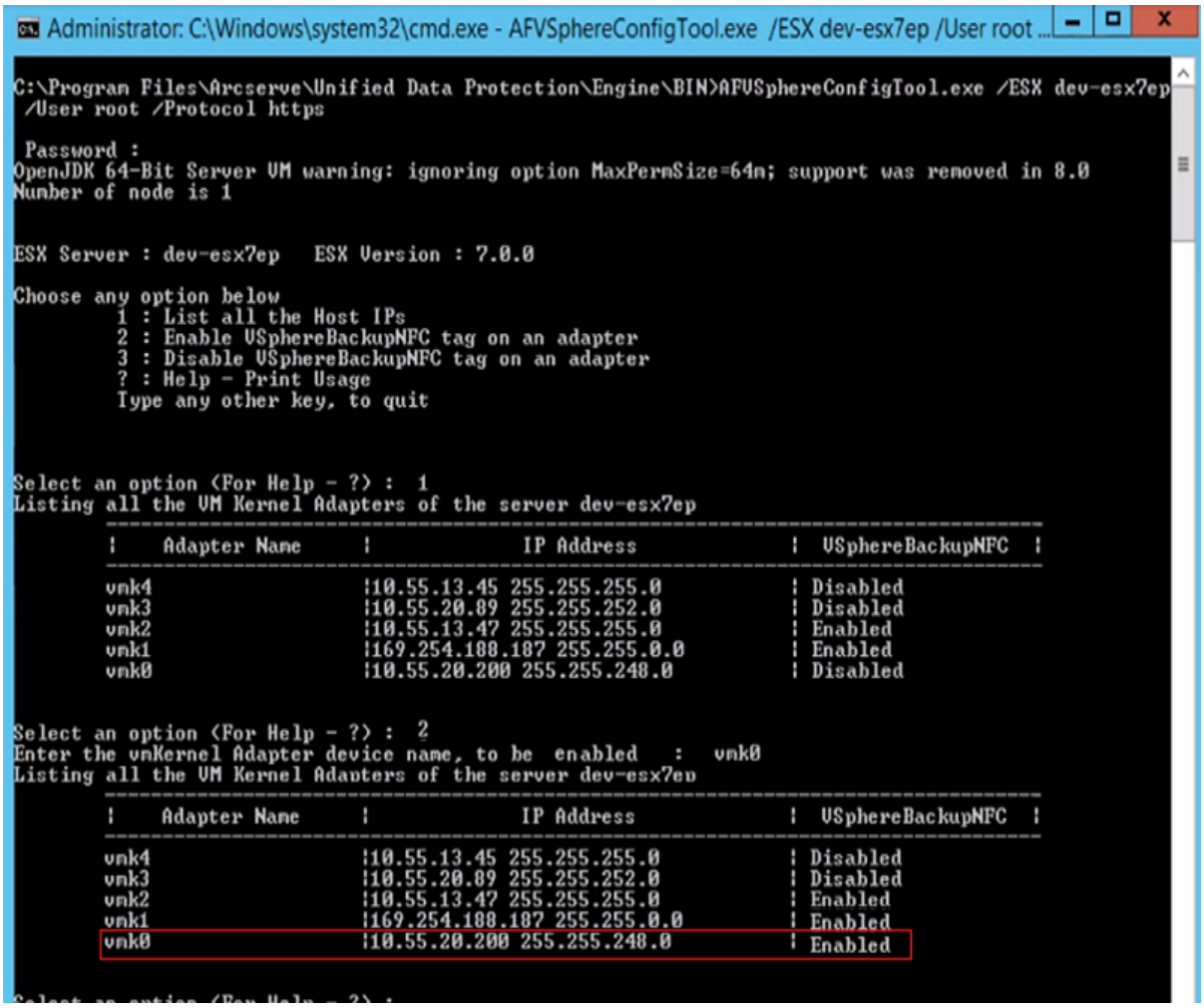


- Para activar la etiqueta VSphereBackupNFC en un adaptador, escriba el número de opción. Por ejemplo, escriba 2 para la opción.

  Cuando se le solicite que introduzca el nombre del dispositivo del adaptador de kernel de la máquina virtual, especifique el nombre del dispositivo.

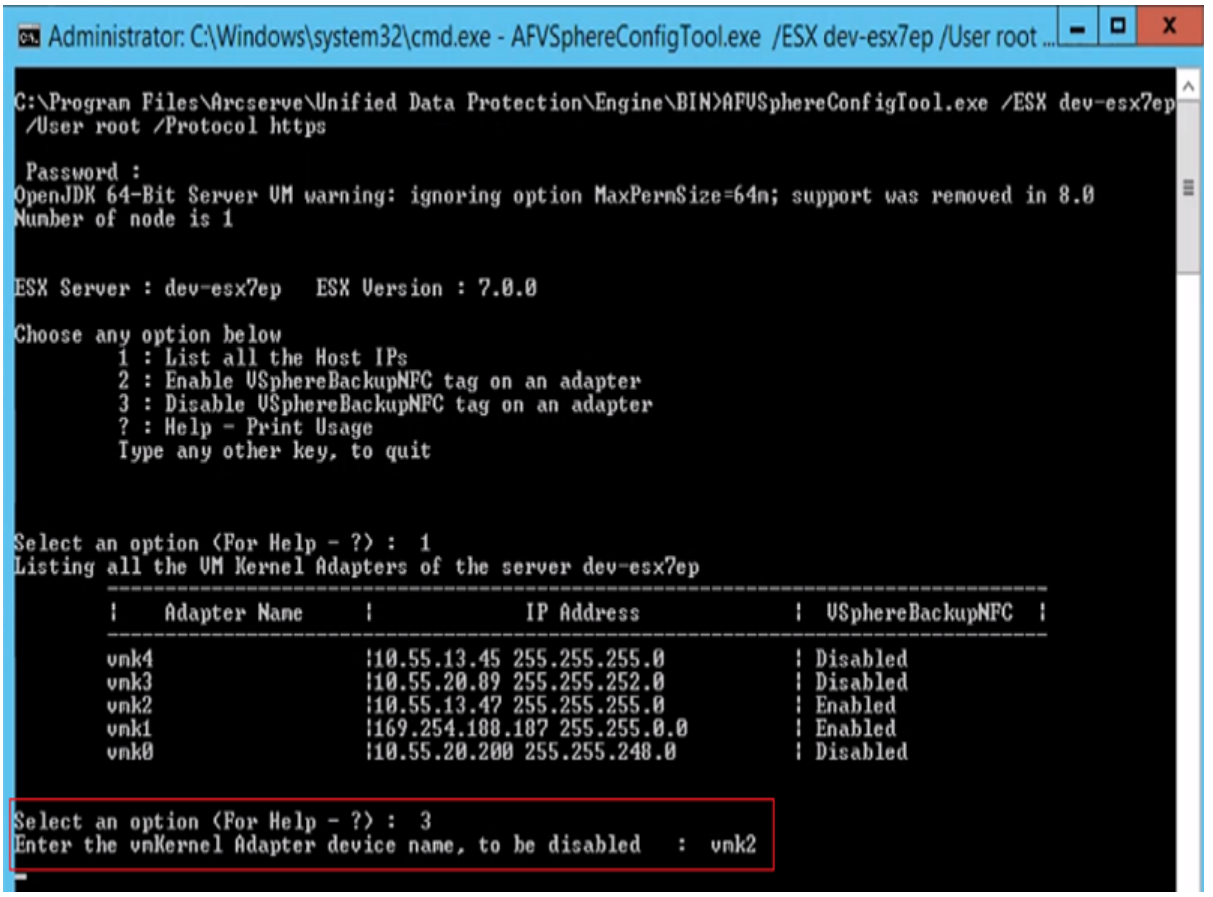


La etiqueta VSphereBackupNFC se activa en el adaptador seleccionado.

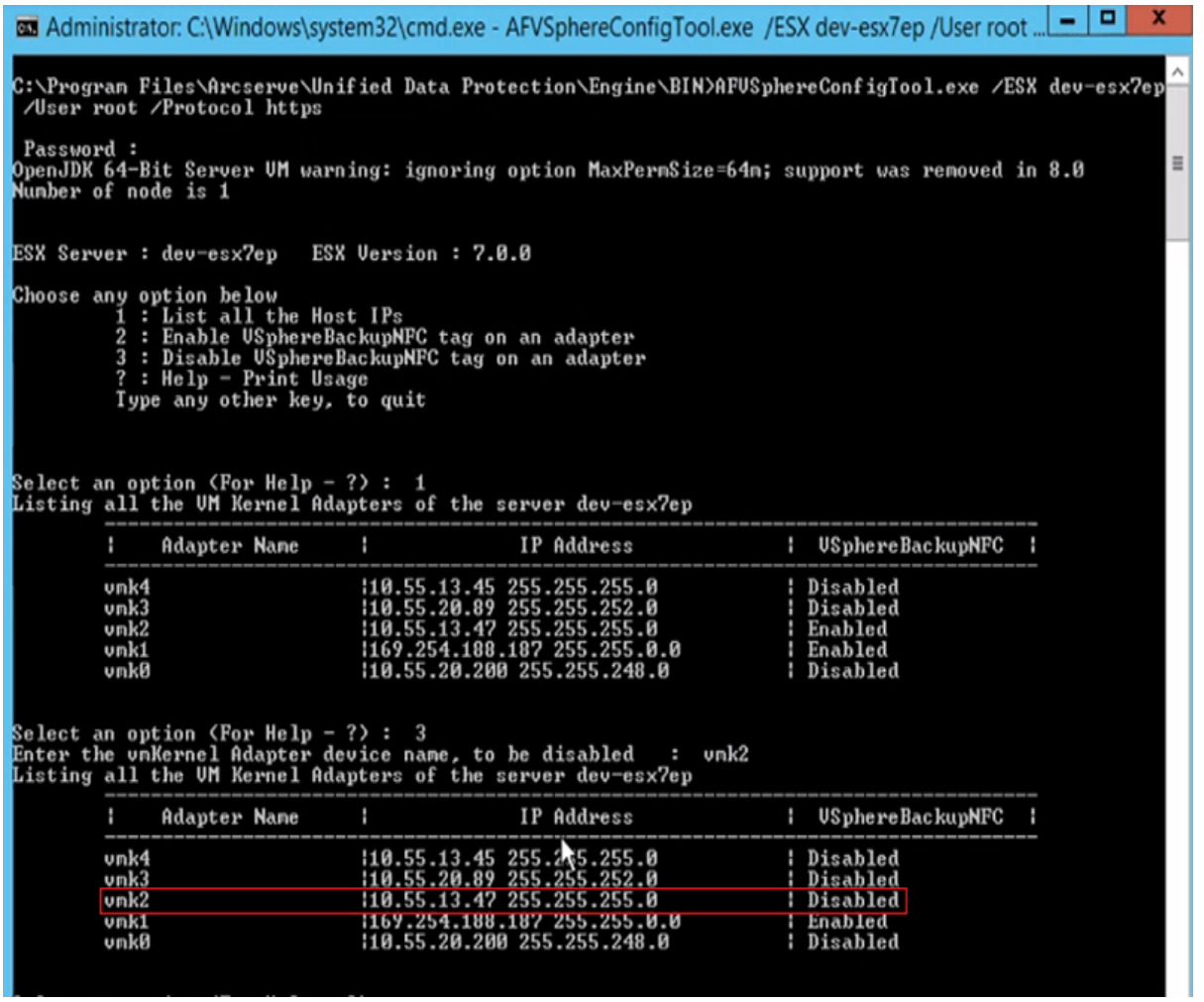


- Para desactivar la etiqueta VSphereBackupNFC en un adaptador, especifique el número de opción. Por ejemplo, escriba 3 para la opción.

  Cuando se le solicite que introduzca el nombre del dispositivo del adaptador de kernel de la máquina virtual, especifique el nombre del dispositivo.



La etiqueta VSphereBackupNFC se desactiva en el adaptador seleccionado.



4. Especifique cualquier clave (excepto 1, 2, 3 y ?) para cerrar el símbolo del sistema.

Capítulo 9: Uso de la utilidad de diagnóstico

La utilidad de diagnóstico permite recopilar registros de los equipos. Si se pone en contacto con el equipo de Soporte de Arcserve debido a cualquier problema, el equipo de soporte utilizará los registros para investigar y corregir el problema.

Esta sección incluye los siguientes temas:

Recopilación de la información de diagnóstico

La información de diagnóstico es una recopilación de registros, eventos, registro e información de la aplicación del producto y el sistema que necesita el equipo de Soporte de Arcserve para investigar cualquier error. Arcserve UDP permite recopilar toda esta información en una ubicación, por lo general una ruta de acceso de recurso compartido de red. Cuando se ponga en contacto con Soporte de Arcserve, tendrá esta información a su disposición. Se pueden recopilar los datos de diagnóstico para los equipos de Windows, Linux, VMware e Hyper-V.

Nota: En el caso de los servidores de copia de seguridad de Linux, la opción **Recopilar datos de diagnóstico** solo se encuentra disponible en los **nodos de <nombre_sitio>:** Vista **Grupos de servidores de copia de seguridad de Linux**.

Siga estos pasos:

1. En la consola, haga clic en **Recursos**.
2. Siga uno de estos pasos en función del tipo de nodo:

   Para los servidores de copia de seguridad de Linux

   - En el panel de navegación izquierdo, vaya a **Nodos** y haga clic en **Grupos de servidores de copia de seguridad de Linux**.
   - En el panel central, seleccione todos los nodos de Linux necesarios.

   Para todos los demás servidores y nodos

   - En el panel de navegación izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.
   - En el panel central, seleccione todos los nodos necesarios.
3. Haga clic en **Acciones**, **Recopilar datos de diagnóstico**.

   Se abrirá el cuadro de diálogo **Recopilar información de diagnóstico**.
4. (Opcional) Seleccione la casilla de verificación.
5. Proporcione la ruta de recurso compartido de red para almacenar los datos.

   Notas:

   - Al recopilar la información de diagnóstico de un sitio remoto, deberá especificar el destino como el servidor de puerta de enlace o cualquier otro equipo que pueda acceder al Agente o al servidor de puntos de recuperación en dicho sitio.

- Si desea especificar la ruta local como el destino, convierta dicha ruta en la de UNC y especifique esta última. Por ejemplo, **C:\test** puede especificarse como **\\<Nombredelequipolocal>\C$\test**.
- En el caso de las copias de seguridad sin agente basadas en host (máquinas virtuales), la opción Recopilar datos de diagnóstico reúne datos del servidor proxy de Arcserve UDP.
- La opción Recopilar datos de diagnóstico reúne datos de los equipos que tengan instalado el Agente de Arcserve UDP.

6. Haga clic en **Enviar**.

   Se envía una tarea para recopilar los datos.

   Si la tarea finaliza correctamente, podrá ver los datos en la carpeta compartida. Se agrega la marca de hora actual como sufijo al nombre del archivo ZIP.

Recopilación de información de diagnóstico de un agente independiente

La información de diagnóstico es una recopilación de registros, eventos, claves de registro e información de la aplicación del producto y el sistema que necesita el equipo de Soporte de Arcserve para investigar cualquier error. El Agente de Arcserve UDP permite recopilar toda esta información en una ubicación, por lo general una ruta de recurso compartido de red. Cuando se ponga en contacto con Soporte de Arcserve, tendrá esta información a su disposición.

Siga estos pasos:

1. Usando el símbolo del sistema, vaya a la siguiente ruta:

   ```
   %ProgramFiles% \Arcserve\Unified Data Protection\Engine\BIN\DiagnosticUtility
   ```

2. Ejecute el comando siguiente para descubrir cómo ejecutar el archivo por lotes:

   ```
   arcserveAgentSupport.bat -help
   usage: arcserveAgentSupport.bat [OPTIONS]
   -help print help
   -pass <arg> usrPass (Si la ruta de exportación es un recurso compartido remoto, se accede con la contraseña de usuario)
   -path <arg> export path (Puede ser un recurso compartido remoto)
   -user <arg> usrName (Si la ruta de exportación es un recurso compartido remoto, se accede con el nombre de usuario)
   -xmlConfig <arg> xmlConfigurationFile (Opcional)
   ```

3. Utilice el siguiente comando para recopilar la información de diagnóstico:

   ```
   arcserveAgentSupport.bat -path <remote share path> -user <username> -pass <password>
   ```

   Ejemplo: arcserveAgentSupport.bat -path \\remote_share\data -user abc -pass xyz

   donde \\remote_share\data es la ruta, abc es el nombre de usuario y xyz, la contraseña

   Se puede encontrar el archivo .zip con la información de diagnóstico en el recurso compartido remoto.

Carga de información de diagnóstico al sitio web de Arcserve usando el FTP

Se pueden cargar cualquier tipo de registros o archivos al FTP del Soporte de Arcserve utilizando un protocolo de transferencia de archivos (FTP). Sin embargo, los usuarios (los que solicitan un ticket) pueden activar el vínculo del FTP durante el proceso inicial de creación del ticket o al cargar el ticket en línea. Una vez activado, FTP genera el vínculo del FTP con las credenciales de inicio de sesión. Esta información se proporciona al usuario en un correo electrónico automatizado. Se puede utilizar el nombre de usuario y la contraseña que se envían en un correo electrónico automatizado para cargar y descargar archivos del FTP.

Cuando se inicia sesión en el FTP utilizando ftp://supportftp.arcserve.com, aparecerá la carpeta principal. Si crea un ticket en el portal de Soporte de Arcserve, se crea una subcarpeta con el número de ticket en la carpeta principal. Por ejemplo, si crea un ticket con el número Ticket-00XXXX30, aparecerá una subcarpeta llamada Ticket-00XXXX30 en la carpeta principal.

ftp://supportftp.arcserve.com/Ticket-00XXXX30/

Nombre de usuario y Contraseña: Utilice el nombre de usuario y la contraseña generados automáticamente que se envían en un correo electrónico automatizado.

Carpeta: Ticket-00XXXX30

Nota: Para los usuarios japoneses, la contraseña es la dirección de correo electrónico del solicitante sin el nombre de dominio. Por ejemplo, si la dirección de correo electrónico registrada es abc@yahoo.jp, la contraseña es abc.

Cuando se resuelve el ticket, el servidor FTP recibe una notificación. A continuación, se comprime la carpeta y se suprime la carpeta original. La carpeta comprimida está disponible durante los siguientes tres meses y más tarde se suprime de forma permanente.

Importante: No comparta el nombre de usuario con otras personas.

Siga estos pasos para cargar cualquier tipo de archivos al sitio web de Arcserve mediante el FTP:

1. El solicitante del ticket (usuario) o un agente de Soporte de Arcserve inician sesión en el portal de Soporte de Arcserve y crean un ticket de soporte.

   El agente de Soporte de Arcserve o el solicitante del ticket seleccionan la casilla de verificación del ticket de soporte y lo cargan.

Se generará automáticamente un vínculo de FTP para la carpeta Inicio del FTP. El permiso se establece exclusivamente para el solicitante que abrió el ticket.

Por ejemplo, esta sería la carpeta del FTP:

ftp://supportftp.arcserve.com/<Número_ticket>

2. Una vez que se crea el vínculo del FTP, Soporte de Arcserve envía automáticamente al solicitante del ticket (usuario) un correo electrónico con dicho vínculo junto con las credenciales de inicio de sesión.
3. El usuario inicia sesión en el vínculo del FTP y carga los archivos.

   De esta forma, se habrá completado correctamente el proceso de carga de archivos al servidor FTP de Arcserve.

Descompresión de registros del Agente

Los archivos de registro generados por la utilidad de diagnóstico están en formato zip. Para ver los archivos de registro, descomprima los archivos.

Siga estos pasos:

1. Copie el archivo .arcZIP al equipo donde se haya instalado el Agente de UDP.

   El archivo .arcZIP se crea mediante la utilidad de diagnóstico.

2. Usando el símbolo del sistema, vaya a la siguiente ruta:

   ```
   %ProgramFiles% \Arcserve\Unified Data Protection\Engine\BIN\DiagnosticUtility
   ```

3. Ejecute el comando siguiente para descubrir cómo ejecutar el archivo por lotes:

   ```
   arcserveAgentSupportInternal.bat -help
   BaseOperation loadDefaultValue
   Información: Load Agent install path C:\Program Files\Arcserve\Unified Data Protection\Engine\
   uso: arcserveAgentSupportInternal.bat [OPCIONES] rawfile
   -help         Mostrar ayuda
   -keepFile     Conservar archivo temporal
   -path <arg>   Ruta en la que debe descomprimirse el contenido
   ```

   Se muestra la sección de ayuda.

4. Utilice el siguiente comando para descomprimir el archivo:

   ```
   arcserveAgentSupportInternal.bat -path <debe_ser_en_la_misma_máquina_en_la_que_desea_descomprimir> <nombre_del_archivo_zip>
   ```

   Los registros del Agent se descomprimen.

Descompresión de los registros de la consola

Los archivos de registro generados por la utilidad de diagnóstico están en formato zip. Para ver los archivos de registro, descomprima los archivos.

Siga estos pasos:

1. Copie el archivo .arcZIP al equipo que tenga instalado la consola de UDP.

   El archivo .arcZIP se crea mediante la utilidad de diagnóstico.

2. Usando el símbolo del sistema, vaya a la siguiente ruta:

   ```
   %ProgramFiles% \Arcserve\Unified Data Protection\Management\BIN\DiagnosticUtility
   ```

3. Ejecute el comando siguiente para descubrir cómo ejecutar el archivo por lotes:

   ```
   arcserveConsoleSupportInternal.bat -help
   BaseOperation loadDefaultValue
   Información: Load Agent install path C:\Archivos de programa\Arcserve\Unified Data Protection\Management \
   uso: arcserveConsoleSupportInternal.bat [OPCIONES] raw-file
   -help              Mostrar ayuda
   -ignoreFailed      Ignorar error de importación de tabla
   -keepFile          Conservar archivo temporal
   -noClean           No limpiar la base de datos
   -path <arg>        Ruta en la que debe descomprimirse el contenido
   -u                 Solo descomprimir el archivo
   ```

   Se muestra la sección de ayuda.

4. Utilice el siguiente comando para descomprimir el archivo.

   ```
   arcserveConsoleSupportInternal.bat –path <debe_ser_en_la_misma_máquina_en_la_que_desea_descomprimir> <nombre_del_archivo_zip>
   ```

   Nota: El comando no sobrescribe la base de datos de la consola. Si desea sobrescribir la base de datos de la consola, edite el comando *arcserveConsoleSupportInternal.bat*, elimine "*-u*" del archivo y guarde el archivo.

   Los registros de la consola se han descomprimido.

Omisión del contenido de la carpeta histórica del registro utilizando el registro

Se puede utilizar el Agente de UDP para recopilar todos los registros, incluido el historial de registros, del motor. A veces, mientras se recopila el historial de registros, el Agente de UDP procesa los archivos a un ritmo lento y hace que el tamaño del archivo parezca mayor. Para evitar estas discrepancias, se puede excluir la carpeta LogHistory.

Siga estos pasos:

1. Agregue la clave al registro en la siguiente ubicación:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

2. Introduzca los siguientes detalles:

   Nombre de clave: *SkipLogHistory*

   Tipo: *DWORD(32-bit)*

   Valor: 1 (se utiliza el valor 1 para omitir la carpeta LogHistory y 0 se utiliza para recopilar LogHistory)

Recopilación de registros del equipo de la puerta de enlace utilizando la línea de comandos

Debe tener instalado el producto de la puerta de enlace de Arcserve UDP para recopilar los registros desde la línea de comandos.

Siga estos pasos para recopilar los registros desde la línea de comandos:

1. Abra el símbolo del sistema y vaya a *<Directorio de instalación de la puerta de enlace>\BIN\Diagnostic Utility*.

   Ejemplo: C:\Archivos de programa\Arcserve\Unified Data Protection\Gateway\BIN\Diagnostic Utility\

2. Para comprimir los registros, ejecute el siguiente comando:

   arcserveGatewaySupport.bat -Path "<Ruta de destino>"

3. Para descomprimir los registros, ejecute el siguiente comando:

   arcserveGatewayInternalSupport.bat -Path "<Ruta de destino>" "<ruta de origen>"

Recopilación de registros del servidor de puntos de recuperación utilizando la línea de comandos

El producto de Arcserve UPD debe estar instalado con el componente del servidor de puntos de recuperación para recopilar los registros del servidor de puntos de recuperación desde la línea de comandos.

Siga estos pasos para recopilar los registros desde la línea de comandos:

1. Abra el símbolo del sistema y vaya a *<Directorio de instalación del agente>\BIN\Diagnostic Utility*\.

   Ejemplo: C:\Archivos de programa\Arcserve\Unified Data ProtectionEngine\BIN\Diagnostic Utility\

2. Para comprimir los registros, ejecute el siguiente comando:

   arcserveAgentSupport.bat -path <remote share path> -user <username> -pass <password>

3. Para descomprimir los registros, ejecute el siguiente comando:

   arcserveAgentSupportInternal.bat –path <destino> <origen (archivo sin formato)>

Notas:

- Los registros del servidor de puntos de recuperación dispone de los registros de las tareas que se ejecutan en el servidor de puntos de recuperación.
- Los registros del servidor de puntos de recuperación se deben recopilar desde la línea de comandos y no desde la interfaz de usuario de la Consola.
- Algunos registros de tareas relacionadas con el servidor de puntos de recuperación no se pueden recopilar desde la interfaz de usuario de la Consola cuando se recopilan registros de la máquina virtual desde la Consola.

Ejemplo: Cuando se configura una tarea de replicación del proveedor de servicios gestionados (MSP), configure las tareas con dos consolas donde la Consola-1 tendrá la copia de seguridad como tarea principal y la replicación como tarea secundaria. En la Consola-2, la tarea de replicación gestionada remotamente está configurada y compartida con la Consola-1.

En este escenario, en la Consola-2 no se pueden recopilar los registros de la tarea de replicación al recopilar los registros de la máquina virtual desde la Consola. Se deben recopilar dichos registros de la replicación desde la línea de comandos del equipo del servidor de puntos de recuperación que es el destino de la tarea de replicación.

Recopilación de registros de código auxiliar de la instancia de Hyper-V con el agente instalado

Se pueden recopilar registros de código auxiliar de la instancia de Hyper-V que tiene instalado el agente. Hyper-V también puede actuar como servidor proxy para ayudar a recopilar los registros de código auxiliar de Hyper-V.

Cuando Hyper-V actúa como servidor proxy (el equipo de Hyper-V debe tener instalado el agente)

Abra el símbolo del sistema y vaya a *<Directorio de instalación del agente>\BIN\Diagnostic Utility*.

Ejemplo: *C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN\Diagnostic Utility*

- Para comprimir los registros: ejecute *arcserveAgentSupport.bat -Path "Destino"*
- Para descomprimir los registros: ejecute *ArcserveAgentInternalSupport.bat -Path "Destino" "Origen"*

Cuando Hyper-V no funciona como un servidor proxy (recopilar toda la carpeta de copia de seguridad de la máquina virtual basada en el host de UDP)

Requisito previo: El equipo debe tener Java instalado.

Siga estos pasos:

1. Importe el registro desde la siguiente ruta al equipo que tiene instalado el agente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine.

2. Copie toda la carpeta DiagnosticUtility de un equipo que ya tenga instalado el agente y péguela en la carpeta de la siguiente ruta:

   C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN

   Nota: Debe crear manualmente esta estructura de directorios.

3. Cree una carpeta vacía con el nombre "Logs" en la siguiente ruta:

   C:\Archivos de programa\Arcserve\Unified Data Protection\Engine

4. Copie la carpeta "Common" de un equipo que ya tenga instalado el agente en la ruta siguiente:

   C:\Archivos de programa\Arcserve\Unified Data Protection

- Para comprimir los registros: ejecute *arcserveAgentSupport.bat -Path "Destino"*
- Para descomprimir los registros: ejecute *ArcserveAgentInternalSupport.bat -Path "Destino" "Origen"*

Recopilación de mensajes del visor de eventos de Hyper-V

Se pueden recopilar mensajes del visor de eventos de Hyper-V con el agente instalado en una carpeta con el nombre *hyperVEventViewerFiles*.

Siga estos pasos para recopilar los mensajes del visor de eventos desde la línea de comandos:

1. Abra el símbolo del sistema y vaya a *<Directorio de instalación del agente>\BIN\Diagnostic Utility*.

   Ejemplo: C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN\Diagnostic Utility\
2. Para comprimir los mensajes del visor de eventos, ejecute *arcserveAgentSupport.bat -Path "Destino"*
3. Para descomprimir los mensajes del visor de eventos, ejecute *ArcserveAgentInternalSupport.bat -Path "Destino" "Origen"*

Recopilación de la carpeta CA_LIC y de los archivos OLF

CA_LIC y los archivos OLF se recopilan en los registros cuando se recopilan desde el equipo que ya tiene instalado el agente, con un nombre de carpeta CA_LIC.

- Para la recopilación utilizando la CLI: Abra el símbolo del sistema y vaya a *<Directorio de instalación del agente>\BIN\Diagnostic Utility*.

  Ejemplo: *C:\Archivos de programa (x86)\Arcserve\SharedComponents\CA_LIC*
- Para la recopilación utilizando la Consola: Vaya al nodo del agente, haga clic con el botón secundario del ratón y haga clic en **Recopilar información de diagnóstico**.
- Para comprimir los registros: Ejecute *arcserveAgentSupport.bat -Path "Destino"*

- Para descomprimir los registros: Ejecute *ArcserveAgentInternalSupport.bat -Path "Destino" "Origen"*

Recopilación de la lista de directorios de los directorios del almacén de datos o del destino de la copia de seguridad

Lista de directorios para las carpetas del motor y de la gestión

Motor: Este registro se recopila en la carpeta *agentLogs* (después de descomprimir arczip) con el nombre *EngineDirectoryBrowseInfo.log*.

Gestión: Este registro se recopila en la carpeta *consoleLogs* (después de descomprimir arczip) con el nombre *ManagementDirectoryBrowseInfo.log*.

Lista de directorios para los almacenes de datos:

- **Sin deduplicación:** El registro se recopila para el almacén de datos sin deduplicación con el nombre *CommonStorePathDirectoryBrowseInfo.log* (después de descomprimir arczip) en la carpeta *agentLogs*
- **Deduplicación:** Se recopilan cuatro registros en los almacenes de datos de deduplicación (después de descomprimir arczip) en la carpeta *agentLogs* con los nombres siguientes:
    1. *CommonStorePathDirectoryBrowseInfo.log*
    2. *HashRolePathDirectoryBrowseInfo.log*
    3. *IndexRolePathDirectoryBrowseInfo.log*
    4. *DataRolePathDirectoryBrowseInfo.log*

Capítulo 10: Instalación manual de Sophos Intercept X Advanced for Server en Arcserve UDP

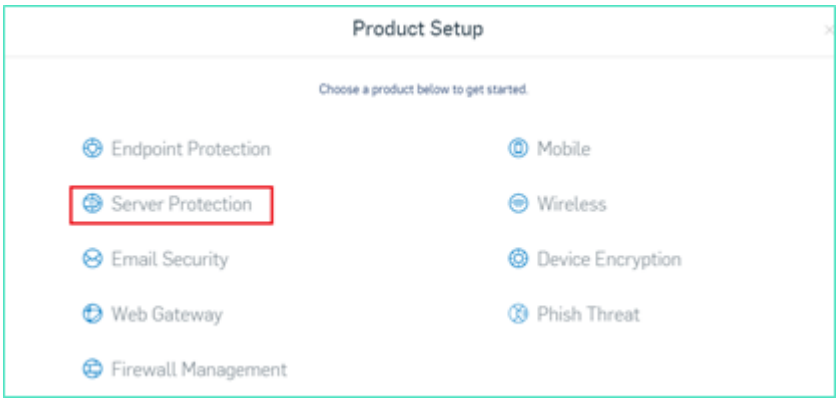
La instalación de Sophos Intercept X Advanced for Server en Arcserve UDP permite lo siguiente:

- Proteger los datos y las copias de seguridad del sistema de ransomware y otros ataques
- Protección de punto final que combina la detección de malware basada en firmas y sin firma.
- Red neuronal de aprendizaje profundo
- Tecnología contra vulnerabilidades de seguridad
- Las tecnologías contra ransomware CyptoGuard y WipeGuard, entre otras, para detener el mayor número de amenazas de puntos finales.

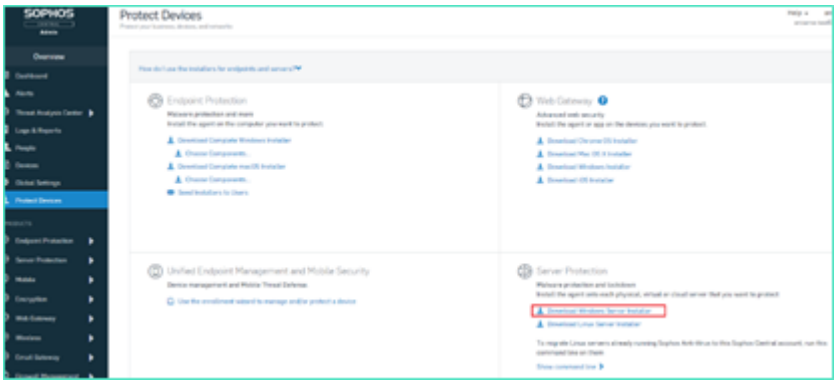
Siga estos pasos:

1. En el sitio web de Soporte de Arcserve, cree una cuenta.
2. Para solicitar una copia gratuita de Sophos Intercept X Advanced, proporcione todos los detalles relevantes en el formulario de solicitud de Sophos y envíelo a Soporte de Arcserve. Es obligatorio compartir los detalles del ID de correo electrónico y el ID de pedido. Recibirá una confirmación por correo electrónico generada automáticamente.

   Después de confirmar su ID de correo electrónico, Arcserve procesa su solicitud y crea una cuenta en Sophos Central. A continuación, le envía un correo electrónico con instrucciones sobre cómo crear una contraseña.
3. Para crear una contraseña para su nueva cuenta en Sophos Central, siga las instrucciones del correo electrónico.
4. Inicie sesión en Sophos Central.
5. Abra el cuadro de diálogo Product Setup y, a continuación, seleccione **Server Protection**.



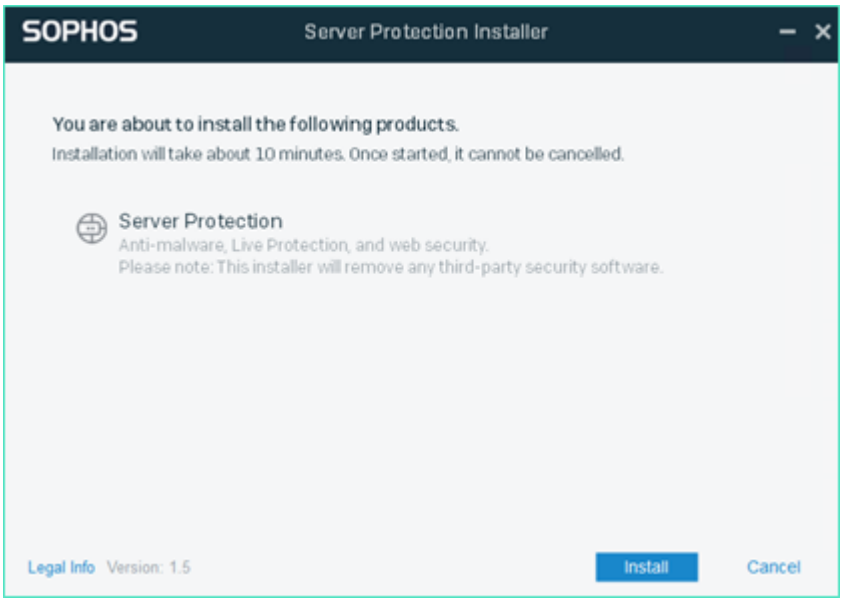
6. En la sección Server Protection, haga clic en **Download Windows Server Installer** y, a continuación, guarde el instalador **SophosSetup.exe** en una carpeta de UDP.



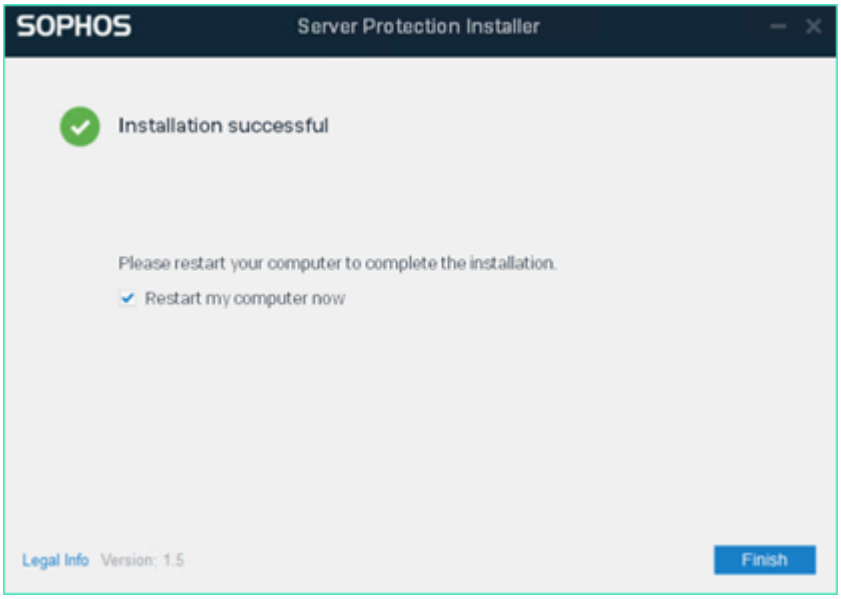
7. Para iniciar el instalador, abra la carpeta y, a continuación, haga doble clic en **SophosSetup.exe**.

   Nota: Para evitar un comportamiento inesperado durante la instalación de Sophos Intercept-X, desactive Windows Defender u otro software antivirus del servidor. Sophos eliminará algunos productos de seguridad que no sean de Sophos de los servidores de Windows. Para obtener más información, consulte Sophos CRT: Lista de software de seguridad de terceros eliminado por Sophos.

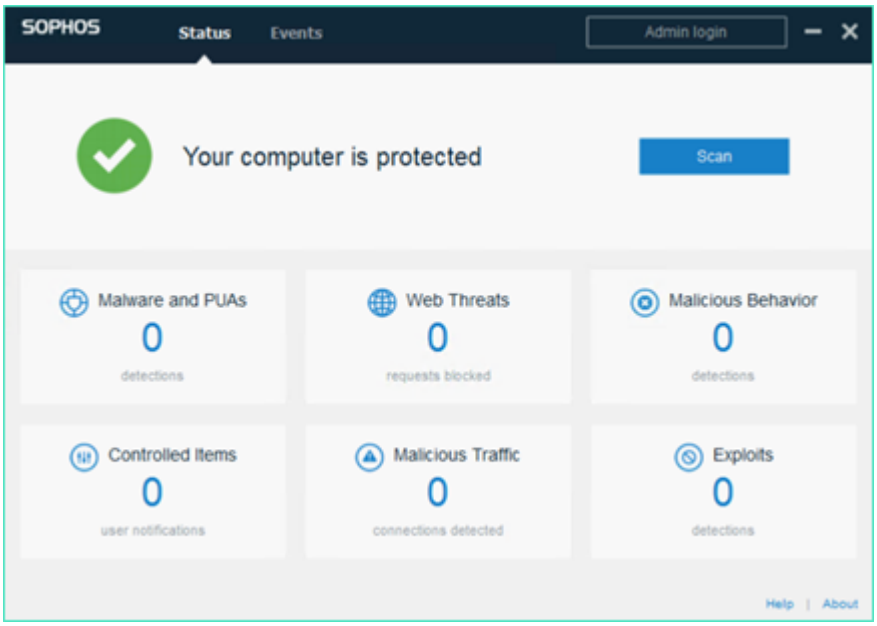
8. Haga clic en **Instalar**.



9. Para reiniciar el sistema inmediatamente, haga clic en **Finish**. Para reiniciar más tarde, desactive la opción **Restart my computer now**.



10. Para ver el estado de protección, abra la interfaz de **Sophos Intercept X**.



El estado indica que Arcserve UDP 8.0 está protegido contra ataques de ransomware, malware, amenazas web y ataques de día cero.

11. Para acceder a Sophos Central, haga clic en **Admin Login**. Le permite gestionar Sophos Intercept X Advanced Server, establecer alertas y políticas, etc.

    Notas:

    - Es obligatorio disponer de acceso a Internet en Arcserve UDP para instalar la aplicación *Sophos Intercept X Advanced* y cualquier actualización relacionada. Sophos Intercept X Advanced se basa en la nube y no hay ningún instalador sin conexión disponible.
    - Si ya ha adquirido otra instancia de UDP anteriormente y tiene una cuenta de Sophos a través de Arcserve, utilice la misma cuenta para todos los dispositivos de Arcserve UDP 8.0.
    - Si ya tiene una cuenta de Sophos a raíz de otra compra o la ha obtenido directamente de Sophos, proporcione una dirección de correo electrónico diferente para tener una cuenta independiente en Sophos Central.
    - Si se produce un error en la instalación de Sophos por cualquier motivo, siga las instrucciones en pantalla o por correo electrónico que se proporcionan junto con el mensaje de error.
    - Para recibir las actualizaciones de Sophos Intercept X Advanced for Server como, por ejemplo, las actualizaciones de definiciones de malware y las actualizaciones de versiones, debe tener un servicio de mantenimiento o suscripción válido y activo para Arcserve UDP.

Para obtener más ayuda, póngase en contacto con Soporte de Arcserve en el teléfono +1 844 765 7043 o en línea, o póngase en contacto con su oficina de soporte local de Arcserve.

Capítulo 11: Aplicación de prácticas recomendables

Esta sección incluye los siguientes temas:

Prácticas recomendadas para proteger el servidor de Arcserve UDP

Puede migrar la Consola del antiguo servidor al nuevo sin perder ningún dato.

- No se debe tener la solución de copia de seguridad en el mismo dominio que Active Directory.
- Utilice cuentas de copia de seguridad.
- No utilice cuentas de administrador del dominio para tener acceso a las tareas relacionadas con el usuario. Por ejemplo, el administrador que utiliza los privilegios de administrador para leer mensajes de correo electrónico, explorar en línea, etc.
- Separe la Consola de UDP del servidor de puntos de recuperación y cree VSB para la Consola de UDP.
- Si es posible, utilice una red/VLAN de copia de seguridad dedicada.
- Si es posible, desactive SMB v1.

  Nota: No se puede desactivar cuando se utiliza Red Hat o Centos v6.6 y posterior ya que utilizan SMB v1.

Exclusión de archivos desde la exploración de antivirus

El software de antivirus puede interferir en la correcta ejecución del proceso de Virtual Standby mediante un bloqueo del acceso a los archivos de manera temporal o bien poniendo en cuarentena o suprimiendo archivos que se han clasificado incorrectamente como sospechosos o peligrosos. Se puede configurar la mayoría de software de antivirus para excluir archivos o carpetas específicos para que se pueda omitir explorar ciertos datos. Es importante configurar el software de antivirus correctamente de modo que no interfiera en operaciones de copia de seguridad y restauración, o en cualquier otro tipo de proceso.

En un servidor Hyper-V, el software antivirus corrompe el archivo de configuración de la máquina virtual. El servidor Hyper-V cambia el estado de la máquina virtual al modo 'guardar' y la máquina virtual se corrompe y queda inservible. En tales casos, se tiene que suprimir la máquina virtual y realizar una conversión completa para crear una máquina virtual nueva.

Para garantizar que la pausa virtual local y remota funciona correctamente y para evitar que la máquina virtual entre en el modo 'guardar', excluya los siguientes archivos que apuntan a máquinas virtuales de Hyper-V:

- Directorio de archivos de configuración de la máquina virtual:

  (Valor predeterminado) C:\Archivos de programa\Microsoft\Windows\Hyper-V

  Directorio de archivos de configuración de la máquina virtual de Virtual Standby de Arcserve UDP

- Directorio de archivos del disco duro virtual de la máquina virtual:

  (Valor predeterminado) discos duros de C:\Usuarios\Public\Documents\Hyper-V\Virtual Hard Disks

  Directorio de archivos del disco duro de la máquina virtual de Virtual Standby de Arcserve UDP

- Directorio de archivos de instantáneas:

  (Valor predeterminado) %systemdrive%\ProgramData\Microsoft\Windows\Hyper-V\Snapshots

  Directorio de archivos de la instantánea de la máquina virtual de Virtual Standby de Arcserve UDP

Configuración de los parámetros de multitransmisión

Los valores de configuración relacionados con la replicación sobre WAN se guardan en la siguiente clave de registro:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\Network]

La lista siguiente muestra la clave de registro y su valor predeterminado:

- "WAN_EnableAutoTunning"=REG_DWORD:0x00000001 (1)
- "WAN_ChunkSizeByte"=REG_DWORD:0x000010000 (65536)
- "WAN_NumberofStreams"=REG_DWORD:0x00000005 (5)
- "WAN_RTT_Threshold"=REG_DWORD:0x00000014 (20)
- "WAN_MultiStreamsMaxCacheSize"=REG_DWORD:0x04000000 (67108864)
- "WAN_SendCommandFragDataMerged"=REG_DWORD:0x00000000 (0)

La descripción siguiente describe los valores de configuración de la clave de registro:

WAN_EnableAutoTunning

Especifica el conmutador para activar o desactivar la multitransmisión. Si el valor es 0, se desactiva la multitransmisión. Para otros valores, la multitransmisión está activada. El valor predeterminado para activar la multitransmisión es 1.

WAN_ChunkSizeByte

Especifica el tamaño del fragmento de datos para cada paquete. El tamaño del paquete afecta al rendimiento. Si el ancho de banda de WAN es más alto, el tamaño del fragmento de datos se puede aumentar aún más.

El valor predeterminado es 64 k bytes. El intervalo se limita de 512 bytes a 1 M bytes en el código.

WAN_NumberofStreams

Especifica el número de flujos que se debe crear en WAN, cuando la latencia es mayor que el número de WAN_RTT_Threshhold. El número de flujos predeterminado es 5. El intervalo de flujos va de 1 a 10.

WAN_RTT_Threshold

Cuando RTT es mayor que WAN_RTT_Threshold, se crean varios sockets. La unidad de WAN_RTT_Threshold es el milisegundo (ms). El valor predeterminado es 20 milisegundos. El intervalo se limita de 20 ms a 600 ms.

WAN_MultiStreamsMaxCacheSize

Especifica que el tamaño de la memoria se adjudicará se activa la multitransmisión. Este búfer de memoria se utilizará para colocar en la memoria caché la memoria recibida destrozada. El intervalo está comprendido entre 16 MB y 64 MB. El valor predeterminado es 64 MB. Si el valor es cero, el valor se establecerá en 64 MB. La unidad de este valor es BYTE.

WAN_SendCommandFragDataMerged

Especifica que si el valor no es cero, la biblioteca de comunicación agrupa los archivos pequeños y los envía en un fragmento. Si el valor es cero, se envían los archivos pequeños individualmente. El valor predeterminado es cero.

Notas:

- En una tarea de replicación, es posible que el número de conexiones de socket no sea coherente con el registro WAN_NumberofStreams.

  Tarea de replicación desde no GDD a no GDD

  Cuando RTT es mayor que WAN_RTT_Threshold, el número de conexiones de socket es igual a WAN_NumberofStreams.

  Tarea de replicación desde no GDD a GDD o desde GDD a GDD

  Hay cuatro tipos de conexiones. Solamente la conexión del bloque de datos funciona con la función de multitransmisión. Así, cundo RTT es mayor que WAN_RTT_Threshold, la conexión de socket total es 3+WAN_NumberofStreams.

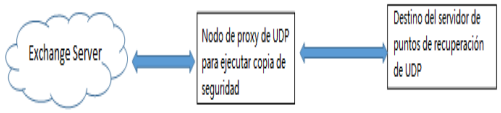
- La tarea de replicación detecta el estado de red para determinar si la comunicación está en WAN o no. Si el estado de la red es débil, se puede aceptar la LAN como WAN.

Relacionados con Exchange Online

Esta sección incluye los siguientes temas:

Configuración para obtener un rendimiento óptimo

Posible topología:



Se puede tener instalado el servidor proxy en el servidor de puntos de recuperación o por separado. Sin embargo, se recomienda poner ambos en el mismo nodo para obtener un rendimiento óptimo.

Configuración recomendada para el servidor proxy

- Arquitectura: Equipo de Windows de 64 bits. Para obtener más información sobre los sistemas operativos compatibles con Arcserve UDP, haga clic aquí.
- Memoria: 8 GB o superior
- CPU: 2 núcleos

Configuración recomendada para el servidor de puntos de recuperación:

Consulte las Notas de la versión para obtener los requisitos del sistema.

Prácticas recomendadas para las copias de seguridad

- Se debe esperar una mayor duración de la copia de seguridad en la primera copia de seguridad completa que obtiene los datos del servidor de Microsoft Exchange Online a través de un vínculo WAN.
- Como la duración de la copia de seguridad para la primera copia de seguridad completa es larga, garantice la configuración necesaria para el hardware, la red y la disponibilidad de los recursos (por ejemplo, el espacio en disco en el destino, la memoria, la CPU, etc.) durante la copia de seguridad para evitar interrupciones debido a errores en el entorno.
- Reanude la copia de seguridad desde el punto de pausa durante alguno de los siguientes escenarios:
  - Asegúrese de que no se está ejecutando una copia de seguridad durante un período de inactividad o interrupción de red planeado. Si se está ejecutando, se deberá cancelar la copia de seguridad. Cuando se cancela, la copia de seguridad conserva el punto de recuperación de la copia de seguridad parcialmente y se puede reanudar desde el punto de pausa en la siguiente programación de la copia de seguridad.
  - Si durante la copia de seguridad el equipo se apaga o se termina el proceso de forma inesperada, se eliminará el punto de recuperación de la tarea en ejecución. Inicie la copia de seguridad de nuevo. La copia de seguridad no se inicia desde el punto de pausa. Se realiza la copia de seguridad de todos los datos otra vez.
- Siempre se recomienda utilizar un nodo con el mecanismo de protección automática para proteger todos los buzones de correo, incluidos los buzones de correo recién creados después de crear el plan.
- En Arcserve UDP , el tamaño compatible de los datos protegidos está limitado a 8 terabytes (comprimidos) de forma predeterminada. Para configurar el tamaño, se puede crear el siguiente valor del registro en el nodo del servidor proxy:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<GUIDNodo>]

  " VirtualDiskSize "=dword:00000002

  El ejemplo anterior establece el tamaño en 2 TB.

Nota: Al aumentar el tamaño del disco virtual convierte la siguiente tarea de copia de seguridad incremental en una completa y también afecta a la velocidad de las tareas siguientes:

Copia en cinta, Replicación, Copia de punto de recuperación en la nube.

- Seleccione el tamaño del disco virtual basándose en el tamaño actual de los datos de origen y su crecimiento.

  Por ejemplo: si el tamaño total de todos los usuarios es de 5 TB y el crecimiento medio de los datos por día es de 1 %, es decir, 50 GB, se necesitarán 5 TB + 50 GB * 30 días = 6,5 TB de espacio en disco para alojar la primera copia de seguridad completa y las 30 copias de seguridad incrementales diarias durante un mes.

  Como resultado, el tamaño mínimo del disco requerido es de 7 TB (sin comprimir). Para conservar más puntos de recuperación, utilice el mismo método utilizado para calcular el tamaño.

- Utilice las programaciones de limitación correctamente para asegurarse de que la copia de seguridad obtenga el ancho de banda deseado fuera del horario laboral. Ejecute una copia de seguridad pequeña con pocos usuarios para evaluar la utilización de la red por parte de la tarea de copia de seguridad y para establecer los valores de la limitación en consecuencia.

- Asegúrese de que la cuenta de la copia de seguridad cumpla los requisitos previos obligatorios. Para obtener más información, consulte este vínculo.

- Si el vínculo de la red utilizado para conectar el servidor de Exchange Online es inestable y da como resultado frecuentes cancelaciones de las copias de seguridad, configure la política de retención del punto de recuperación para mantener un gran número de sesiones no combinadas.

  Valor predeterminado de las copias de seguridad incrementales diarias: 7

  Valor predeterminado de las copias de seguridad manuales: 31

  Configure las programaciones de la copia de seguridad para conservar al menos una copia de seguridad diaria, semanal y mensual.

- Asegúrese de que la instalación tenga suficientes licencias. Se puede gestionar la licencia mediante el gestor de licencias. Para obtener más información, consulte la pregunta 4 en la sección Preguntas más frecuentes.

Prácticas recomendadas para la restauración

Asegúrese de que la cuenta utilizada para la restauración ha solicitado los permisos para suplantar al usuario de destino seleccionado. Para obtener más detalles, consulte este vínculo.

Preguntas más frecuentes sobre Exchange Online

1. ¿Puedo utilizar el servidor de puntos de recuperación directamente para realizar la copia de seguridad de los usuarios de Exchange Online sin utilizar ningún servidor proxy?

   Sí, se puede hacer.

2. ¿Necesito tener una cuenta de administrador/administrador de grupo para realizar la copia de seguridad de los buzones de Exchange Online?

   No, la cuenta de copia de seguridad solo necesita un conjunto específico de permisos. Para obtener más detalles, consulte este vínculo.

3. ¿Qué tipo de rendimiento puedo esperar de las copias de seguridad de Exchange Online si el ancho de banda de Internet es bueno?

   Además del ancho de banda de la red, el rendimiento también está limitado por la velocidad a la que se leen los datos de Exchange Server que está controlado por el diseño de Exchange Server.

   A veces, Exchange Server rechaza la conexión con Arcserve UDP para leer los datos. En tales casos, Arcserve UDP sigue intentándolo hasta que obtiene una conexión correcta. Este tiempo de espera más largo puede producir un rendimiento inferior.

4. Si tengo más usuarios configurados en el plan de la copia de seguridad que el número de licencias, ¿puedo ejecutar copias de seguridad parciales de los usuarios con licencia?

   No, no se puede. Si se ejecuta la copia de seguridad para más usuarios que el número de licencias disponibles, se producirá un error en la copia de seguridad de todos los usuarios. Por ejemplo, si se han configurado 100 usuarios que se deben proteger en la Consola de Arcserve UDP pero se tienen 90 licencias disponibles, se producirá un error en la copia de seguridad. Para ejecutar correctamente la copia de seguridad, se deben eliminar 10 o más usuarios de la lista de usuarios protegidos.

5. ¿Cómo puedo mejorar el rendimiento de la copia de seguridad?

   Tenga en cuenta los siguientes puntos para garantizar un rendimiento óptimo:

   - Divida una copia de seguridad grande en tareas de copia de seguridad más pequeñas y fáciles de gestionar.

- En la configuración del plan, excluya las carpetas de las que no se desea realizar la copia de seguridad. Por ejemplo, Clutter, Sync Issues, etc.
- Compruebe periódicamente la infraestructura de la red interna y externa.

Relacionados con Microsoft Azure

Esta sección incluye los siguientes temas:

Prácticas recomendadas para una máquina virtual instantánea en Microsoft Azure

Para proteger los nodos en la red local, se debe instalar la Consola de UDP en el host.

- Seleccione HTTPS como protocolo al instalar los componentes de UDP.
- La forma más sencilla para crear un grupo de recursos es crear al menos una máquina virtual de prueba. Azure le guiará a través de los pasos para crear todos los recursos para la máquina virtual de prueba que puede utilizar para la máquina virtual en espera.
- (Opcional) Cree un servidor de puntos de recuperación en Azure.

  Siga estos pasos:

  1. Abra los puertos TCP 8014 y 8015 de entrada.
  2. Si accede al servidor de puntos de recuperación desde un explorador web remoto, resuelva el nombre del servidor de puntos de recuperación en la dirección IP pública.
  3. Utilice la tarea compartida del plan "Replicación en un servidor de puntos de recuperación gestionado remotamente".

Implementación de Arcserve UDP en Microsoft Azure

Revise las siguientes prácticas recomendadas antes de implementar Arcserve UDP en Microsoft Azure:

1. Debe instalar la Consola de Arcserve UDP localmente para proteger los nodos que se encuentran en la red local.

2. Seleccione el protocolo HTTPS durante la instalación de los componentes de Arcserve UDP.
3. La forma más sencilla de crear recursos de Azure es crear al menos una máquina virtual de prueba que se pueda utilizar como la máquina virtual de Virtual Standby más tarde.
4. Cree el servidor de puntos de recuperación de Arcserve UDP en Azure.
    - Mantenga los puertos TCP 8014 y 8015 abiertos para las conexiones entrantes.
    - Debe resolver el nombre del servidor de puntos de recuperación para la dirección IP pública si accede al servidor de puntos de recuperación desde un explorador web remoto.
    - Utilice la tarea compartida del plan **Replicación en un servidor de puntos de recuperación gestionado remotamente** para replicar tareas.

Capítulo 12: Solución de problemas

Esta sección incluye los siguientes temas:

Información relacionada con un error de comunicación de Arcserve UDP

En esta sección se incluyen los siguientes temas de solución de problemas relacionados con errores de comunicación de Arcserve UDP:

- Arcserve UDP no se puede comunicar con nodos de Windows
- No se pueden recibir alertas de correo electrónico desde la cuenta de Gmail
- Arcserve UDP no se puede comunicar con el servidor de copia de seguridad de Linux de Arcserve UDP en nodos remotos
- Arcserve UDP no se puede comunicar con el servidor de puntos de recuperación de Arcserve UDP en nodos remotos
- Arcserve UDP no se puede comunicar con el servidor de Arcserve Backup en nodos remotos
- Arcserve UDP no se puede comunicar con el sitio remoto

Arcserve UDP no se puede comunicar con nodos de Windows

Válido en sistemas operativos Windows.

Síntoma

Arcserve UDP no se puede comunicar con nodos de Windows.

Solución

La tabla siguiente describe los motivos por los cuales Arcserve UDP no se puede comunicar con nodos de Windows y la acción correctiva correspondiente:

Causa	Acción correctiva
La red no estaba disponible o no estaba estable en el momento de aplicar los planes.	Compruebe que la red se encuentre disponible y en situación estable e inténtelo de nuevo. Arcserve UDP puede hacer ping hacia el nodo remoto y el nodo remoto puede volver a hacer ping hacia Arcserve UDP.
El recurso compartido de red Admin$ del nodo remoto no estaba disponible cuando Arcserve UDP intentaba comunicarse con el nodo.	Compruebe que el recurso compartido de red Admin$ del nodo remoto esté disponible e inténtelo de nuevo.
El nodo del Agente de Arcserve Unified Data Protection para Windows no ha podido gestionar la carga cuando Arcserve UDP intentaba comunicarse con el nodo.	Verifique que la CPU del nodo remoto del Agente de Arcserve Unified Data Protection para Windows se encuentra en un estado normal e inténtelo de nuevo.
El servicio Agente de Arcserve Unified Data Protection para Windows del nodo remoto no se estaba ejecutando cuando Arcserve UDP intentaba comunicarse con el nodo.	Verifique que el Agente de Arcserve Unified Data Protection para Windowsse esté ejecutando en el nodo remoto e inténtelo de nuevo.
Se ha utilizado un protocolo o un puerto incorrecto para comunicarse con el nodo.	Utilice el protocolo o el puerto correcto para agregar o actualizar el nodo remoto en la vista de nodos de Arcserve UDP.
El servicio Agente de Arcserve Unified Data Protection para Windows no se estaba comunicando correctamente.	Reinicie el servicio Agente de Arcserve Unified Data Protection para Windows en el nodo remoto e inténtelo de nuevo.

No se pueden recibir alertas de correo electrónico desde la cuenta de Gmail

La cuenta de Gmail está bloqueada por Google si se utiliza la cuenta de Gmail en los valores de configuración del correo electrónico.

Válido en plataformas de Windows.

Síntoma

Al configurar las cuentas de Gmail, no se reciben alertas de correo electrónico. Cuando se intenta configurar la cuenta de Gmail para obtener alertas de correo electrónico y se hace clic en Enviar un correo electrónico de prueba, se recibirá uno de los siguientes mensajes de error:

El correo electrónico de prueba ha producido un error debido a credenciales del usuario incorrectas.

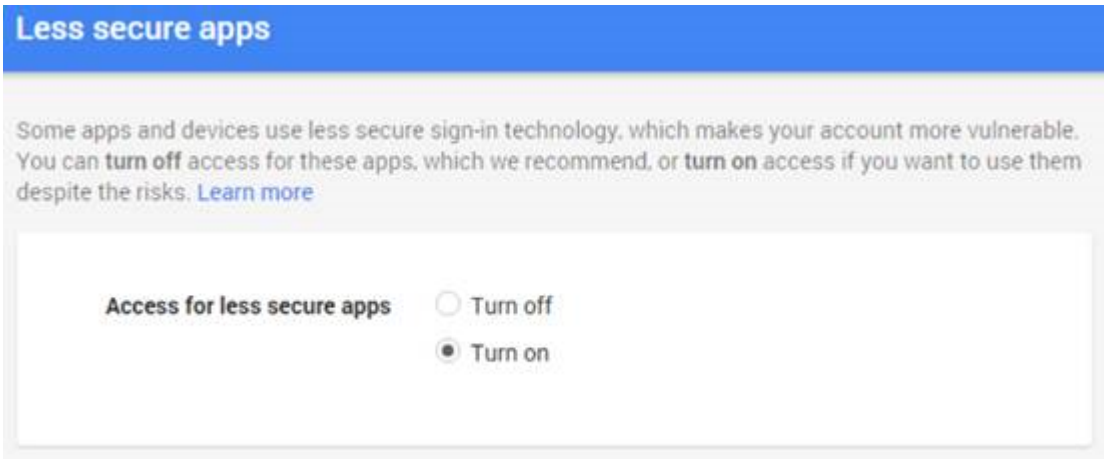
o

Se ha producido un error al enviar el correo electrónico de prueba: Las credenciales del usuario no son válidas.

Solución

1. Proporcione las credenciales correctas e inténtelo de nuevo.
2. La seguridad de Google bloquea los correos electrónicos de la cuenta de Gmail configurada fuera de Google. Para evitar este problema, en el vínculo siguiente modifique la configuración seleccionando Activar para utilizar el acceso para aplicaciones menos seguras:

   https://www.google.com/settings/security/lesssecureapps



Arcserve UDP no se puede comunicar con el servidor de copia de seguridad de Linux de Arcserve UDP en nodos remotos

Válido en los sistemas operativos de Linux.

Síntoma

Arcserve UDP no se puede comunicar con el servidor de copia de seguridad de Linux de Arcserve UDP en nodos remotos.

Solución

La tabla siguiente describe los motivos por los cuales Arcserve UDP no se puede comunicar con el servidor de copia de seguridad de Linux de Arcserve UDP en nodos remotos y la acción correctiva correspondiente:

Causa	Acción correctiva
La red no estaba disponible o no era estable cuando Arcserve UDP intentó comunicarse con el nodo del servidor de copia de seguridad de Linux.	Compruebe que la red se encuentre disponible y en situación estable e inténtelo de nuevo. Arcserve UDP puede hacer ping en el nodo remoto del servidor de copia de seguridad de Linux y el nodo remoto del servidor de copia de seguridad de Linux puede devolver el ping a Arcserve UDP.
El nodo del servidor de copia de seguridad de Linux de Arcserve UDP no ha podido gestionar la carga cuando Arcserve UDP intentaba comunicarse con el nodo.	Compruebe que la CPU en el nodo remoto del servidor de copia de seguridad de Linux de Arcserve UDP se encuentre en estado normal e inténtelo de nuevo.
El servicio del servidor de copia de seguridad de Linux de Arcserve UDP en el nodo remoto no se estaba ejecutando cuando Arcserve UDP intentaba comunicarse con el nodo.	Compruebe que el servicio del servidor de copia de seguridad de Linux de Arcserve UDP en el nodo remoto se esté ejecutando e inténtelo de nuevo.
El servicio del servidor de copia de seguridad de Linux de Arcserve UDP no se estaba comunicando correctamente.	Reinicie el servicio del servidor de copia de seguridad de Linux de Arcserve UDP en el nodo remoto e inténtelo de nuevo.

Arcserve UDP no se puede comunicar con el servidor de puntos de recuperación de Arcserve UDP en nodos remotos

Válido en sistemas operativos Windows.

Síntoma

Arcserve UDP no se puede comunicar con el servidor de puntos de recuperación de Arcserve UDP en nodos remotos.

Solución

La tabla siguiente describe los motivos y la acción correctiva correspondiente:

Causa	Acción correctiva
La red no estaba disponible o no estaba estable cuando Arcserve UDP intentaba comunicarse con el nodo del servidor de puntos de recuperación.	Compruebe que la red se encuentre disponible y en situación estable e inténtelo de nuevo. Arcserve UDP puede hacer ping en el nodo remoto del servidor de puntos de recuperación y el nodo remoto del servidor de puntos de recuperación puede volver a hacer ping en Arcserve UDP.
El recurso compartido de red Admin$ del nodo del servidor de puntos de recuperación de Arcserve UDP no estaba disponible cuando Arcserve UDP intentaba comunicarse con el nodo.	Compruebe que el recurso compartido de red Admin$ del nodo del servidor de puntos de recuperación esté disponible e inténtelo de nuevo.
El nodo del servidor de puntos de recuperación de Arcserve UDP no ha podido gestionar la carga cuando Arcserve UDP intentaba comunicarse con el servidor.	Compruebe que la CPU en el nodo remoto del servidor de puntos de recuperación se encuentre en estado normal e inténtelo de nuevo.
El servicio del Agente de Arcserve UDP, el servicio del almacén de datos del servidor de puntos de recuperación de Arcserve UDP o el servidor de uso compartido de puertos del servidor de puntos de recuperación de Arcserve UDP en el nodo remoto no se estaban ejecutando cuando Arcserve UDP intentaba comunicarse con el nodo.	Compruebe que el servicio del Agente de Arcserve UDP, el servicio del almacén de datos del servidor de puntos de recuperación de Arcserve UDP y el servidor de uso compartido de puertos del servidor de puntos de recuperación de Arcserve UDP en el nodo remoto se estén ejecutando e inténtelo de nuevo.
Se ha utilizado un protocolo o un puerto incorrecto para comunicarse con el ser-	Utilice el protocolo o el puerto correcto para agregar o actualizar el

vidor de puntos de recuperación.	nodo del servidor de puntos de recuperación en la vista de nodos de destino de Arcserve UDP.
El servicio del Agente de Arcserve UDP, el servicio del almacén de datos del servidor de puntos de recuperación de Arcserve UDP o el servidor de uso compartido de puertos del servidor de puntos de recuperación de Arcserve UDP no se estaban comunicando correctamente.	Reinicie el servicio del Agente de Arcserve UDP, el servicio del almacén de datos del servidor de puntos de recuperación de Arcserve UDP y el servidor de uso compartido de puertos del servidor de puntos de recuperación de Arcserve UDP en el nodo remoto e inténtelo de nuevo.

Arcserve UDP no se puede comunicar con el servidor de Arcserve Backup en nodos remotos

Válido en sistemas operativos Windows.

Síntoma

Arcserve UDP no se puede comunicar con el servidor de Arcserve Backup en nodos remotos.

Solución

La tabla siguiente describe los motivos por los cuales Arcserve UDP no se puede comunicar con de servidor de Arcserve Backup en nodos remotos y la acción correctiva correspondiente:

Causa	Acción correctiva
La red no estaba disponible o no era estable cuando Arcserve UDP intentó comunicarse con el nodo del servidor de Arcserve Backup.	Compruebe que la red se encuentre disponible y en situación estable e inténtelo de nuevo. Arcserve UDP puede hacer ping en el nodo remoto del servidor de Arcserve Backup y el nodo remoto del servidor de Arcserve Backup puede devolver el ping a Arcserve UDP.
El nodo del servidor de Arcserve Backup no ha podido gestionar la carga cuando Arcserve UDP intentaba comunicarse con el nodo.	Compruebe que la CPU en el nodo remoto del servidor de Arcserve Backup se encuentre en estado normal e inténtelo de nuevo.
El servicio relacionado con el servidor de Arcserve Backup en el nodo remoto no se estaba ejecutando cuando Arcserve UDP intentaba comunicarse con el nodo.	Compruebe que el servidor de Arcserve Backup en el nodo remoto se esté ejecutando e inténtelo de nuevo.
Se ha utilizado un protocolo o un puerto incorrecto para comunicarse con el nodo del servidor de Arcserve Backup.	Utilice el protocolo o el puerto correcto para agregar o actualizar el servidor de Arcserve Backup en la vista de nodos de destino de Arcserve UDP.
El servicio relacionado con el servidor de Arcserve Backup no se estaba comunicando correctamente.	Reinicie el servicio relacionado con el servidor de Arcserve Backup en el nodo remoto e inténtelo de nuevo.

Arcserve UDP no se puede comunicar con el sitio remoto

Válido en sistemas operativos Windows.

Síntoma

Arcserve UDP no se puede comunicar con el sitio remoto.

Solución

La tabla siguiente describe los motivos por los cuales Arcserve UDP no se puede comunicar con el sitio remoto y la acción correctiva correspondiente:

Causa	Acción correctiva
La red no está disponible o no está estable.	Compruebe que la red se encuentre disponible y en situación estable e inténtelo de nuevo.
Se ha reinstalado Arcserve UDP y el sitio remoto no está registrado en Arcserve UDP.	Registre el sitio remoto en Arcserve UDP.
Ha cambiado el nombre de host o la dirección IP de Arcserve UDP y el sitio remoto no está registrado en Arcserve UDP.	Registre el sitio remoto en Arcserve UDP.
Ha cambiado el nombre de host o la dirección IP del sitio remoto y el sitio remoto no está registrado en Arcserve UDP.	Registre el sitio remoto en Arcserve UDP.

Relacionados con planes, tareas y configuración

En esta sección se incluyen los siguientes temas de solución de problemas relacionados con la configuración y las tareas de copia de seguridad:

- Error en la tarea de copia de seguridad tras cambiar la dirección IP o el nombre de host de la Consola
- Cómo agregar la contraseña de cifrado para un destino cifrado existente
- No se pueden aplicar valores de configuración de la copia de seguridad al nodo
- Error en la implementación del plan tras cambiar la contraseña del equipo proxy de copia de seguridad sin agente
- Valores de configuración desactivados al abrir la interfaz de usuario del Agente
- Error al pausar y reanudar cuando el Agente no está conectado a la red
- El servicio del Agente de Arcserve UDP se ejecuta lentamente
- Configuración del registro para volver a ejecutar una tarea de copia en cinta
- Configuración del registro para copiar varios puntos de recuperación del mismo tipo a la cinta en la misma tarea
- Falta un archivo o carpeta de la copia de seguridad de la carpeta compartida de NFS o el nombre de archivo o carpeta está dañado
- Error de la copia de seguridad de la carpeta compartida de NFS
- Nombre de servidor incorrecto en la solicitud de licencia para las rutas UNC
- Restablecimiento de la Consola de UDP activada para MFA cuando TOTP no está disponible

Error en la tarea de copia de seguridad tras cambiar la dirección IP o el nombre de host de la Consola

Síntoma

He instalado la Consola y el servidor de punto de recuperación en el mismo equipo. La copia de seguridad funcionaba correctamente pero después de cambiar la dirección IP/nombre de host de la Consola, se produce un error en la tarea de copia de seguridad.

Solución

Este problema ocurre cuando se tienen planes asignados a nodos y, a continuación, se modifica la dirección IP/nombre de host de este equipo.

Para resolver esta incidencia, actualizar manualmente los nodos del agente y ejecute la tarea de copia de seguridad otra vez.

Siga estos pasos:

1. Vaya a la página Nodos: Todos los nodos.
2. Seleccione el nodo.
3. Haga clic con el botón secundario del ratón y seleccione **Actualizar**.
4. Haga clic en **Aceptar**.

Los nodos se actualizan.

Cómo agregar la contraseña de cifrado para un destino cifrado existente

Síntoma

Se ha olvidado de agregar la contraseña de cifrado para el destino de copia de archivos.

Solución

Ahora se puede agregar la contraseña de cifrado.

Siga estos pasos:

1. Abra el plan.
2. Abra el destino de copia de archivos en el que se debe agregar la contraseña de cifrado.
3. Cambie el tipo de destino de Almacenamiento en la nube\Recurso compartido de red a Recurso compartido de red\Almacenamiento en la nube.
4. Proporcione cualquier recurso compartido de red o almacenamiento en la nube y guarde los valores.
5. Vuelva a abrir el plan y vaya al destino de la copia de archivos.
6. Cambie el destino a Distribuidor de la nube\Recurso compartido de red.
7. Seleccione Distribuidor de la nube\Recurso compartido de red y, a continuación, seleccione la ruta del proveedor del contenedor o depósito.
8. Proporcione la contraseña de cifrado correcta.
9. Guarde el plan.

No se pueden aplicar valores de configuración de la copia de seguridad al nodo

Síntoma

Tengo dos consolas, la Consola A y la Consola B. Agrego un servidor de puntos de recuperación (RPS) a la Consola A y creo un plan para el servidor de puntos de recuperación. A continuación, agrego el servidor de puntos de recuperación a la Consola B. Ahora la Consola B gestiona este servidor de puntos de recuperación. Sin embargo, cuando actualizo el nodo del agente de la Consola A del que se realiza una copia de seguridad en el servidor de puntos de recuperación, obtengo el error siguiente:

No se pueden aplicar valores de configuración de la copia de seguridad al nodo. (Se ha producido un error al buscar el plan del servidor de punto de recuperación de Arcserve UDP en este servidor.)

Solución

Para evitar este error, siga estos pasos:

1. Seleccione el plan en la Consola A.
2. En el panel central, haga clic en **Acciones** y, a continuación, seleccione **Implementar ahora**.

   El plan se vuelve a implementar y los valores de configuración de la copia de seguridad se aplican al nodo.

Error en la implementación del plan tras cambiar la contraseña del equipo proxy de copia de seguridad sin agente

Síntoma

Si la consola y el servidor proxy se encuentran en equipos diferentes, se produce un error en el plan de reimplementación después de cambiar la contraseña del equipo proxy. El mensaje de error indica que las credenciales no son correctas.

Solución

Siga estos pasos para solucionar la incidencia:

1. En la vista de nodo en la Consola, actualice el servidor proxy con las nuevas credenciales.
    a. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.
    b. Haga clic con el botón secundario del ratón en el nodo y seleccione **Actualizar** para actualizar el servidor proxy.
2. Si el servidor de puntos de recuperación y el servidor proxy se encuentran en el mismo equipo, actualice el servidor de puntos de recuperación con las nuevas credenciales.
    a. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.
    b. Haga clic en el servidor de puntos de recuperación desde el panel central y seleccione **Actualizar**.
3. Reinicie el servicio del Agente de Arcserve UDP en el equipo proxy.
4. Vuelva a implementar el plan.

Valores de configuración desactivados al abrir la interfaz de usuario del Agente

Si no se eliminan los nodos del Agente de Arcserve UDP (Windows) desde la interfaz de usuario de Arcserve UDP antes de desinstalar la Consola de Arcserve UDP, los valores de configuración se desactivarán al abrir la interfaz de usuario del agente en esos nodos del Agente de Arcserve UDP (Windows).

Síntoma

No se notifica al nodo del Agente de Arcserve UDP (Windows) de que la Consola de Arcserve UDP está desinstalada. Se supone que se está gestionando.

Solución

Elimine los archivos RegConfigPM.xml y BackupConfiguration.xml que se encuentran bajo el directorio <UDP_ENGINE_HOME>\Configuration en el nodo del Agente de Arcserve UDP (Windows) y, a continuación, reinicie el servicio de Windows Servicio del Agente de Arcserve UDP.

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Error al pausar y reanudar cuando el Agente no está conectado a la red

Síntoma

Si el agente no está conectado a la red e intento pausar un plan, el plan no se pausa. Similarmente, si el agente no está conectado a la red e intento reanudar un plan, el plan no se reanuda.

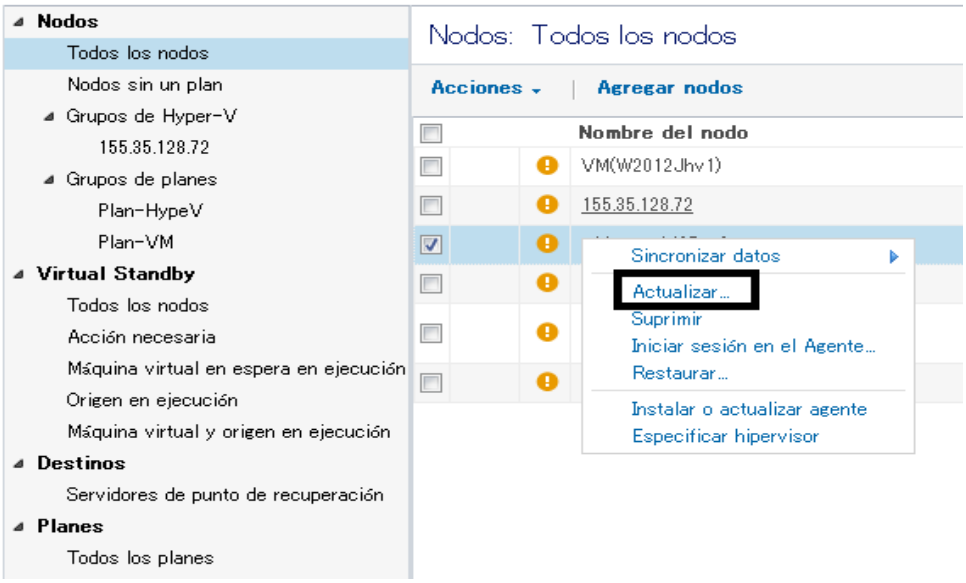
Solución

Se puede resolver esta incidencia actualizando manualmente el nodo desde la consola.

Siga estos pasos:

1. Haga clic en la ficha Recursos en la Consola.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en Todos los nodos.

   Se muestran todos los nodos agregados en el panel central.
3. En el panel central, seleccione el nodo.
4. Haga clic con el botón secundario del ratón y seleccione **Actualizar**.



El nodo se actualiza y el plan se actualiza.

El servicio del Agente de Arcserve UDP se ejecuta lentamente

Válido en sistemas operativos Windows.

Síntoma 1:

El servicio del Agente de Arcserve UDP se ejecuta en los sistemas del Agente de Arcserve UDP lentamente. Se pueden detectar otros síntomas como:

- El servicio del Agente de Arcserve UDP deja de responder u ocupa el 100% de los recursos de CPU.
- Los nodos del Agente de Arcserve UDP presentan un rendimiento bajo o no pueden comunicarse con el servicio web.

Solución 1:

En diversas configuraciones de entorno, se puede detectar que el servicio del Agente de Arcserve UDP ocupa demasiado tiempo de CPU o que la respuesta es lenta. De forma predeterminada, Tomcat está configurado para adjudicar una cantidad limitada de memoria a los nodos, lo cual puede no ser apropiado para el entorno del usuario. Para verificar este problema, puede revisar los siguientes archivos de registro:

<D2D_home>\TOMCAT\logs\casad2dwebsvc-stdout.*.log
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stder.*.log
<D2D_home>\TOMCAT\logs\catalina.*.log
<D2D_home>\TOMCAT\logs\localhost.*.log

Busque el mensaje siguiente:

java.lang.OutOfMemoryError

Para corregir este problema, se debe aumentar la cantidad de memoria adjudicada.

Para aumentar la memoria, realice los siguientes pasos:

1. Abra el Editor del registro y acceda a la clave siguiente:

   Sistemas operativos x86:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java

   Sistemas operativos x64:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java

2. Utilice una de las opciones siguientes:

- Si el mensaje que aparece en el archivo de registro es el siguiente:

  java.lang.OutOfMemoryError: Espacio PermGen

  Añada el texto siguiente al valor de Options.

  -XX:PermSize=128M -XX:MaxPermSize=128M

  Nota: Puede ser necesario aumentar el valor de -XX:MaxPermSize para adaptarlo al entorno.

- Si el mensaje que aparece en el archivo de registro es uno de los siguientes:

  java.lang.OutOfMemoryError: Java heap space
  java.lang.OutOfMemoryError: GC overhead limit exceeded

  Aumente el valor del siguiente DWORD:

  JvmMx

3. Reinicie el servicio del Agente de Arcserve UDP.

Síntoma 2

Las copias de seguridad programadas se omiten y dejan de ejecutarse.

Solución 2

Cuando se configura el valor MAX como 20 o menos que 20 para las copias de seguridad simultáneas, deben realizarse los siguientes pasos:

1. Aumente el valor del siguiente DWORD:

   JvmMx=256

   Nota: Este DWORD se trata en la Solución 1.

2. Añada el texto siguiente al valor de Options.

   -XX:MaxPermSize=128M

   Nota: Este DWORD se trata en la Solución 1.

Cuando se configura el valor MAX como 50 o menos que 20 para las copias de seguridad simultáneas, deben realizarse los siguientes pasos:

1. Aumente el valor del siguiente DWORD:

   JvmMx=512

   Nota: Este DWORD se trata en la Solución 1.

2. Añada el texto siguiente al valor de Options.

   -XX:MaxPermSize=256M

   Nota: Este DWORD se trata en la Solución 1.

Configuración del registro para volver a ejecutar una tarea de copia en cinta

Síntoma

La tarea de copia en cinta no se ha ejecutado debido a un error de medios y desea volver a ejecutarla.

Solución

Se puede controlar el número de reintentos y el intervalo de tiempo entre ellos para la tarea de copia en cinta usando las dos claves de registro siguientes. Ambas claves de registro se encuentran en el equipo en el que se haya instalado el servidor de Arcserve Backup:

NumberOfRetryCopyToTapeJob

Si se produce un error en una tarea de copia en cinta, Arcserve UDP vuelve a intentar la tarea. El número de reintentos se configura mediante la clave de registro **NumberOfRetryCopyToTapeJob**. Sin embargo, si se cambia la información del punto de recuperación o del nodo que se debe copiar en la tarea, Arcserve UDP restablece el número de errores acumulados a 0. Esto significa que, una vez cambiada la información del punto de recuperación o del nodo que se debe cambiar en la tarea, la copia en cinta se puede ejecutar sin ninguna limitación relacionada con el número de reintentos. Asimismo, si se reinicia el servicio web de Arcserve Backup, Arcserve UDP restablece el número de errores acumulados a 0.

La clave de registro se encuentra en el servidor de Arcserve Backup, en la ubicación siguiente:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo\NumberOfRetryCopyToTapeJob

El tipo es DWORD.

Predeterminado: 1

TimeIntervalOfRetryCopyToTapeJob

Controla el intervalo de tiempo de reintento para la tarea incorrecta de copia en cinta. Esta clave de registro se usa junto con **NumberOfRetryCopyToTapeJob**.

La clave de registro se encuentra en el servidor de Arcserve Backup, en la ubicación siguiente:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo\TimeIntervalOfRetryCopyToTapeJob

El tipo es DWORD.

Predeterminado: 1 hora

Configuración del registro para copiar varios puntos de recuperación del mismo tipo a la cinta en la misma tarea

Síntoma

De forma predeterminada, la tarea de copia en cinta copia todos los puntos de recuperación calificados en la cinta incluso si son del mismo tipo. Como resultado, se consume más espacio de cinta y se tarda mucho tiempo en realizar la copia. Es posible que solo desee copiar el último de los puntos de recuperación calificados.

Solución

Se puede configurar el registro en el nodo del servidor de Arcserve Backup para que active la copia en cinta del punto de recuperación más reciente del mismo tipo.

Siga estos pasos:

1. En el nodo del servidor de Arcserve Backup, agregue el siguiente valor DWORD al registro que se encuentra en [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo]:

   "CopyLatestRecoveryPointOfSameType"=dword:00000001

2. Reinicie el servicio web del servidor de Arcserve Backup para que se apliquen los cambios.

   Todas la tareas de copia en cinta en el nodo del servidor de Arcserve Backup copiarán el último punto de recuperación del mismo tipo en la cinta.

Falta un archivo o carpeta de la copia de seguridad de la carpeta compartida de NFS o el nombre de archivo o carpeta está dañado

Síntoma

Cuando se realiza la copia de seguridad de la carpeta compartida de NFS, faltan algunos archivos o carpetas de los datos de la copia de seguridad o el nombre de un archivo o carpeta se ha dañado.

Solución

Este problema se produce si un archivo o carpeta en la carpeta compartida de NFS tiene un nombre con un código de idioma no admitido. Como solución, exporte una carpeta compartida de SMB en lugar de la carpeta compartida de NFS. Tenga en cuenta que también puede agregar la ruta UNC o NFS con el protocolo de SMB.

Para obtener más información sobre cómo agregar una ruta UNC y una codificación de idioma admitida, consulte Adición de una ruta UNC.

Error de la copia de seguridad de la carpeta compartida de NFS

Síntoma

Cuando se realiza la copia de seguridad de la carpeta compartida de NFS, se produce un error en la tarea.

Solución

Este problema se produce si se modifican los valores de UID (identificador de usuario) y GID (identificador de grupo) de los valores predeterminados. Mantenga siempre los valores predeterminados de UID y GID para el cliente de NFS y el servidor de NFS.

Restablecimiento de la Consola de UDP activada para MFA cuando TOTP no está disponible

Síntoma

Después de activar el proceso de inicio de sesión de la autenticación multifactor (MFA) en la Consola de UDP, es posible realizar lo siguiente:

- Olvidarse de escanear el código QR
- Perder el dispositivo móvil que contiene una aplicación de autenticación

- Desinstalar la aplicación de autenticación

Solución 1

Si es un superadministrador o un usuario administrador o no administrador, póngase en contacto con el administrador u otros usuarios administradores de UDP para restablecer el código QR desde la Consola de UDP.

Solución 2

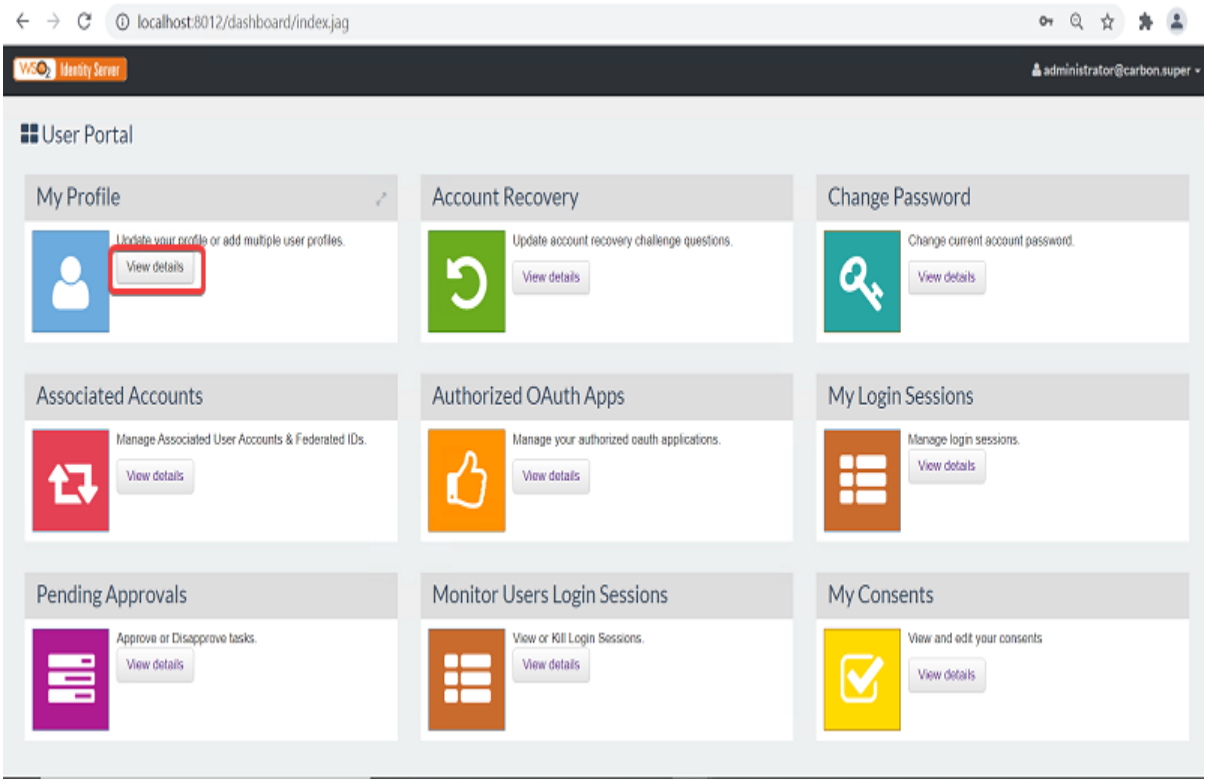
Si es un superadministrador o un usuario administrador, puede escanear la imagen del código QR para obtener un TOTP nuevo mediante el portal del cuadro de mandos de Identity Server.

Siga estos pasos:

1. Inicie sesión en el cuadro de mandos de Identity Server.

   Por ejemplo: *https://localhost:8012/dashboard*

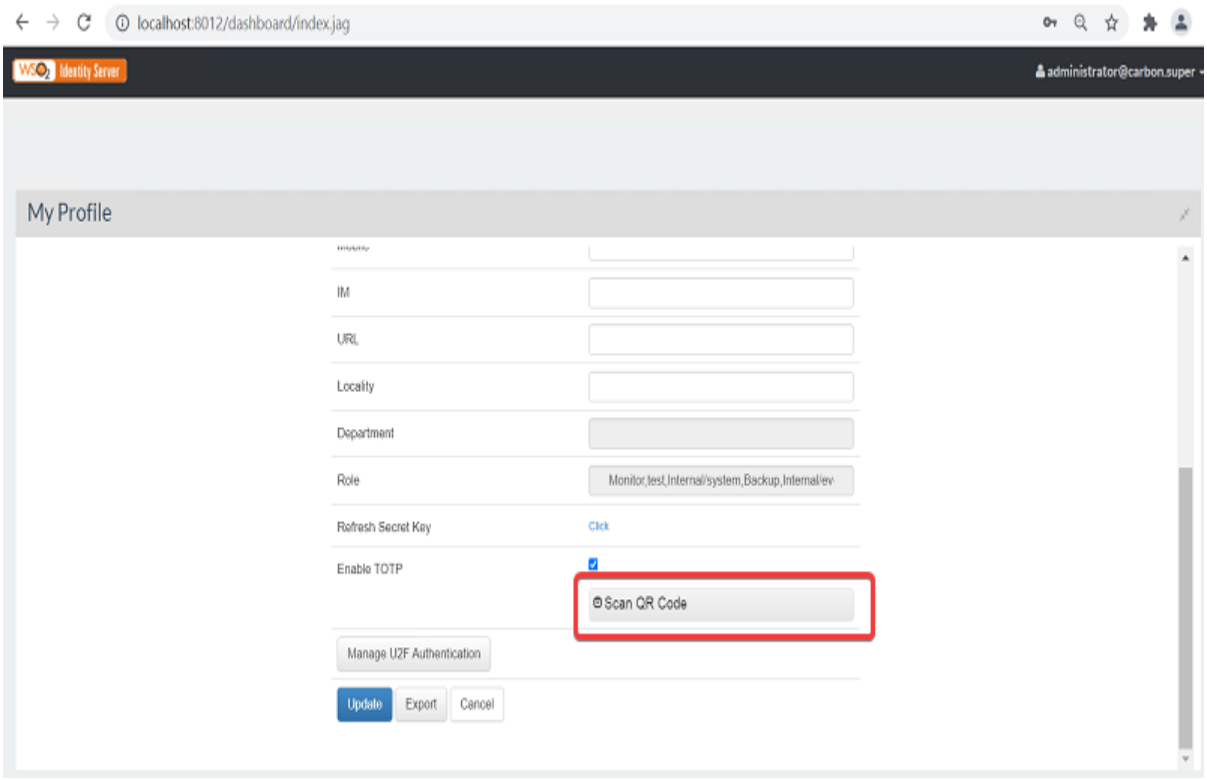
   Se abrirá la página User Portal.



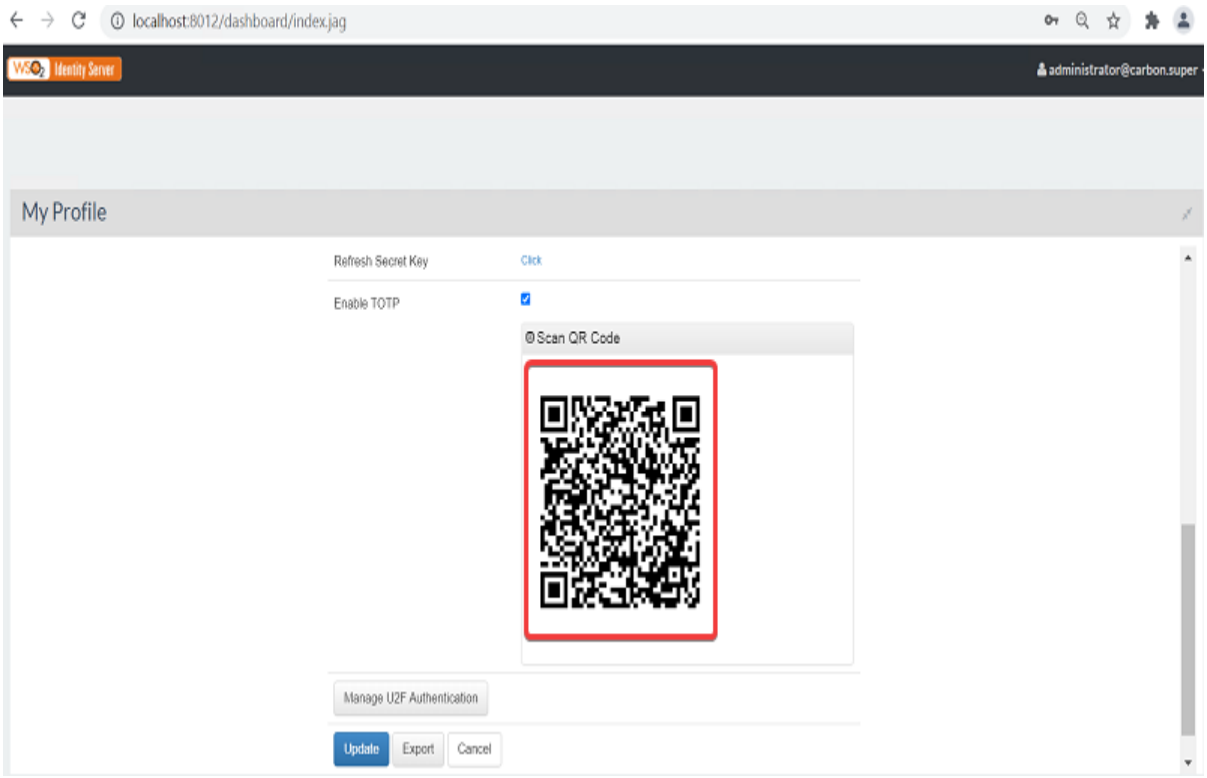
2. En la página User Portal, haga clic en **View Details**.

   Aparecerá la página My Profile.

3. En la página My Profile, en Enable TOTP, haga clic en **Scan QR code** para ver la imagen del código QR.



4. Para generar el TOTP, escanee la imagen del código QR con una aplicación de autenticación.



5. Vaya a la página de inicio de sesión de la Consola de UDP y, a continuación, inicie sesión con el nuevo TOTP generado.

Solución 3

Si es un usuario superadministrador, puede eliminar completamente la configuración existente.

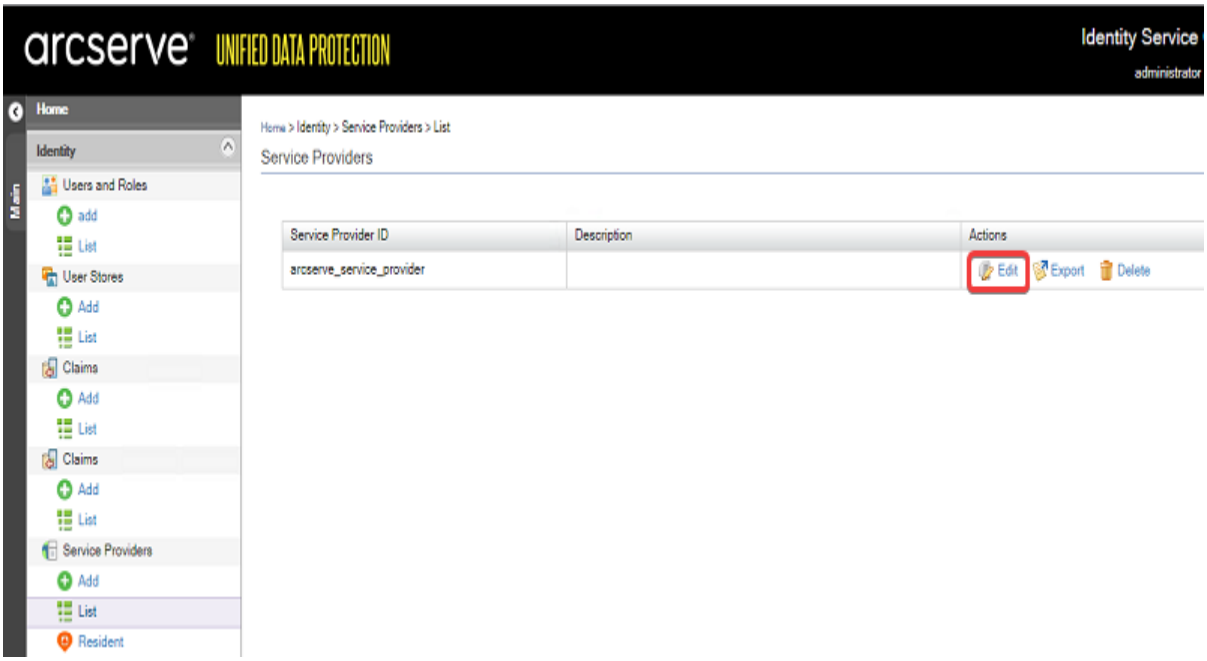
Siga estos pasos:

1. Vaya a la ruta …*Program Files**Arcserve**Unified Data Protection**Management**IdentityServer**repository**conf* y, a continuación, abra el archivo *carbon.xml* con un editor.
2. En el archivo carbon.xml, marque como comentario las etiquetas XML *HideMenuItemIds* y, a continuación, guarde el archivo.

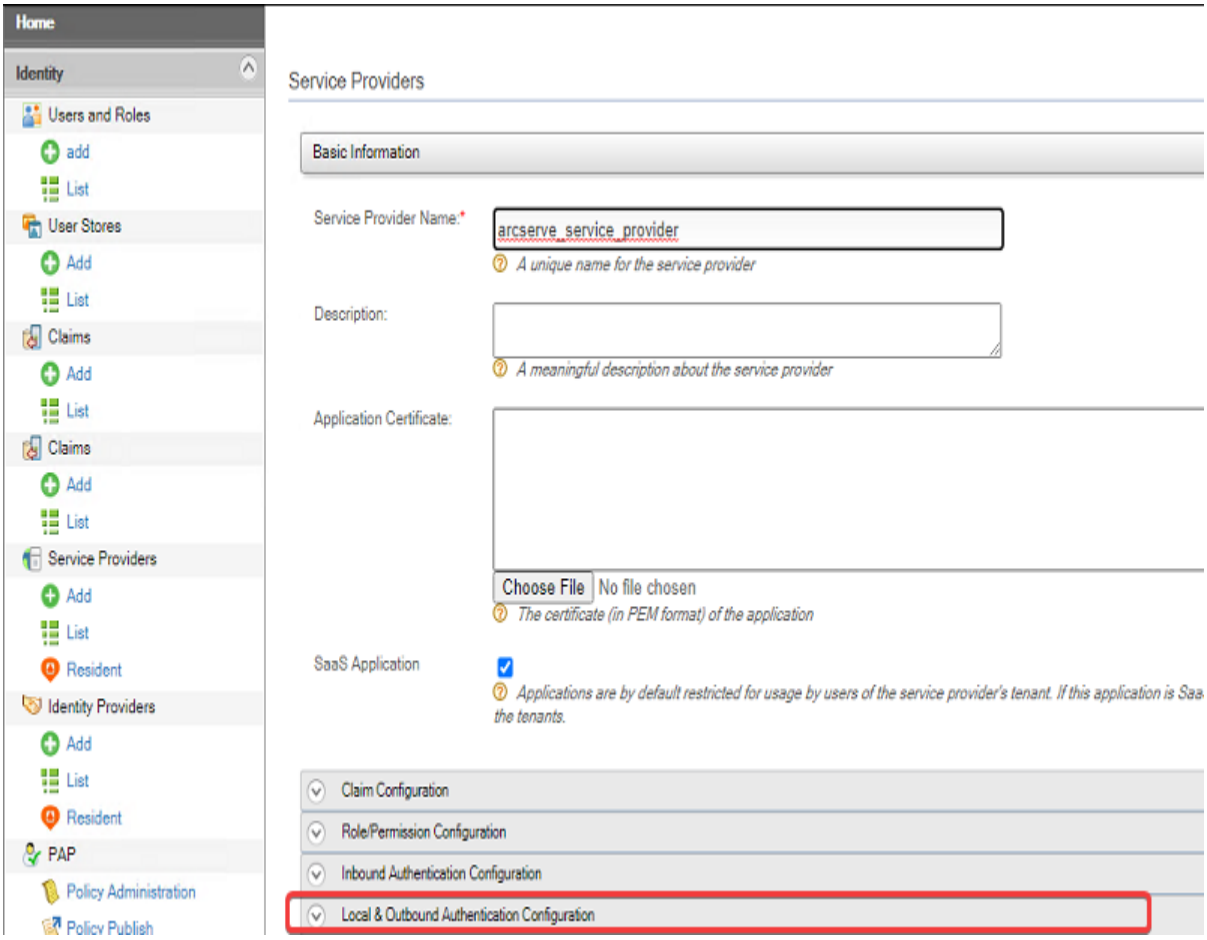


3. Reinicie el servicio de identidad de Arcserve UDP.
4. Inicie la Consola de gestión de usuarios. Para obtener más información, consulte Inicio de la Consola de gestión de usuarios de Arcserve UDP.

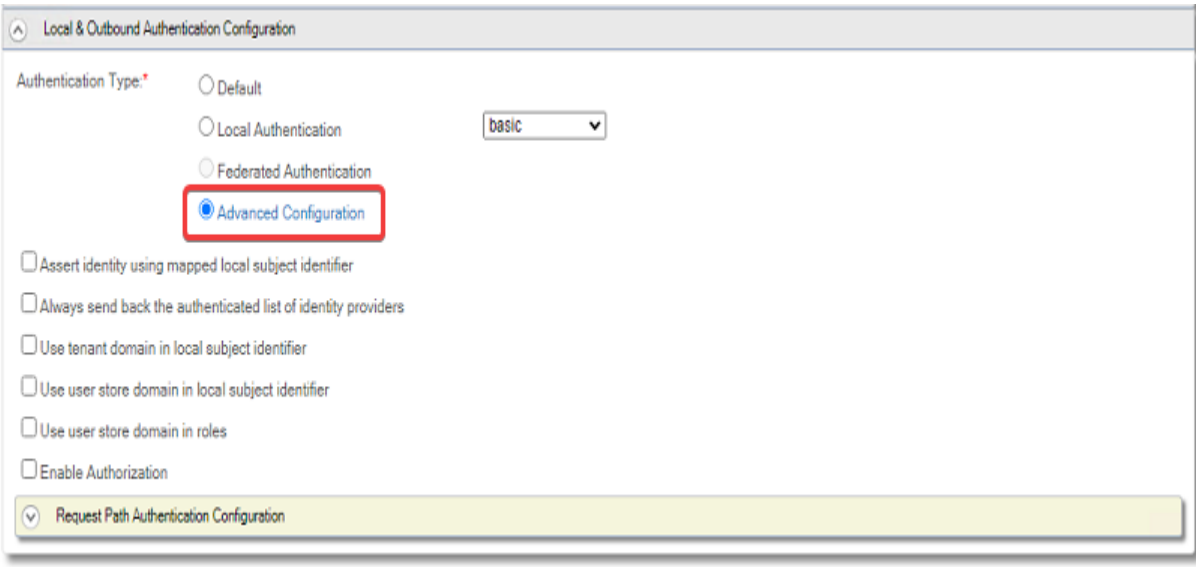
   Aparecerá la página Consola del servicio de identidad.
5. Vaya a **Inicio** > **Identidad** > **Proveedores de servicios** > **Lista**.



6. En la lista de proveedores de servicios, para *arcserve_service_provider*, haga clic en **Editar**.



7. Expanda la lista desplegable **Local & Outbound Authentication Configuration** (Configuración de la autenticación saliente y local) y, a continuación, seleccione **Configuración avanzada**.

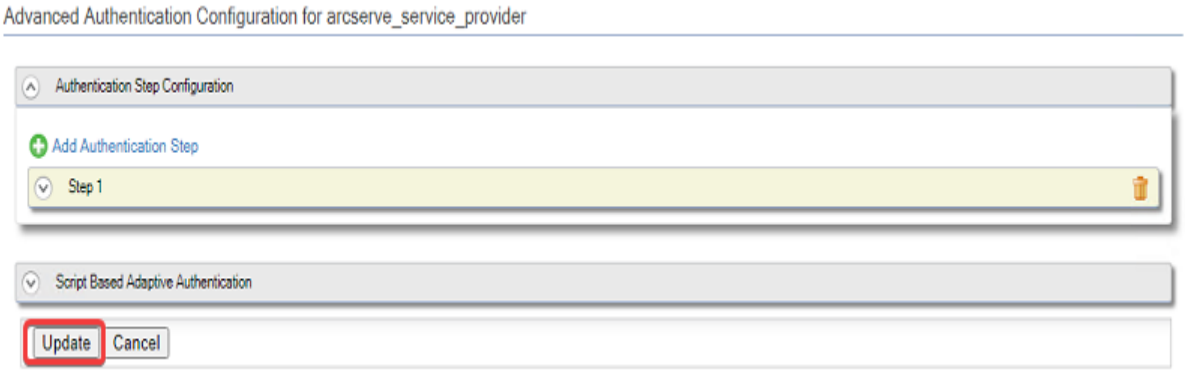


Aparecerá la página *Configuración avanzada para arcserve_service_provider*.

8. En la página *Configuración avanzada para arcserve_service_provider*, en Configuración del paso de autenticación, para eliminar el paso 2, haga clic en el icono **Suprimir**.



9. Haga clic en **Actualizar** para guardar los cambios.



Se eliminan los valores de configuración existentes.

10. Vaya a la página de inicio de sesión de UDP y, a continuación, inicie sesión con el nombre de usuario y la contraseña.
11. Vaya a **Configuración** > **Gestión de usuarios**.
12. En la sección Autenticación multifactor, para desactivar MFA, **desactive** la opción.
13. Haga clic en **Guardar**.

    La configuración para el inicio de sesión de MFA se ha eliminado correctamente.

Relacionados con la máquina virtual instantánea

En esta sección se incluyen los siguientes temas de solución de problemas relacionados con la máquina virtual instantánea:

- Error al crear una máquina virtual instantánea en VMware debido a un nombre de almacén de datos de NFS duplicado
- Error al crear una máquina virtual instantánea con Windows 2008 como el servidor de recuperación para VMware o el servidor Windows 2008 R2 Hyper-V
- Se ha producido un error al iniciar una máquina virtual instantánea si el equipo de origen es un servidor de Active Directory de Windows 2008/2012/2016
- Se ha producido un error al encender la máquina virtual después de restaurar Hyper-V
- Error en la tarea de máquina virtual instantánea debido a un fallo del servicio NFS de Windows
- No se puede acceder o suprimir la carpeta de archivos de la máquina virtual instantánea incluso con privilegios de administrador
- Fallo de inicio de la máquina virtual instantánea en Hyper-V después de reiniciar el servidor de recuperación
- Error al crear un almacén de datos de NFS de VMware y aparición del error No se puede determinar el nombre de host
- Se ha producido un error al implementar el servicio de integración en la máquina virtual invitada en Hyper-V
- Error en la máquina virtual instantánea de Linux en un servidor Hyper-V en un idioma distinto al inglés
- Consumo de una licencia adicional para rutas UNC que se encuentran en una máquina virtual de Hyper-V con licencia
- Se produce un error de licencia al cambiar la edición o el tipo de licencia y al crear una máquina virtual instantánea

Error al crear una máquina virtual instantánea en VMware debido a un nombre de almacén de datos de NFS duplicado

Síntoma

Se produce un error en la creación de la máquina virtual instantánea y aparece el siguiente mensaje de error:

Se ha producido un error al crear el almacén de datos basado en NFS [arcserve_UDP_<NombreHost/IP>] con el nombre de recurso compartido de NFS [arcserve_UDP_IVM_{GUID}]. Código de error: 12. mensaje de error: La clave, nombre o identificador especificado ya existe (detalles:).

El motivo de este error puede ser que ya existe un almacén de datos de NFS con el mismo nombre y no se elimina, o el vCenter/Host aún tiene las referencias del almacén de datos NFS en sus registros. Sin embargo, cuando se inicia sesión en el host directamente, ve un almacén de datos NFS. Este almacén de datos probablemente esté marcado como inactivo y aparezca atenuado.

Solución

Para resolver este problema:

1. Inicie sesión en el host de ESX y elimine el almacén de datos NFS.
2. Reinicie los agentes de gestión en el host ESX mediante el comando siguiente:

   ```
   /sbin/services.sh restart
   ```

Para obtener más información sobre cómo trabajar en el host ESX, consulte la documentación de VMware.

Error al crear una máquina virtual instantánea con Windows 2008 R2 como el servidor de recuperación para VMware o el servidor Windows 2008 R2 Hyper-V

Síntoma

Se produce un error al crear una máquina virtual instantánea y aparece el siguiente mensaje en el registro de actividades de tareas:

Windows no puede comprobar la firma digital de este archivo. Es posible que un cambio de hardware o de software reciente haya instalado un archivo dañado o con una firma incorrecta, o bien que sea software malintencionado de origen desconocido.

Solución

No se puede crear la máquina virtual instantánea porque el controlador de esta está firmado con un certificado digital protegido que no es compatible con Windows 2008 R2 hasta que aplique un parche de Microsoft.

Aplique el parche 3033929 de Microsoft e intente crear la máquina virtual instantánea de nuevo.

Se ha producido un error al iniciar una máquina virtual instantánea si el equipo de origen es un servidor de Active Directory de Windows 2008/2012/2016

Síntoma

Se ha producido un error al iniciar la máquina virtual instantánea si la máquina virtual es un servidor de Active Directory de Windows 2008.

Cuando el equipo de origen es un servidor de Active Directory de Windows que está realizando la tarea de máquina virtual instantánea, se produce un error al iniciar la máquina virtual instantánea y se muestra una pantalla con el siguiente mensaje:

DETENCIÓN: los servicios del directorio c00002e2 no podrán iniciarse a causa del error siguiente: no funciona el dispositivo adjunto al sistema. Estado del error: 0xc0000001.

Solución 1:

Si el hipervisor de destino es Hyper-V, agregue la siguiente clave de registro en el hipervisor de HyperV y, a continuación, active la tarea de máquina virtual instantánea.

Si el hipervisor de destino es ESX/Vcenter, agregue la siguiente clave de registro en el equipo proxy, que se utiliza para ejecutar la tarea de máquina virtual instantánea y, a continuación, active la tarea de máquina virtual instantánea.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\InstantVM
```

Tipo de registro: Valor de DWORD

Nombre: RenameADLog

Valor: 1

Limitaciones:

- Si la base de datos NTDS y las rutas del archivo de registro NTDS están en volúmenes diferentes, la solución anterior no es adecuada.
- A partir de ahora, la solución anterior solo es válida para el servidor de Active Directory de Windows 2008.

Solución 2:

Solucionar manualmente el problema iniciando sesión en la máquina virtual instantánea.

Siga estos pasos:

1. Encienda la máquina virtual instantánea.
2. MIentras se está encendiendo la máquina virtual, pulse la tecla F8 antes de que el sistema operativo empiece a cargarse y elija el modo **Restauración del servicio de directorio**.
3. Cambie el nombre de todos los archivos *.log en la carpeta *C:\Windows\NTDS*. Por ejemplo, cambie el nombre del archivo edb.log a edb.log.old.
4. Ejecute el comando:

   ```
   esentutl /p "C:\Windows\NTDS\ntds.dit"
   ```

5. Reinicie el sistema.

Nota: La solución anterior es válida para todas las versiones de servidores de Windows con Active Directory instalado.

Se ha producido un error al encender la máquina virtual después de restaurar Hyper-V

Síntoma

No se puede encender la máquina virtual después de restaurar la máquina virtual de Hyper-V. Se muestra el siguiente error:

Synthetic Ethernet Port (Instance ID …): Failed to Power on with Error 'Attempt to access invalid address.'

Solución

Este error se produce porque la dirección MAC de la máquina virtual restaurada está en conflicto con las máquinas virtuales existentes. Elimine el adaptador de la NIC de la máquina virtual restaurada y agregue manualmente uno nuevo para solucionar la incidencia y poder encendar la máquina virtual correctamente.

Error en la tarea de máquina virtual instantánea debido a un fallo del servicio NFS de Windows

Síntoma

Si se ha instalado el Agente de Arcserve UDP y Arcserve Backup en el servidor de recuperación de la máquina virtual instantánea, al crear una máquina virtual instantánea en el servidor VMware ESX(i), el servicio NFS de Windows no se inicia y se produce un error en la tarea de máquina virtual instantánea.

Solución

El motivo por el que el servicio NFS de Windows no se inicia es porque el número de puerto predeterminado de dicho servicio es 111 y este es el que utiliza el servicio **Servidor de llamada a procedimiento remoto** de Arcserve Backup.

Para resolver este problema, cambie el número de puerto predeterminado del servicio **Servidor de llamada a procedimiento remoto** de Arcserve Backup a otro puerto e intente volver a crear la máquina virtual instantánea. Para obtener más información sobre el cambio del puerto predeterminado, consulte Modificación del archivo de configuración de puertos y Puertos de comunicación del servidor primario y del servidor miembro en la documentación de Arcserve Backup.

No se puede acceder o suprimir la carpeta de archivos de la máquina virtual instantánea incluso con privilegios de administrador.

Síntoma

La carpeta de archivos de la máquina virtual instantánea no está accesible o no se puede suprimir debido al error Se requiere permiso de administrador incluso cuando el usuario ya tiene privilegios de administrador.

Solución

Es un problema de NFS. En primer lugar se debe eliminar el recurso compartido de NFS y, a continuación, se podrá suprimir la carpeta. Utilice el siguiente comando para suprimir la carpeta:

nfsshare /delete [nombre del recurso compartido de NFS]

Fallo de inicio de la máquina virtual instantánea en Hyper-V después de reiniciar el servidor de recuperación

Síntoma

Cuando se inicia la máquina virtual instantánea (IVM) y, a continuación, se reinicia el servidor de recuperación de Hyper-V, se produce un error al iniciarse la IVM.

Solución

Para resolver este error de arranque, reinicie la IVM.

Error al crear un almacén de datos de NFS de VMware y aparición del error No se puede determinar el nombre de host

Válido para VMware

Síntoma

Se produce un error en la creación de la máquina virtual instantánea y aparece el siguiente mensaje de error:

Error al crear el almacén de datos de NFS de VMware por parte del servidor <hostname of recovery server>.

Mensaje de error: Se ha producido un error durante la configuración del host.

Detalles: Error en la operación; informe de diagnóstico: No se puede determinar el nombre de host <un nombre de host, pero no un servidor de recuperación>.

Ejemplo

Error al crear el almacén de datos de NFS de VMware por parte del servidor 'host1'.

Mensaje de error: Se ha producido un error durante la configuración del host.

Detalles: Error en la operación; informe de diagnóstico: No se puede determinar el nombre de host 'host2'.

Solución

Este error se produce porque el servidor ESX enumera todos los almacenes de datos de NFS cuando se crea un almacén de datos de NFS de máquina virtual instantánea, incluso cuando algunos ya no están disponibles. Por ejemplo, el almacén de datos de NFS creado por **host2** sigue existiendo incluso si **host2** no está disponible porque se ha suprimido el equipo. Por tanto, el servidor ESX no puede determinar el nombre del host.

Para resolver este problema, suprima el almacén de datos no disponible en el servidor ESX.

Siga estos pasos:

1. Inicie sesión en el servidor ESX usando SSH.
2. Escriba el comando siguiente:

   ```
   esxcfg-nas -l
   ```

   El mismo error se muestra en la línea de comandos.

```
Se ha producido un error al realizar la operación: No
se puede determinar el nombre de host 'host2'.
```

3. Agregue una asignación en el archivo **/etc/hosts** del servidor ESX para solucionar este problema.

   <IP address> <hostname>

   Nota: La dirección IP debe ser accesible.

   Ejemplo: 10.57.X.X host2

4. Enumere todos los almacenes de datos de NFS usando el comando siguiente:

   ```
   esxcfg-nas –l
   ```

   ```
   arcserve_UDP_<hostname> es /arcserve_UDP_IVM_{ESX_gene-
   rated_number} desde <hostname> desmontado no dis-
   ponible
   ```

   Ejemplo: esxcfg-nas –l

   arcserve_UDP_host2 es /arcserve_UDP_IVM_{991555E6-09A4-4D80-A47E-522831A62Axx} desde host2 desmontado no disponible

5. Utilice el siguiente comando para suprimir el almacén de datos no disponible:

   ```
   esxcfg-nas -d arcserve_UDP_host2
   ```

6. Elimine la asignación de <hostname> en el archivo **/etc/hosts** desde el servidor ESX.

   Ahora podrá utilizar la función NFS de la manera habitual.

   Nota: Para obtener más información sobre esta incidencia, consulte el artículo de la base de conocimiento de VMware.

Se ha producido un error al implementar el servicio de integración en la máquina virtual invitada en Hyper-V

Síntoma

Al realizar copias de seguridad de una máquina virtual que tiene la aplicación (SQL o Exchange) instalada, el punto de recuperación no incluye la información del editor y el registro de actividad de la tarea de copia de seguridad muestra el mensaje de advertencia siguiente:

Se ha producido un error al implementar el servicio de integración para la máquina virtual.

Solución

Estos problemas suceden a menudo cuando el cortafuegos desactiva Windows Management Instrumentation (WMI) en la máquina virtual invitada. Para solucionar este problema, utilice los pasos siguientes:

1. Inicie sesión en la máquina virtual invitada.
2. Abra el Panel de control.
3. Abra Firewall de Windows.
4. Haga clic en Permitir una aplicación o una característica a través de Firewall de Windows.
5. Active Windows Management Instrumentation (WMI).
6. Haga clic en Aceptar.

Error en la máquina virtual instantánea de Linux en un servidor de Hyper-V en un idioma distinto al inglés

Se produce un error en la máquina virtual instantánea de Linux en un servidor Hyper-V en un idioma distinto al inglés debido a un problema de conexión incluso cuando se desactiva el cortafuegos.

Síntoma

Se produce un error en la creación de la máquina virtual instantánea y aparece el siguiente mensaje de error:

Se ha producido un error al conectar con el host de Hyper-V [nombre de servidor de Hyper-V de destino]. Asegúrese de que la dirección del host es correcta y las credenciales son válidas.

Solución

Este problema puede estar causado por una configuración incorrecta de la información de conexión del servidor de Hyper-V.

Para obtener más detalles, consulte **Configuración de la información de conexión al servidor Hyper-V para la máquina virtual instantánea** en la *Guía del usuario del Agente de Arcserve UDP para Linux*.

Consumo de una licencia adicional para rutas UNC que se encuentran en una máquina virtual de Hyper-V con licencia

Síntoma

Las rutas UNC que se encuentran en la máquina virtual en un hipervisor consumen una licencia de socket adicional incluso cuando la licencia ya se ha aplicado antes en el host del hipervisor. Este error da como resultado un consumo de licencias adicionales.

Solución

La copia de seguridad del host del hipervisor y las rutas UNC que se encuentran en el mismo hipervisor consumen la misma licencia. Sin embargo, al realizar la copia de seguridad de las rutas UNC que se encuentran en cualquier máquina virtual que está en el mismo hipervisor, las rutas UNC y los recursos compartidos consumirán una licencia adicional. Este problema solo ocurre si la máquina virtual no se ha agregado ni importado como un nodo a la Consola y también cuando se agregan rutas UNC con un nombre que no sea el nombre proporcionado mientras se agrega la máquina virtual a la Consola.

Siga estos pasos:

1. Agregue el nodo (la máquina virtual que tiene las rutas UNC) a la Consola y especifique los detalles del hipervisor para el nodo o importe el nodo desde el hipervisor.
2. Agregue las rutas UNC o los recursos compartidos con el mismo nombre que sea el que se ha agregado en el paso 1.

Se produce un error de licencia al cambiar la edición o el tipo de licencia y al crear una máquina virtual instantánea

Síntoma

Después de agregar o cambiar un tipo de licencia o edición en la Consola y de crear una máquina virtual instantánea sin ejecutar ninguna tarea de copia de seguridad, aparece un mensaje de error de error de licencia. Sin embargo, la próxima vez que ejecuta una máquina virtual instantánea, identificará correctamente la nueva licencia y se creará la máquina virtual instantánea.

Solución

Siga estos pasos:

1. Después de agregar una nueva licencia a la Consola de UDP para el plan existente, ejecute la tarea de copia de seguridad.
2. Ahora cree una máquina virtual instantánea.

Relacionados con el Agente de Linux

En esta sección se incluyen los siguientes temas de solución de problemas relacionados con el Agente de Arcserve UDP para Linux:

- Configuración de destino de la copia de seguridad desactivada al abrir la interfaz de usuario del Agente de Linux
- El estado de la tarea, el historial de tareas y el registro de actividades no son visibles

Configuración del destino de la copia de seguridad desactivada al abrir la interfaz de usuario del Agente de Linux

Si el Servidor de copia de seguridad de Linux no se elimina de la consola de Arcserve UDP antes de desinstalar la consola, la configuración del destino de la copia de seguridad se desactivará al abrir la interfaz de usuario del Servidor de copia de seguridad.

Síntoma

No se notifica al Servidor de copia de seguridad que la consola de Arcserve UDP no está instalada. El Servidor de copia de seguridad supone que todavía está gestionado por la consola.

Solución

Inicie sesión en el servidor de copia de seguridad de y ejecute el siguiente comando:

```
# /opt/Arcserve/d2dserver/bin/d2dreg --release
```

El Servidor de copia de seguridad se libera de la consola y ahora se pueden cambiar los valores de configuración de copia de seguridad desde la interfaz de usuario del Servidor de copia de seguridad.

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

El estado de la tarea, el historial de tareas y el registro de actividades no son visibles

Síntoma

No puedo ver el estado de tarea, el historial de tareas y el registro de actividades para los nodos de Linux en la Consola de Arcserve UDP.

Solución

El servidor de copia de seguridad de Linux no se puede conectar a Arcserve UDP mediante el nombre de host.

Siga estos pasos:

1. Cree el archivo server_ip.ini en la ubicación siguiente de Arcserve UDP:

   "Ruta de instalación de UDP"\Management\Configuration\server_ip.ini

2. Introduzca la dirección IP de Arcserve UDP en este archivo.
3. Inicie sesión en la Consola de Arcserve UDP y actualice el servidor de copia de seguridad de Linux y los nodos de Linux.

   Nota: El servidor de copia de seguridad de Linux solo se puede actualizar en Grupos del servidor de copia de seguridad de Linux, donde todos los servidores de copia de seguridad de Linux se clasifican.



El estado de la tarea, el historial de tareas y el registro de actividades son visibles

Se ha producido un error al restaurar el volumen del sistema de SUSE15 con el sistema de archivos XFS

Se ha producido un error al restaurar el volumen del sistema de SUSE15 con el sistema de archivos XFS.

Síntoma

Se ha producido un error al realizar la tarea de restauración del nodo de SUSE15 con el sistema de archivos XFS.

Solución

El problema se produce porque no se ha montado el volumen del sistema. Cree un CentOS 7.5 Live CD y utilice este Live CD para realizar la reconstrucción completa instantánea.

Si el problema persiste, utilice la opción Conversación en vivo para ponerse en contacto con Soporte de Arcserve. Permite optimizar la conversación entre el usuario y el equipo de Soporte técnico, lo que le permite abordar sus preocupaciones de manera inmediata teniendo, al mismo tiempo, acceso al producto.

Relacionados con la restauración

En esta sección se incluyen los siguientes temas de solución de problemas relacionados con la restauración:

- No se pueden restaurar los archivos
- Adición de la base de datos de contenido restaurado a la aplicación web original
- No se puede montar la base de datos mientras se restaura la base de datos de Microsoft Exchange
- El campo De no se muestra correctamente en los correos electrónicos enviados por aquellos usuarios que tengan permisos “en nombre de” en un buzón compartido
- Se produce un error en las tareas de restauración después las copias de seguridad de la integración sencilla

No se pueden restaurar los archivos

Síntoma

Debido a una limitación de Microsoft, los datos de archivos en los volúmenes de deduplicación de NTFS de un sistema Windows 2012 R2 no se pueden leer desde un sistema Windows 2012. Como resultado, si el Agente de UDP de un sistema Windows 2012 se está utilizando para restaurar una máquina virtual con el SO invitado Windows 2012 R2 y con volúmenes de deduplicación de NTFS, es posible que se produzca el siguiente problema. El problema ocurre solamente durante una operación de restauración del punto de recuperación a nivel de archivo o de montaje.

El archivo o directorio está corrupto y no se puede leer.

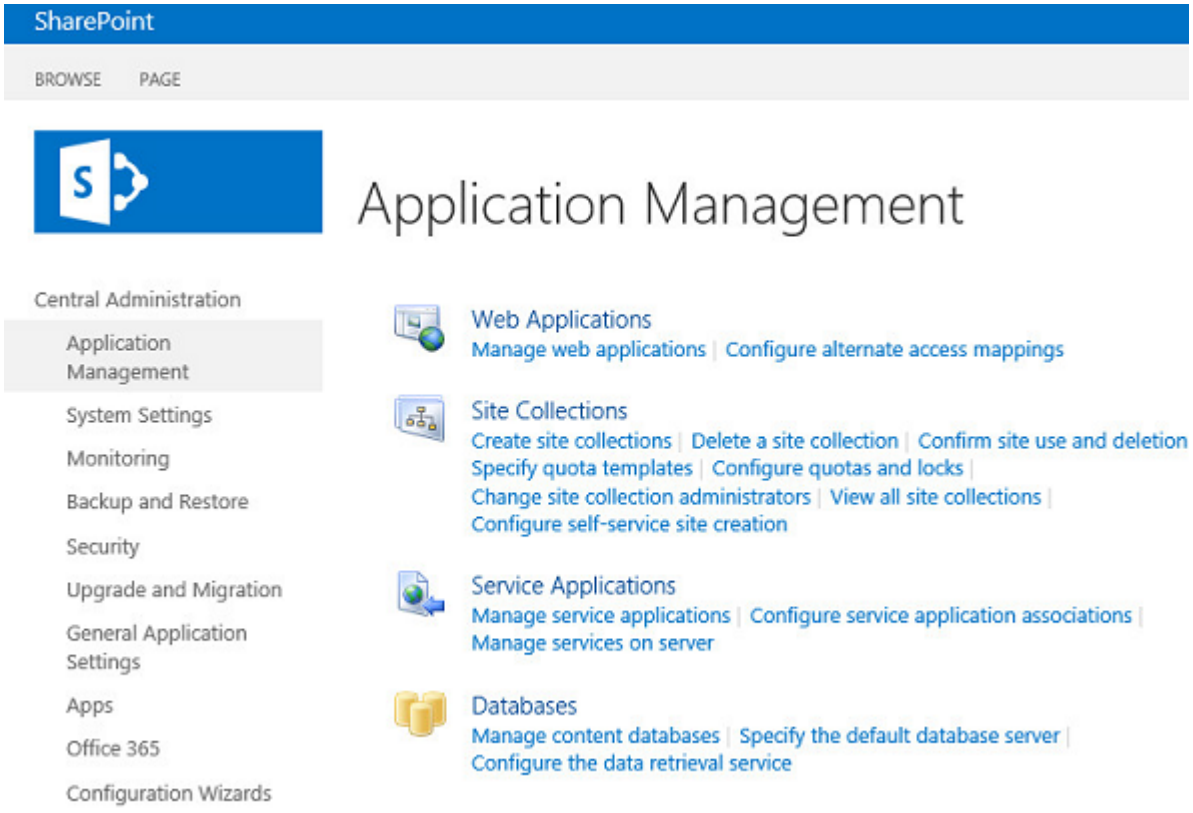
Solución

Cuando se produce este problema, inicie el proceso de restauración desde un Agente de UDP instalado en un sistema Windows 2012 R2.

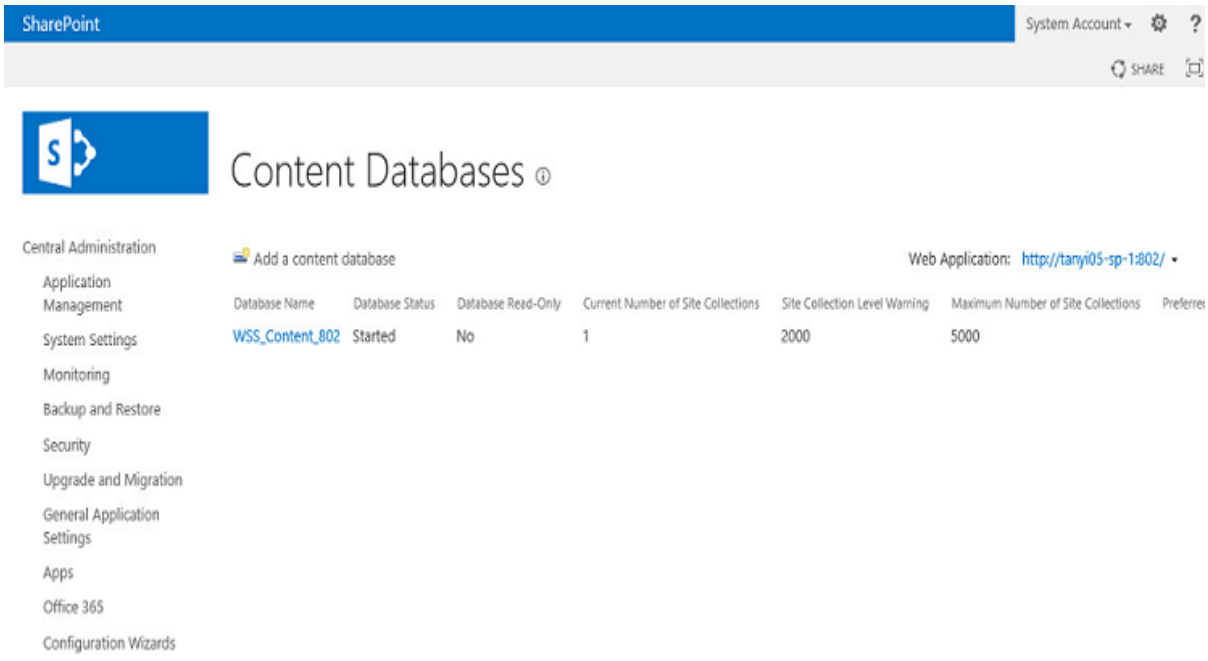
Adición de la base de datos de contenido restaurado a la aplicación web original

Siga estos pasos:

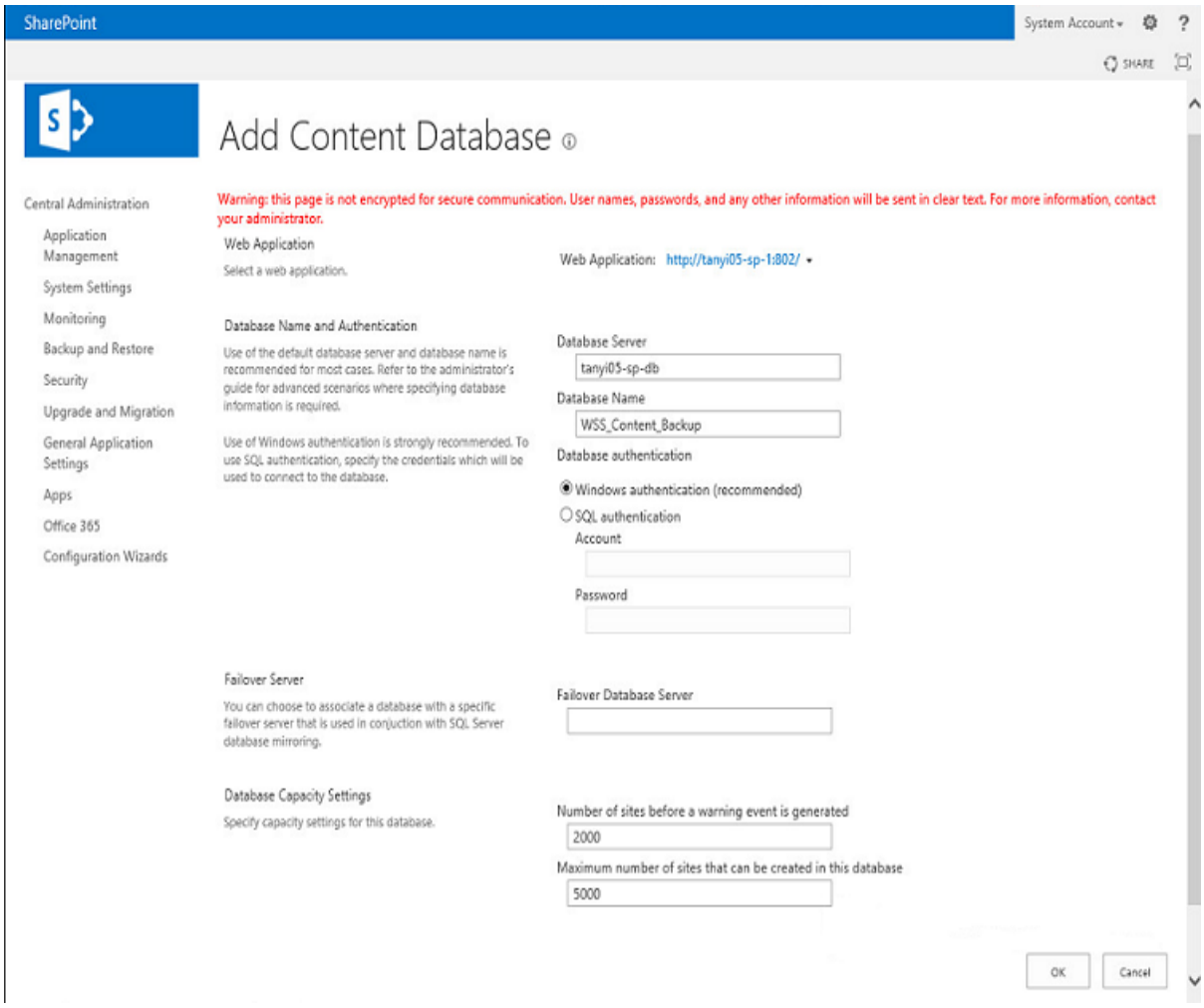
1. Abra la Administración central de SharePoint y seleccione Administración de aplicaciones.



2. Seleccione Administrar bases de datos de contenido.



3. Seleccione la aplicación web y haga clic en Agregar una base de datos de contenido.
4. Escriba el nombre y el servidor de la base de datos (por ejemplo, WSS_Content_ Backup) y haga clic en Aceptar.



La base de datos de contenido estará ahora asociada a su aplicación web original.

No se puede montar la base de datos mientras se restaura la base de datos de Microsoft Exchange

Síntoma

Al restaurar una base de datos de Microsoft Exchange, no es posible montar la base de datos. Faltan los registros necesarios o los registros de transacciones no son contiguos. Se producen errores de eventos como 454, 455 y 2006 en el registro de eventos.

Las dos razones siguientes pueden causar el error de montaje de la base de datos:

Razón 1: Se activará la opción Borrar definitivamente el registro de Exchange en los valores de configuración de UDP y esta opción suprime los registros de transacciones después de cada copia de seguridad. A continuación, el usuario intenta restaurar una sesión anterior después de que se produzcan varias operaciones de borrado definitivo del registro en la copia de seguridad.

Razón 2: Los usuarios han suprimido manualmente los registros de transacciones u otros programas han suprimido los registros como, por ejemplo, el software antivirus.

Solución

Solución 1: Si se ha activado la opción Borrar definitivamente el registro de Exchange y los registros de transacciones no son contiguos, restaure todas las sesiones de una en una empezando por la sesión más reciente y hasta que se produzca un error al restaurar una sesión. Si se produce un error al restaurar la última sesión, intente la solución 2.

Solución 2: Si la solución 1 no funciona, utilice la solución 2. Esta solución permite solucionar los dos problemas.

Por ejemplo, se desea restaurar la base de datos de prueba de la sesión 1. Los siguientes pasos utilizan Test (Prueba) como el nombre de la base de datos.

1. Inicie sesión en Exchange Server donde se encuentra la base de datos.
2. Suprima todos los archivos (como, por ejemplo, *.edb, *.log, *.jrs, *.chk) de la carpeta de la base de datos.
3. Monte la base de datos para crear una base de datos vacía.

   Mount-Database -Identity Test
4. Vuelva a restaurar la misma sesión en la ubicación original.

   Si la restauración se realiza correctamente, no es necesario realizar los siguientes pasos. Si se produce un error en la restauración, continúe con los siguientes pasos.

5. Monte la base de datos otra vez.

   Mount-Database -Identity Test

6. Cree una base de datos temporal.

   new-mailboxdatabase -name OtherDatabase

7. Mueva el buzón de correo a cualquier otra base de datos.

   get-mailbox -datatbase Test -resultsize unlimited | new-moverequest -targetdatabase OtherDatabse

8. Elimine la base de datos del buzón de correo del equipo de destino.

   remove-mailboxdatabase -identity Test

9. Cree una base de datos del buzón de correo con el mismo nombre.

   new-mailboxdatabase -name Test

10. Vuelva a restaurar la misma sesión en la ubicación original.

    La base de datos se ha montado correctamente.

El campo De no se muestra correctamente en los correos electrónicos enviados por aquellos usuarios que tengan permisos “en nombre de” en un buzón compartido

Síntoma

Al restaurar los correos de Exchange, si un usuario con privilegios "en nombre de" para un buzón de correo compartido envía el correo electrónico, la información del campo De no se muestra correctamente después de la restauración. El campo De solo muestra el nombre del <host remitente>.

Solución

Siga estos pasos para solucionar la incidencia:

1. Realice una de las acciones siguientes:

   Para la copia de seguridad sin agente

   - En el servidor proxy HBBU, cree un archivo grtcfg.ini en la carpeta Configuration:

     [ruta_instalación_producto]\Engine\Configuration

   Para la copia de seguridad basada en el agente

   - En el equipo de agente, cree un archivo grtcfg.ini en la carpeta Configuration:

     [ruta_instalación_producto]\Engine\Configuration

2. Agregue el siguiente contenido al archivo grtcfg.ini:

   [common]

   0xFF07_enable=1

3. Vuelva a enviar la tarea de restauración.

Se produce un error en las tareas de restauración después las copias de seguridad de la integración sencilla

Síntoma

Al enviar copias de seguridad de la integración sencilla desde el gestor de Arcserve Backup para realizar copias de seguridad del nodo de Exchange Online desde el servidor de puntos de recuperación, ya se ha realizado la copia de seguridad del nodo con la sesión de copia en cinta. Se produce un error en las tareas cuando los datos de origen incluyen sesiones de Arcserve D2D de las que se ha realizado la copia de seguridad previamente mediante Arcserve Backup. Aparecerá el mensaje de error AW0813 en el registro de actividades.

Solución

El comportamiento del diseño de Arcserve Backup es el responsable de este comportamiento. Se debe modificar este comportamiento para permitir a Arcserve Backup hacer copia de seguridad de las sesiones de Arcserve D2D de las que antes se ha realizado la copia de seguridad.

Siga estos pasos:

1. Desde el servidor de Arcserve D2D (nodo) del que está realizando la copia de seguridad, abra el editor del registro de Windows.
2. Abra la siguiente clave:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\ClientAgent\Parameters\AllowRedundantD2DBackups
3. Cambie el valor DWORD de AllowRedundantD2DBackups a 1.

   Nota: Si la clave de registro descrita anteriormente no está presente en el nodo del que está realizando la copia de seguridad, se deberá crear la clave.
4. Cierre el editor del Registro de Windows.

   Para obtener más detalles, consulte el artículo de la base de conocimiento.

La restauración a la carpeta compartida de NFS daña el nombre de archivo

Síntoma:

Cuando realizo la restauración a una carpeta compartida de NFS, los nombres de archivos o carpetas se restauran dañados.

Solución:

UDP no es compatible con la restauración de los archivos y carpetas en la carpeta compartida de NFS. Se recomienda exportar una carpeta compartida del bloque de mensajes del servidor (SMB) y, a continuación, restaurar a la misma carpeta.

Nota: Si el nombre de archivo o carpeta se daña durante la sesión de la copia de seguridad de NFS, incluso después de la restauración, el nombre de archivo o carpeta permanecerá dañado.

Relacionados con las puertas de enlace, los servidores de puntos de recuperación, los almacenes de datos, las consolas y las bases de datos

En esta sección se incluyen los siguientes temas de solución de problemas relacionados con el servidor de puntos de recuperación (RPS), el almacén de datos y la base de datos:

- El nombre del almacén de datos ya está en uso
- Error de conexión al almacén de datos debido a un problema de DNS
- El almacén de datos se cambia al modo de solo restauración
- Error cuando la versión del servidor de puntos de recuperación es inferior a la versión de la Consola
- No es posible agregar el mismo recurso en distintos sitios
- Cómo activar truncamientos del registro cuando la base de datos SQL está en modo de recuperación completa
- En la exploración de puntos de recuperación no se muestran los puntos de recuperación disponibles cuando el RPS está configurado con FQDN
- Acceso denegado al agregar el servidor de puntos de recuperación
- Error de cambio de la vista de UDP para el punto de recuperación
- Acceso denegado al agregar o actualizar nodos
- Error de apertura de la Consola de UDP tras el cambio de la contraseña del administrador de SQL
- Error al montar los puntos de recuperación debido al tiempo de espera
- Cómo actualizar las credenciales del servidor de la puerta de enlace
- Cómo actualizar la puerta de enlace cuando se cambian las credenciales del proxy de la puerta de enlace
- En la Consola se muestra el mensaje: Identity service is starting (El servicio de identidades se está iniciando)

El nombre del almacén de datos ya está en uso

Síntoma:

Cuando creo un almacén de datos, a veces aparece el siguiente mensaje incluso si especifico un nombre del almacén de datos nuevo:

Otro almacén de datos está utilizando ya este nombre en el servidor. Especifique un nombre del almacén de datos diferente.

Solución:

Esto sucede cuando se tiene un almacén de datos existente pero, por algún motivo, el UUID del almacén de datos en el registro está corrupto. Se puede suprimir el almacén de datos desde la interfaz gráfica de usuario, pero el nombre permanece en el registro del servidor de punto de recuperación.

Para solucionar este problema, especifique un nombre nuevo.

Error de conexión al almacén de datos debido a un problema de DNS

Síntoma:

Durante la reconstrucción completa, se produce un error al establecer la conexión con la carpeta compartida expuesta al Servidor de puntos de recuperación. A pesar de que el nombre de usuario y la contraseña son correctos, no se puede examinar el nodo en el Servidor de puntos de recuperación.

Solución:

Cuando se activa la función UAC de Windows en el Servidor de puntos de recuperación, incluso una cuenta que pertenezca al grupo de administradores locales no podrá acceder a una carpeta compartida del almacén de datos si la cuenta no tiene acceso a este recurso compartido de forma explícita.

Mediante el administrador integrado del Servidor de puntos de recuperación, conceda los privilegios de lectura y escritura a la cuenta utilizada en la reconstrucción completa para la carpeta compartida expuesta por el almacén de datos especificado.

El almacén de datos se cambia al modo de solo restauración

Síntoma

Me doy cuenta de que un almacén de datos se ha cambiado al modo de solo restauración y no me permite realizar la copia de seguridad de ningún dato.

Solución

Cuando un disco que está utilizando un almacén de datos se queda sin espacio en disco, el almacén de datos se cambia al modo de solo restauración. En este modo solo se puede realizar la restauración, pero no se puede realizar la copia de seguridad de los datos en el almacén de datos. O, también, cuando la adjudicación de memoria especificada se utiliza completamente, aumenta la adjudicación de memoria o cambia el almacén de datos de modo de memoria a modo de SSD. Incluso en tales casos, el almacén de datos cambia al modo Restaurar solo.

Para resolver estas incidencias, mueva el almacén de datos a un disco más grande importando el almacén de datos.

Primero copie las carpetas donde el disco está lleno a un disco más grande y con más espacio libre y, a continuación, importe el almacén de datos desde la Consola.

La función **Importar almacén de datos** le permite agregar un almacén de datos al servidor de punto de recuperación. Se puede importar cualquier almacén de datos existente a un servidor de punto de recuperación. Los almacenes de datos suprimidos anteriormente de un servidor de punto de recuperación están disponibles para ser importados.

Siga estos pasos:

1. En la consola, haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Servidores de punto de recuperación**.

   Se mostrará la página **Destinos: servidores de punto de recuperación**.
3. Realice una de las acciones siguientes:
   - Haga clic con el botón secundario del ratón en un servidor de punto de recuperación.
   - Seleccione un servidor de punto de recuperación y en el menú central haga clic en la lista desplegable **Acciones**.
4. Haga clic en **Importar almacén de datos**.

   Se muestra la página **Importación de un almacén de datos**.

5. Realice las acciones siguientes y haga clic en **Siguiente**:
   - Haga clic en **Examinar** para seleccionar la **Carpeta de destino de la copia de seguridad** desde donde se desea importar el almacén de datos.
   - Introduzca la **Contraseña de cifrado**.

   Nota: Déjelo vacío si el almacén de datos no está cifrado.

   Después de autenticar la **Carpeta de destino de la copia de seguridad**, la página **Importación de un almacén de datos** muestra los detalles del almacén de datos.
6. Modifique los detalles, si es necesario, y haga clic en **Guardar**.

   Si se ha copiado la carpeta Destino de los datos, Destino del índice y Destino de hash para el almacén de datos de deduplicación, cambie la ruta de la carpeta.

   Nota: No se puede activar o desactivar la opción de cifrado para un almacén de datos existente.

   El almacén de datos se agrega al servidor de punto de recuperación y se muestra en el cuadro de diálogo **Destinos: Servidores de puntos de recuperación**.

   Ahora el almacén de datos está disponible para las copias de seguridad.

Error cuando la versión del servidor de puntos de recuperación es inferior a la versión de la Consola

Síntoma

Hay un plan con una tarea de copia de seguridad o de replicación, y el destino es el servidor de puntos de recuperación. El servidor de puntos de recuperación es de una versión anterior, mientras que la Consola está actualizada a la última versión. Cuando creo, modifico, vuelvo a implementar, pauso o reanudo un plan, y hay una o más versiones anteriores del servidor de puntos de recuperación, aparece el siguiente error:

La versión del servidor de puntos de recuperación de destino 'rps1' es inferior a la versión de la Consola actual. Para continuar, se debe actualizar el servidor de puntos de recuperación.

Solución

Este error se produce cuando el plan utiliza una versión anterior del servidor de puntos de recuperación. Para resolver este error, actualice el servidor de puntos de recuperación que se utiliza en el plan. Si actualiza el servidor de puntos de recuperación manualmente (fuera de la Consola), no olvide actualizar el servidor de puntos de recuperación en la Consola.

Actualice el servidor de puntos de recuperación en el siguiente orden de preferencia:

Replicar a un servidor de puntos de recuperación remoto (RPS3) > Replicar la tarea (RPS2) > Tarea de copia de seguridad (RPS1)

Primero, actualice RPS3 y, a continuación, RPS2. Por último, actualice RPS1.

Siga estos pasos para llevar a cabo la actualización:

1. Desde la ficha **recursos**, diríjase a la página Destinos: Servidores de punto de recuperación.
2. Seleccione el servidor de punto de recuperación.
3. Haga clic con el botón secundario del ratón y seleccione **Instalar o actualizar el servidor de punto de recuperación**.
4. Haga clic en **Aceptar**.

Siga estos pasos para actualizar:

1. En la ficha **recursos**, vaya a Destinos, en el panel izquierdo, y haga clic en Servidores de punto de recuperación.
2. Seleccione el servidor de punto de recuperación.

3. Haga clic con el botón secundario del ratón y seleccione **Actualizar**.
4. Haga clic en **Aceptar**.

No es posible agregar el mismo recurso en distintos sitios

Síntoma

Cuando agrego un almacén de datos en un sitio remoto, me aparece el siguiente mensaje de error:

No se puede enviar la tarea para una máquina virtual de Hyper-V o de ESX

Solución

El error se produce porque el mismo recurso (nodo, servidor de puntos de recuperación, servidor ASBU, servidor Hyper-V, servidor de ESX y servidor proxy) ya está presente en otro sitio. Para solucionar este error, suprima el recurso de todos los sitios y agréguelo solo en uno.

Cómo activar truncamientos del registro cuando la base de datos SQL está en modo de recuperación completa

Síntoma

Cuando la base de datos está en el modo completo y se realiza una copia de seguridad completa de la base de datos, no se puede truncar el registro de truncamiento de SQL.

Solución

Para solucionar este problema, agregue dos valores de registro para permitir que Arcserve UDP pueda ejecutar el comando BACKUP LOG para realizar la copia de seguridad del registro de transacciones. Este comando marca como reutilizable el espacio que ya se ha escrito en el archivo de la base de datos.

Siga estos pasos para agregar el valor del registro:

1. Abra el editor de tablas de registro en el equipo del agente mediante el comando siguiente:

   ```
   regedit
   ```

2. Vaya a las claves siguientes dependiendo de si la copia de seguridad es basada en el agente o sin agente:

   Para la copia de seguridad basada en el agente para sistemas operativos de 32 bits y 64 bits, vaya a la clave siguiente en el equipo del agente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Si se utiliza una versión anterior a Arcserve UDP v6.5 Actualización 2, para la copia de seguridad sin agente vaya a la siguiente clave. Cree el valor de la tabla de registro en la máquina virtual de la que se desea realizar una copia de seguridad en el servidor proxy. Si la clave de la tabla del registro no está disponible, cree la ruta completa de la clave.

   - **Sistema operativo de 32 bits:**

     HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   - **Sistema operativo de 64 bits:**

     HKEY_LOCAL_MACHINE\SOFTWARE\WoW6432Node\Arcserve\Unified Data Protection\Engine\AFBackupDll

3. Cree los siguientes dos valores de registro y establezca sus valores en 1:

- valor de DWORD llamado BackupSQLLog4Purge
- valor de DWORD llamado ForceShrinkSQLLog

  Se agrega el valor del registro.

La solución se aplicará cuando se produzca la siguiente tarea de borrado definitivo.

En la exploración de puntos de recuperación no se muestran los puntos de recuperación disponibles cuando el RPS está configurado con FQDN

Válido en el sistema operativo de Windows

Síntoma

Cuando el servidor de puntos de recuperación no está en un dominio en el que configura el FQDN (agregando el sufijo DNS) en la Consola de UDP, Explorar puntos de recuperación no muestra un resultado preciso. Aunque se realice una copia de seguridad de algunas sesiones en el servidor de puntos de recuperación, el número de puntos de recuperación se muestra como cero.

Esto se debe a que, cuando el servidor de puntos de recuperación no se encuentra en un dominio, el servidor de puntos de recuperación no se puede detectar usando el FQDN.

Solución

Para solucionar este problema, agregue el sufijo DNS en el host del servidor de puntos de recuperación.

Siga estos pasos:

1. Abra el panel de control y vaya a **Sistema y seguridad**, **Sistemas**.
2. Haga clic en **Change settings (Cambiar configuración)** para los ajustes de grupo de trabajo, dominio y nombre de equipo.

   Se abrirá el cuadro de diálogo Propiedades del sistema.
3. En la ficha **Nombre del equipo**, haga clic en **Cambios**.

   Se abrirá el cuadro de diálogo **Nombre del equipo/cambios del dominio**.
4. Haga clic en **Más**.

   Se abrirá el cuadro de diálogo **Sufijo DNS y nombre del equipo NetBIOS**.
5. En el sufijo DNS primario de este campo de equipo, agregue el sufijo DNS de la red y haga clic en **Aceptar**.

   Por ejemplo, agregue ABC.com.
6. Reinicie el sistema.

Acceso denegado al agregar el servidor de puntos de recuperación

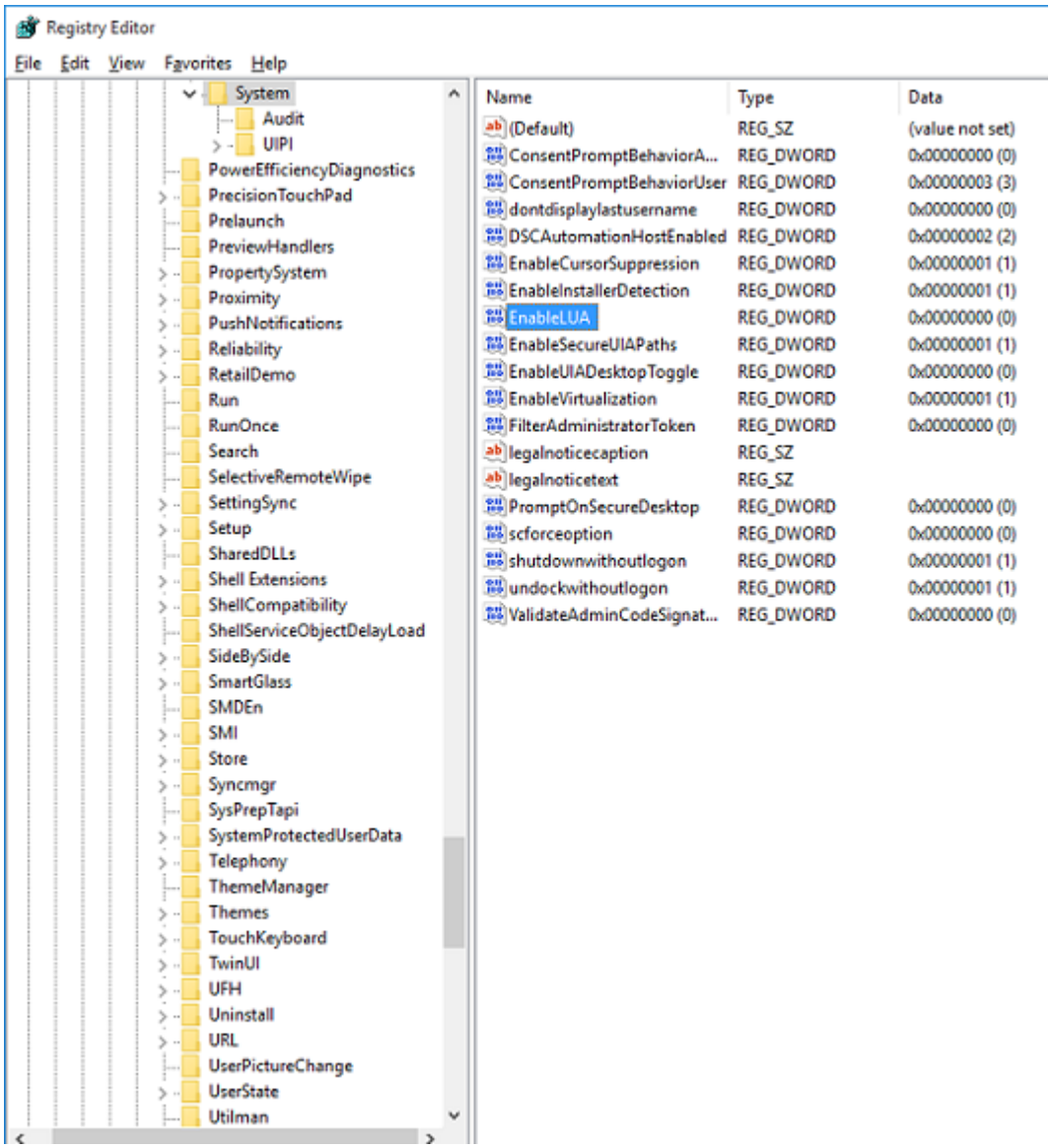
Síntoma:

Si se agrega Windows 10 como servidor de puntos de recuperación, aparecerá un mensaje de error incluso cuando no se está ejecutando el Control de cuentas de usuario:

Acceso denegado. Es posible que la cuenta no disponga de privilegios de administrador o que se trate de una cuenta de administrador no integrada, y que el UAC esté activado.

Solución:

Para Windows 10, para desactivar el Control de cuentas de usuario, modifique el valor de la clave de registro, no solo cambiando el nivel a "No notificarme nunca" en el Panel de control, pero también siguiendo el diagrama de registro que se muestra a continuación.



Establezca el registro "EnableLUA" en 0 para desactivar el Control de cuentas de usuario completamente y reinicie el equipo.

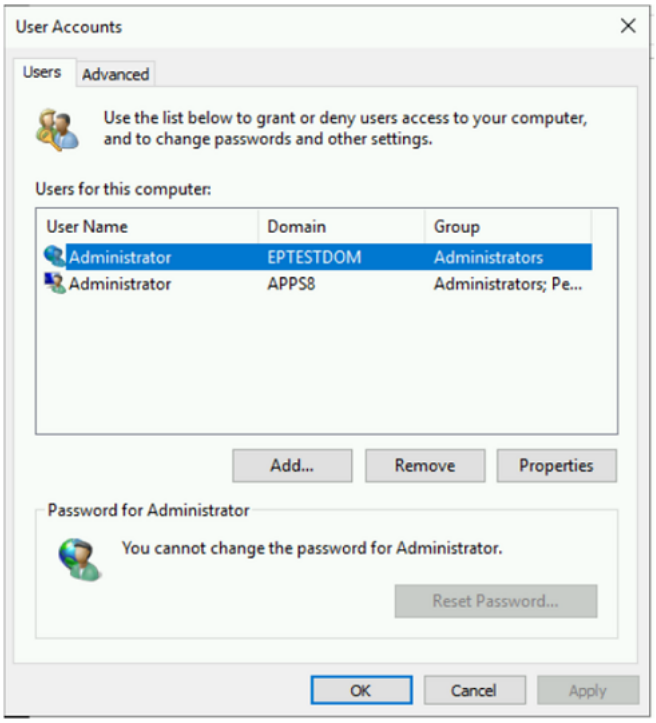
A continuación, agregue Windows 10 como servidor de puntos de recuperación en la consola.

Asignación de roles y privilegios de administrador a un usuario del dominio

Esta sección proporciona información sobre cómo asignar privilegios y roles de administrador a un usuario del dominio.

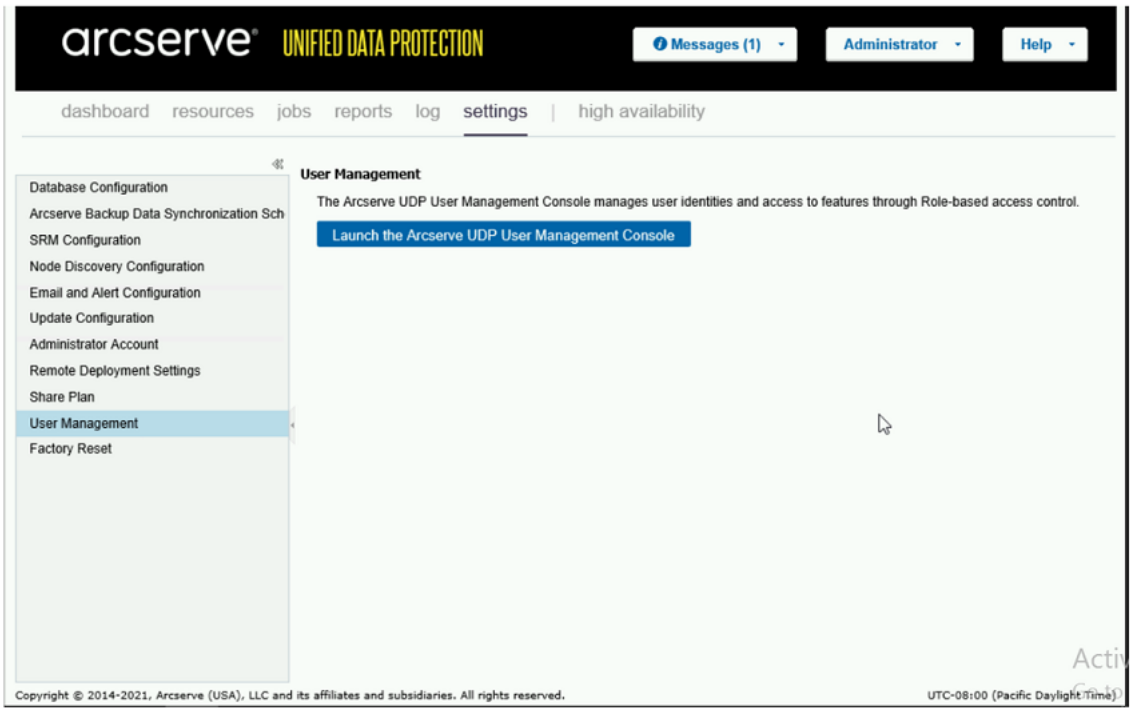
Siga estos pasos:

1. Para configurar el equipo de la Consola de UDP para el dominio, utilice las credenciales de inicio de sesión del administrador.
2. Asegúrese de que el usuario del dominio forme parte del grupo de administradores. Para agregar un usuario al grupo de administradores, en la ventana Cuentas de usuario, haga clic en el botón **Agregar**.



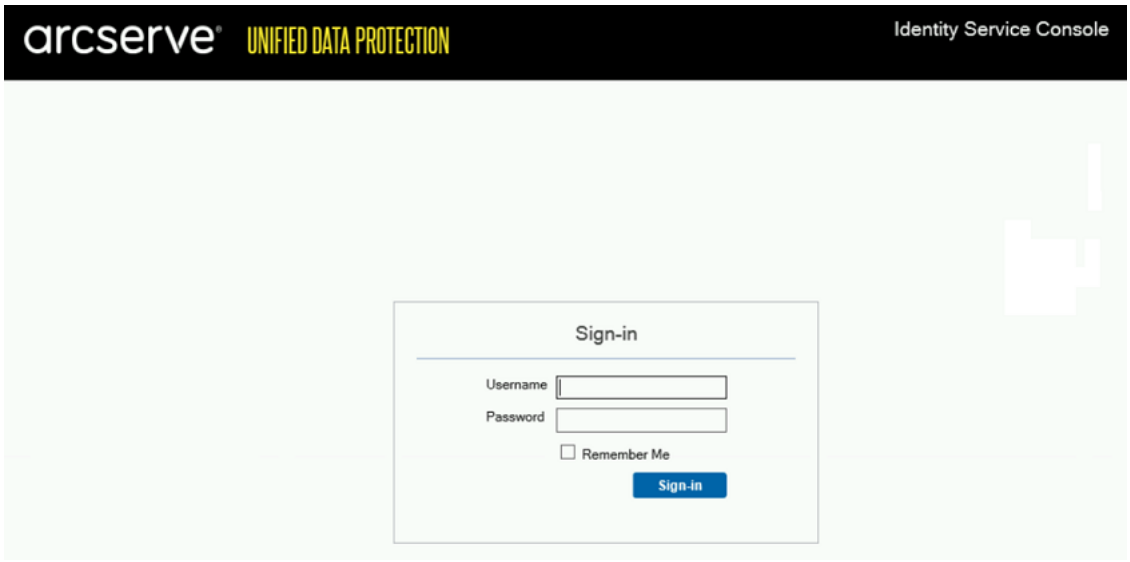
3. Después de agregar el usuario al grupo de administradores, reinicie el servicio de gestión.
4. Para agregar el rol de administrador a un usuario del dominio utilizando la Consola de gestión de usuarios de Arcserve UDP, haga lo siguiente:
    a. Inicie sesión en la Consola de Arcserve UDP con las credenciales del administrador.
    b. Haga clic en la ficha **Configuración**.
    c. En el panel izquierdo, haga clic en **Gestión de usuarios**.

    Se abre la página Gestión de usuarios.



d. Haga clic en el botón **Iniciar la Consola de gestión de usuarios de Arcserve UDP**.

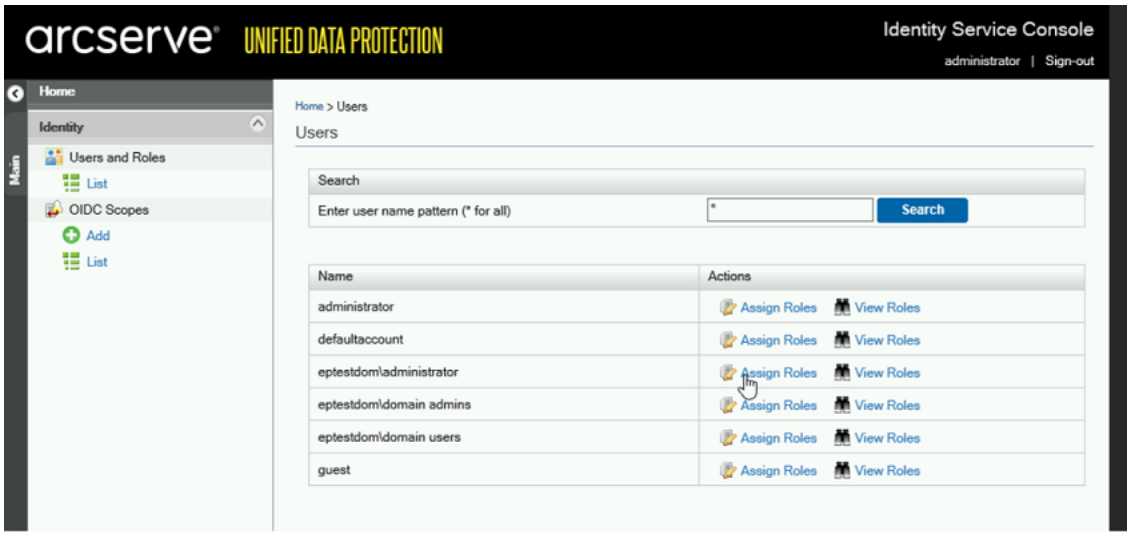
   La Consola de servicio de identidad se abre en una ventana nueva.



e. Proporcione las credenciales del administrador, como el nombre de usuario y la contraseña, y, a continuación, haga clic en **Iniciar sesión**.

   Se abre la página principal de la Consola de servicio de identidad.

f. Vaya a la página **Usuarios** y, a continuación, seleccione un usuario en la lista y haga clic en **Asignar roles** para aplicar permisos de administrador.



g. Inicie sesión en la Consola de UDP utilizando las credenciales del dominio.

Error de cambio de la vista de UDP para el punto de recuperación

Síntoma:

Al cambiar la vista a la vista de UDP para el punto de recuperación del Servidor de puntos de recuperación, a veces se reciben mensajes de error; por ejemplo, un mensaje de error de acceso denegado.

Solución:

Desactive la función UAC para solucionar el problema. Para obtener más información, consulte Cómo desactivar un UAC remoto para un administrador no integrado.

Acceso denegado al agregar o actualizar nodos

Válido en el sistema operativo de Windows

Síntoma

A veces, cuando se agregan o actualizan nodos, se obtiene el error siguiente:

Acceso denegado. Es posible que la cuenta no disponga de privilegios de administrador o que se trate de una cuenta de administrador no integrada, y que el UAC esté activado.

Solución

El segundo error se produce en los siguientes escenarios:

- Ha iniciado sesión como un usuario local o de dominio, que no está en el grupo de administradores locales del nodo para agregarlo o actualizarlo.
- Ha iniciado sesión como un usuario que está en el grupo de administradores locales del nodo, pero dispone de una cuenta de administrador no integrada del nodo para agregarlo o actualizarlo.

Para resolver esta incidencia, siga estos pasos:

1. Agregue el usuario local o de dominio al grupo de administradores locales de ese nodo.
2. Desactive el UAC de ese nodo.

   Siga estos pasos para desactivar el UAC:

   a. Haga clic en Inicio, escriba regedit en el campo Buscar programas y archivos y, a continuación, pulse Intro.

   b. Se abre el Editor del registro de Windows.

      Nota: Puede ser necesario proporcionar credenciales administrativas para poder abrir el Editor del registro de Windows.

   c. Busque y haga clic en la clave de registro siguiente:

      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

   d. En el menú Editar, haga clic en Nuevo y luego en Valor de DWORD (32 bits).

   e. Especifique LocalAccountTokenFilterPolicy como el nombre de la nueva entrada y, a continuación, pulse Intro.

   f. Haga clic con el botón secundario del ratón en LocalAccountTokenFilterPolicy y, a continuación, haga clic en Modificar.

g. Especifique 1 en el campo de datos Valores y, a continuación, haga clic en Aceptar.

h. Salga del Editor del registro.

Notas:

- Este procedimiento no es similar a la desactivación del UAC. Mediante este procedimiento, se pueden desactivar algunas de las funciones del UAC.
- Teniendo en cuenta que se utiliza la tecnología del servicio remoto Instrumental de administración de Windows (WMI) para importar, asegúrese de que el cortafuegos no bloquea el WMI.

Para obtener más información sobre el comportamiento de Windows, consulte la documentación de Microsoft.

Error de apertura de la Consola de UDP tras el cambio de la contraseña del administrador de SQL

Síntoma:

La Consola de Arcserve UDP utiliza SQL Server como base de datos y utiliza el administrador de SQL "sa" para conectarse a la base de datos. Si se cambia la contraseña de "sa", se produce un error al abrir la página principal de la Consola y se muestra el mensaje siguiente:

SQL Server no está disponible actualmente. Verifique el estado del servicio y, a continuación, reinicie el servicio de gestión de Arcserve UDP.

Solución:

1. Ejecute <homedir>\Management\BIN\DBAccountUpdate.bat.
2. Escriba updatePassword.
3. Escriba la nueva contraseña y pulse Intro.

Error al montar los puntos de recuperación debido al tiempo de espera

Síntoma

Cuando el servidor de puntos de recuperación tiene una gran carga, el sistema operativo tarda más tiempo en adjuntar el volumen montado y se produce un error en el montaje de puntos de recuperación. Aparece el siguiente mensaje en los registros de actividades:

El montaje del volumen tarda más tiempo del esperado (2 minutos). Esto puede ocurrir cuando el servidor afronta una carga de trabajo inesperada. Inténtelo de nuevo cuando la carga del servidor sea inferior o compruebe la sección de solución de problemas de la documentación en línea para aumentar el valor del tiempo de espera.

Solución

Para resolver esta incidencia, aumente el valor del tiempo de espera.

Siga estos pasos:

1. Inicie sesión en el servidor de puntos de recuperación y vaya a la siguiente ubicación:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFStorHBAMgmt
   ```

   ```
   "WaitDeviceReadyTimeoutS"=dword:00000078
   ```

   Predeterminado: 120 segundos

2. Cambie el valor del tiempo de espera a un número más alto.

   Por ejemplo, cambie el valor del tiempo de espera a 600 segundos (10 minutos).

Cómo actualizar las credenciales del servidor de la puerta de enlace

Síntoma

Si se cambia el nombre de usuario de la instalación de la puerta de enlace o se caduca la contraseña, aparece el siguiente error durante la implementación del plan:

Agent deployment failed (Error al implementar el Agente).

Se ha producido un error al suplantar al usuario que instaló la Arcserve Remote Management Gateway mediante las credenciales almacenadas. Compruebe si las credenciales aún son válidas y vuelva a implementarlo.

Solución

Para solucionar esta incidencia, actualice el nombre de usuario o la contraseña de la cuenta de la puerta de enlace.

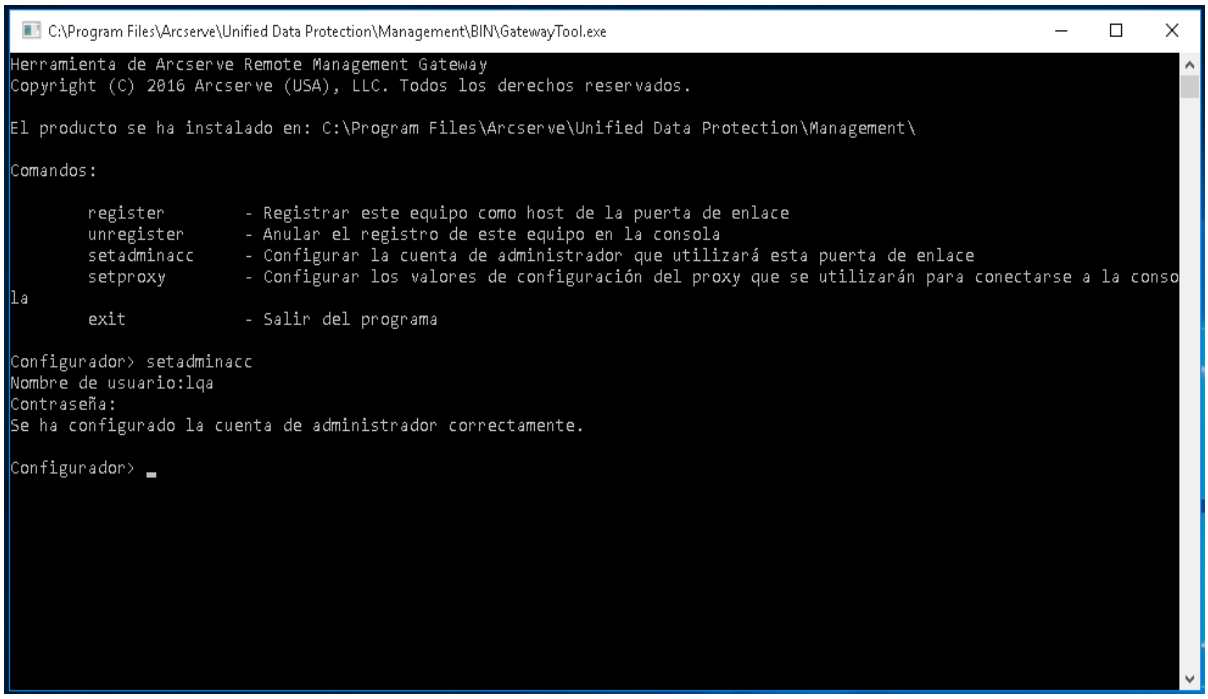
Siga estos pasos:

1. Inicie sesión en el servidor de la puerta de enlace.
2. Vaya a la carpeta BIN en la carpeta de instalación de Arcserve UDP.

   Por ejemplo, C:\Archivos de programa\Arcserve\Unified Data Protection\Management\BIN\GatewayTool.exe
3. Haga clic con el botón secundario del ratón en GatewayTool.exe y seleccione Ejecutar como administrador.
4. En la ventana de símbolo del sistema, escriba **setadminacc**.
5. Especifique el nuevo nombre de usuario.
6. Especifique la nueva contraseña.

   Si todos los detalles son correctos, verá el mensaje siguiente:

   ```
   Se ha configurado la cuenta de administrador correctamente.
   ```



7. Vuelva a implementar el plan.

Cómo actualizar la puerta de enlace cuando se cambian las credenciales del proxy de la puerta de enlace

Síntoma

Cuando se cambian las credenciales del servidor proxy, se interrumpe la conexión con la puerta de enlace. Se obtiene el siguiente mensaje de error al intentar conectarse a la puerta de enlace:

No se puede contactar con la puerta de enlace del sitio proxy. Compruebe el estado del sitio y asegúrese de que la puerta de enlace esté en ejecución.

Solución

Para solucionar esta incidencia, actualice los parámetros en el servicio setproxy GatewayTool.exe.

Siga estos pasos para actualizar el servidor de la puerta de enlace:

1. Inicie sesión en el servidor de puerta de enlace.
2. Vaya a la carpeta BIN en la carpeta de instalación de Arcserve UDP.

   Por ejemplo, C:\Archivos de programa\Arcserve\Unified Data Protection\Management\BIN\GatewayTool.exe
3. Haga clic con el botón secundario del ratón en GatewayTool.exe y seleccione Ejecutar como administrador.
4. En la ventana de símbolo del sistema, escriba **setproxy**.
5. Escriba **2** para seleccionar un proxy personalizado, ya que el proxy de IE no admite las credenciales actualmente.
6. Especifique la dirección IP del servidor proxy.
7. Especifique el puerto del servidor proxy.
8. Escriba **Y** para la autenticación.

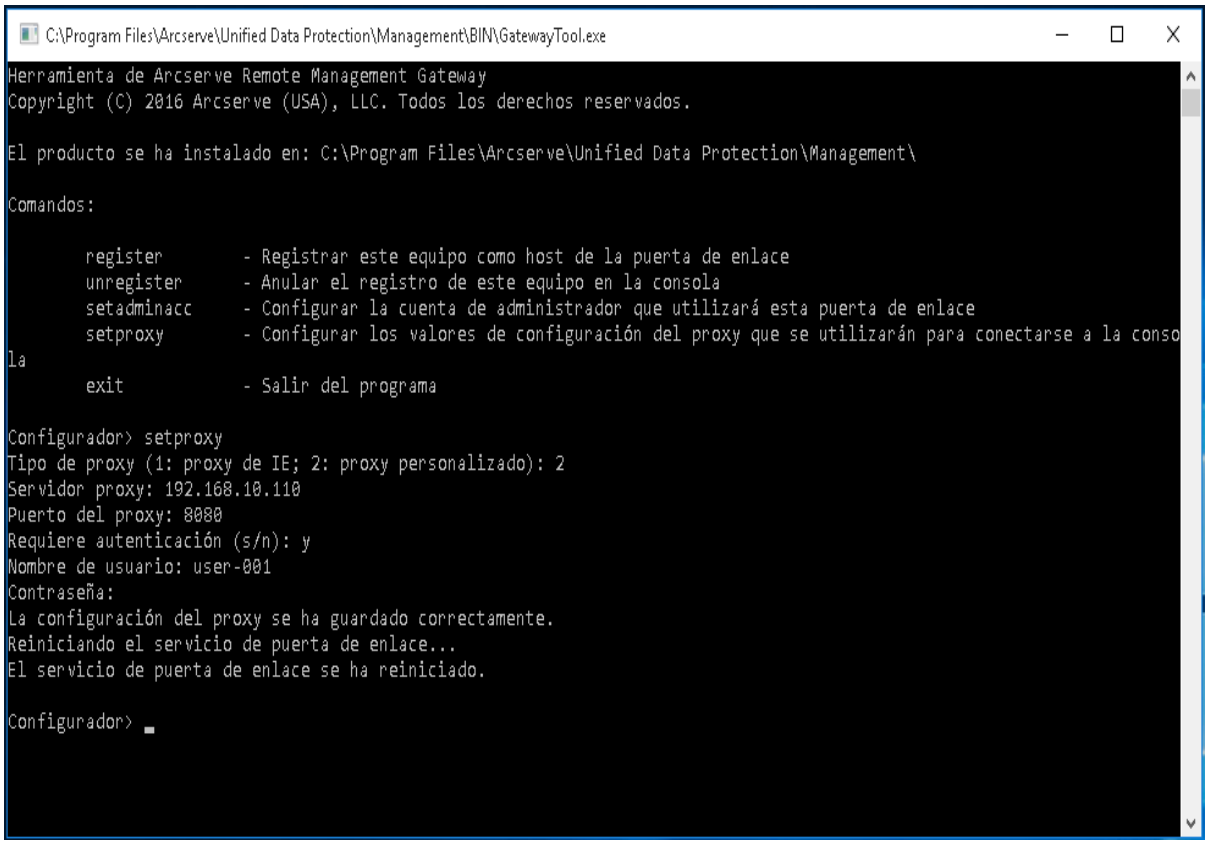
   Nota: Si escribe N, se desactivarán las credenciales.
9. Especifique el nuevo nombre de usuario.
10. Especifique la nueva contraseña.

    Si todos los detalles son correctos, verá el mensaje siguiente:

```
La configuración del proxy se ha guardado correc-
tamente. Reiniciando el servicio de puerta de
enlace...
```

Nota: Si las credenciales de proxy de la puerta de enlace están activadas en un plan, actualice el nombre de usuario y la contraseña del proxy en ese plan.

Asimismo, puede cambiar otras opciones de configuración, como Tipo de proxy, Dirección IP y Número de puerto en **setproxy**.



Si se observa el mensaje **Se ha producido un error al reiniciar el servicio de puerta de enlace; reinícielo manualmente** en la ventana del símbolo del sistema, siga estos pasos:

a. Ejecute **services.msc** para buscar **Arcserve remote management gateway service (Servicio de puerta de enlace de gestión remota de Arcserve)** y, a continuación, reinicie el servicio de puerta de enlace de gestión remota.

b. Si se detiene el servicio remoto después de reiniciar, utilice el Gestor de tareas para finalizar la tarea **tomcat8.exe** manualmente.

c. Actualice **services.msc** y reinicie **Arcserve remote management gateway service (Servicio de puerta de enlace de gestión remota de Arcserve)**.

En la Consola se muestra el mensaje: Identity service is starting (El servicio de identidades se está iniciando)

Síntoma

No se puede iniciar sesión en la Consola de Arcserve UDP. En la Consola se muestran los siguientes mensajes cinco minutos después de haber iniciado sesión:

Identity Service is starting (El servicio de identidades se está iniciando)

Solución

Para resolver este problema, abra la consola de servicio de Windows y reinicie el servicio de la Consola de Arcserve UDP y el **servicio de gestión de Arcserve UDP**.

Relacionados con la restauración y la copia de seguridad de la máquina virtual

En esta sección se incluyen los siguientes temas de solución de problemas relacionados con el servidor de puntos de recuperación (RPS), el almacén de datos y la base de datos:

- Adición de permisos para VDDK en el nivel del servidor de vCenter
- La tarea de copia de seguridad para la plantilla de máquina virtual siempre se convierte en copia de seguridad completa
- La tarea de copia de seguridad de la plantilla de máquina virtual omite los discos independientes
- Se produce un error en la tarea de copia de seguridad de la máquina virtual en el recurso compartido de SMB 3.0 con un mensaje de error
- Se produce un error en la tarea de recuperación de la máquina virtual al restaurar la máquina virtual en un recurso compartido predeterminado de archivos de Windows
- La información del volumen no está disponible para el punto de recuperación
- Permisos para la copia de seguridad sin agente basada en el host y Virtual Standby a nivel del servidor de vCenter
- Conversión de las copias de seguridad incrementales en copias de seguridad de verificación porque la instantánea de la máquina virtual se ha modificado desde la última tarea de copia de seguridad o requiere una consolidación
- Se ha producido un error en la copia de seguridad sin agente para la máquina virtual de VMware para el dispositivo de CD/DVD de la máquina virtual
- Error en la copia de seguridad basada en host sin agente de Hyper-V después de actualizar Arcserve UDP
- Error en la copia de seguridad sin agente basada en host en VMware ESXi 6.0
- Error al crear una instantánea para las máquinas virtuales de Hyper-V cuando se están ejecutando varias tareas
- Se ha producido un error al realizar la copia de seguridad de un disco virtual. Error del sistema=[El sistema no está preparado(21)]
- Error en la tarea de copia de seguridad
- Se produce un error al importar máquinas virtuales de VMware desde vCenter

- No se pueden aplicar valores de configuración de la copia de seguridad al nodo
- Se produce un error en las copias de seguridad debido a la licencia de ESXi
- La copia de seguridad sin agente basada en host no utiliza el modo de transporte HotAdd
- El modo de transporte HotAdd no funciona cuando se intenta realizar la copia de seguridad de una máquina virtual de VMware
- La tarea de copia de seguridad o restauración sin agente basada en host utiliza el modo de transporte NBD o NBDSSL incluso cuando se puede usar el modo SAN
- Control más detallado de VSS sobre las desactivaciones del sistema operativo invitado de Windows
- Error en las operaciones de recuperación al recuperar datos mediante el modo de transporte HotAdd o SAN
- Error de recuperación de la máquina virtual al especificar un puerto no predeterminado
- Error en la tarea de copia de seguridad incremental programada o completa para la máquina virtual de Hyper-V
- Error en el editor VSS de NTDS de Hyper-V al tomar la instantánea VSS en la máquina virtual
- No se conservan los cambios de la dirección de MAC después de la recuperación de máquinas virtuales
- Error en Hyper-V al crear una instantánea VSS
- No se pueden abrir archivos VMDK.
- Problemas causados por duplicados UUID de la máquina virtual duplicados
- Error en la tarea de catálogo del sistema de archivos o error en la comprobación del punto de recuperación para la copia de seguridad sin agente basada en host
- Conversión de la copia de seguridad incremental en copia de seguridad de verificación o incremento del tamaño de copia de seguridad en Hyper-V
- Error en la copia de seguridad sin agente basada en host para la máquina virtual de Hyper-V que tiene una configuración especial de discos diferentes
- Error en la tarea de copia de seguridad para una máquina virtual de VMware

- Desactivación de la nueva exploración de los adaptadores de bus de host cuando el origen y el proxy son distintos en los servidores VMware ESX
- Desactivación de la creación de instantáneas consecutivas en máquinas virtuales de VMware para una copia de seguridad
- La copia de seguridad basada en host sin agente se bloquea cuando se utiliza Windows 2003 R2 de 64 bits como servidor proxy de la copia de seguridad
- Cuando se restaura desde una versión superior del host de ESXi a un host de ESXi con una versión inferior, la máquina virtual se bloquea en la fase de arranque
- La utilización de la memoria RAM alcanza el 99 % cuando las tareas de copia de seguridad se envían a la máquina virtual
- Se produce un error en la tarea de restauración de Hyper-V, no se puede conectar a la utilidad del host
- Se produce un error en la protección automática al detectar y proteger la máquina virtual
- Establecimiento del tamaño de bloque de lectura cuando se realiza la copia de seguridad de un archivo VMDK

Adición de permisos para VDDK en el nivel del servidor de vCenter

Si no se tienen los permisos adecuados, se producirá un error en la tarea de copia de seguridad para maquinas virtuales basadas en el host y la tarea en espera virtual.

Para evitar esta incidencia, verifique que se tienen los permisos adecuados. Los usuarios de vCenter, no necesitan un permiso de administrador en el nivel del servidor de vCenter, pero deben contar con un permiso de administrador en nivel del centro de datos. Además, se deben tener los siguientes permisos a nivel del servidor de vCenter:

- Global, DisableMethods y EnableMethods
- Global, licencia

Para obtener más información, consulte el artículo de la base de conocimiento de VMware.

Para obtener más información sobre el permiso, consulte Permisos para la copia de seguridad sin agente basada en host y Virtual Standby en el nivel del servidor de vCenter.

Permisos para la copia de seguridad sin agente basada en el host y Virtual Standby a nivel del servidor de vCenter

Cuando se configura vCenter para gestionar máquinas virtuales, por lo general, se tendrán que configurar usuarios o grupos con privilegios de administrador de vCenter. Este enfoque ayuda a garantizar que las cuentas de vCenter dispongan de acceso sin límites a la funcionalidad y a las tareas de vCenter. Opcionalmente, se pueden crear usuarios y grupos de vCenter que se pueden utilizar para facilitar solamente operaciones de copia de seguridad o solamente operaciones de copia de seguridad y restauración.

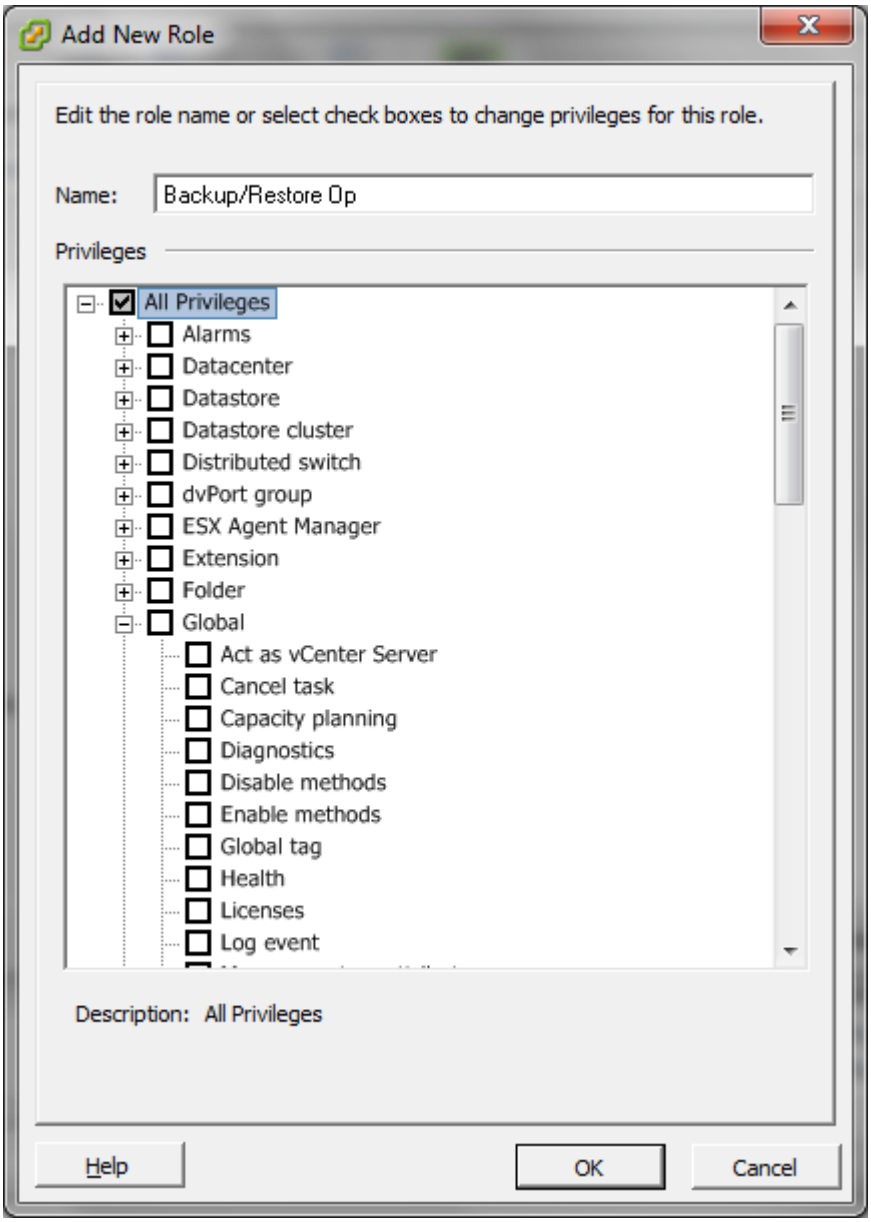
Al utilizar cuentas no administrativas de vCenter para facilitar las operaciones de copia de seguridad y de restauración, se deben crear roles de vCenter, asignar privilegios a los roles y, a continuación, aplicar el rol a los usuarios individuales o a los grupos.

Nota: Como práctica recomendada, VMware aconseja que permita que las cuentas de usuario de vCenter que no sean administrativas puedan ser miembros del grupo de administradores locales de Windows.

Importante: Los pasos siguientes suponen que el usuario está familiarizado con el modo de configurar usuarios de vCenter, sus grupos, roles y permisos. Consulte la documentación de vCenter si es necesario.

Siga estos pasos:

1. Inicie sesión en vCenter mediante VI Client.
2. Abra el cuadro de diálogo Add New Roles y especifique un nombre para el rol.



3. Expanda All privileges.
4. **(Opcional)** Para **facilitar al rol solamente las operaciones de copia de seguridad**, especifique los privilegios siguientes:

   Importante: Para facilitar al rol las operaciones de copia de seguridad y de restauración, continúe al paso siguiente.

   - Expanda la Virtual machine y Configuration y especifique los privilegios siguientes:
     - Seguimiento de cambios de disco
     - Entrega de disco
     - Agregar disco existente

- Agregar disco nuevo
- Agregar o eliminar dispositivo
- Cambiar recurso
- Extraer disco
- Configuración

- Expanda Virtual machine y Provisioning y especifique los privilegios siguientes:
  - Permitir el acceso de solo lectura al disco
  - Permitir la descarga de la máquina virtual
- Expanda Virtual machine y especifique los privilegios siguientes:

  vSphere 4: Expanda State y especifique Create Snapshot y Remove snapshot.

  vSphere 5: Expanda Snapshot management, State y, a continuación, especifique Create Snapshot and Remove snapshot.
- Expanda Global y seleccione los privilegios siguientes:
  - Desactivar métodos
  - Activar métodos
  - Licencias

  Vaya al paso 6.

5. Para **facilitar al rol las operaciones de copia de seguridad y de restauración**, especifique los privilegios siguientes:
   - Expanda Datastore y especifique los privilegios siguientes:
     - Allocate space
     - Explorar el almacén de datos
     - Low level file operations
   - Expanda Global y seleccione los privilegios siguientes:
     - Desactivar métodos
     - Activar métodos
     - Licencias
   - Expanda Host, expanda Local Operations y, a continuación, especifique Reconfigure virtual machine.

Nota: Este privilegio solamente es necesario cuando se realicen operaciones de copia de seguridad y de restauración mediante el modo de transporte HotAdd.

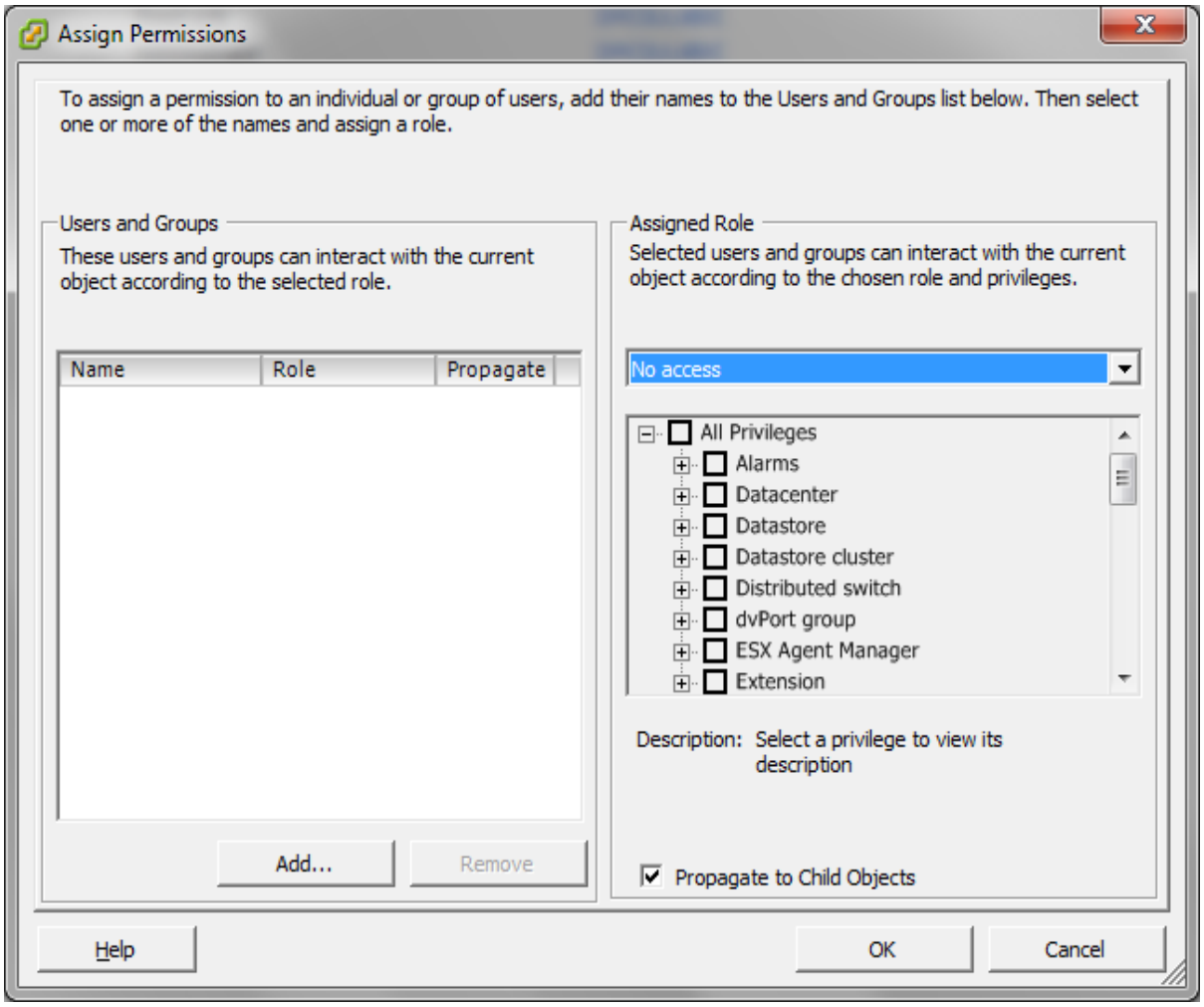
- Expanda Network y especifique Assign Network.
- Expanda Resource y haga clic en Assign Virtual Machine a la agrupación de recursos.
- Expanda la Virtual machine y Configuration y especifique los privilegios siguientes:
  - Agregar disco existente
  - Agregar disco nuevo
  - Agregar o eliminar dispositivo
  - Avanzado
  - Cambiar número de CPU
  - Cambiar recurso
  - Seguimiento de cambios de disco
  - Entrega de disco
  - Dispositivo USB de host
  - Memoria
  - Modify device setting
  - Dispositivo sin formato
  - Volver a cargar desde la ruta
  - Extraer disco
  - Renombrar
  - Reset guest information
  - Configuración
  - Ubicación del archivo de intercambio
  - Actualizar hardware virtual
- Expanda Virtual machine y Guest Operations y especifique los privilegios siguientes:
  - Guest Operation Modifications
  - Guest Operation Program Execution
  - Guest Operation Queries (vSphere 5)

- Expanda Virtual machine e Interaction y especifique los privilegios siguientes:
  - Apagar
  - Encender
- Expanda Virtual machine e Inventory y especifique los privilegios siguientes:
  - Crear nuevo
  - Registrar
  - Eliminar
  - Unregister
- Expanda Virtual machine y Provisioning y especifique los privilegios siguientes:
  - Permitir el acceso de disco
  - Permitir el acceso de solo lectura al disco
  - Permitir la descarga de la máquina virtual
- Expanda Virtual machine y especifique los privilegios siguientes:

  vSphere 4: Expanda State y especifique Create Snapshot, Remove snapshot y Revert to snapshot.

  vSphere 5: Expanda Snapshot management, expanda State y, a continuación, especifique Create snapshot, Remove snapshot y Revert to snapshot.

6. Haga clic en Aceptar para crear la excepción.
7. Abra el cuadro de diálogoAssign Permissions para asignar el rol nuevamente creado a usuarios, grupos, o a ambos.



8. En la lista Users and Groups, seleccione el usuario personalizado que se desee usar para las copias de seguridad y restauraciones.

   En la lista desplegable Assigned Role, especifique el rol que desee aplicar a los usuarios o grupos.

9. Haga clic en Aceptar para aplicar el rol a los usuarios o grupos.

   Los permisos se definen ahora para los roles de vCenter.

La tarea de copia de seguridad para la plantilla de máquina virtual siempre se convierte en copia de seguridad completa y el tamaño de los datos de la copia de seguridad es el tamaño de aprovisionamiento del disco virtual

Síntoma

Cuando se realiza la copia de seguridad de una plantilla de máquina virtual, la tarea de copia de seguridad se convierte en copia de seguridad completa y el tamaño de los datos procesados es igual al tamaño de aprovisionamiento del disco virtual. El siguiente mensaje de advertencia aparece en el registro de actividades.

Como la máquina virtual está configurada como plantilla, la tarea será una copia de seguridad completa y se realizará la copia de seguridad de los discos virtuales como discos completos.

Solución

Este comportamiento es el esperado para la copia de seguridad de la plantilla de máquina virtual. Una solución alternativa consiste en convertir la plantilla en máquina virtual al principio de la copia de seguridad, llevar a cabo la copia de seguridad y volver a convertirla en plantilla al final de la tarea de copia de seguridad. Si prefiere esta solución alternativa, siga estos pasos para establecer un valor del registro en el equipo proxy.

1. Inicie sesión en el equipo proxy.
2. Cree un valor del registro en el nivel del servidor proxy o en el nivel de la máquina virtual.

   Nota: Si se agrega el valor del registro tanto en el nivel de la máquina virtual como en el nivel del servidor proxy, la configuración en el registro del nivel de la máquina virtual tiene prioridad sobre la configuración del registro del nivel del servidor proxy.

   En el nivel de servidor proxy (aplicable a todas las tareas de copia de seguridad que se ejecutan en este servidor proxy)

   a. Abra la clave de registro desde la siguiente ubicación:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

b. Agregue un valor DWORD con el nombre *TemplateDirectBackup* y especifique su valor en 0.

En el nivel de máquina virtual

a. Abra la clave de registro desde la siguiente ubicación:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Agregue un valor DWORD con el nombre *TemplateDirectBackup* y especifique su valor en 0.

Nota: Después de habilitar esta opción, no se puede volver a convertir la máquina virtual en plantilla en caso de que la copia de seguridad termine anormalmente (por ejemplo, durante los bloqueos de las tareas o cuando se reinicia el equipo proxy).

La tarea de copia de seguridad de la plantilla de máquina virtual omite los discos independientes

Síntoma

Cuando se lleva a cabo la copia de seguridad de una plantilla de máquina virtual, la tarea de copia de seguridad omite los discos independientes y aparece el siguiente mensaje de advertencia en el registro de actividades:

Unable to backup virtual disk [datastore_720_4] shuli02-t235/shuli02-t235_1.vmdk because it is an independent disk.

Solución

Este comportamiento es el esperado para la copia de seguridad de la plantilla de máquina virtual. La causa raíz es una limitación de VMware que impide a la aplicación de la copia de seguridad abrir el VMDK de discos independientes. Una solución alternativa consiste en establecer discos independientes en discos dependientes al principio de la copia de seguridad, realizar la copia de seguridad y ponerlos al final de la tarea de copia de seguridad. Si prefiere esta solución alternativa, siga estos pasos para establecer un valor del registro en el equipo proxy.

1. Inicie sesión en el equipo proxy.
2. Cree un valor del registro en el nivel del servidor proxy o en el nivel de la máquina virtual.

   Nota: Si se agrega el valor del registro tanto en el nivel de la máquina virtual como en el nivel del servidor proxy, la configuración en el registro del nivel de la máquina virtual tiene prioridad sobre la configuración del registro del nivel del servidor proxy.

   En el nivel de servidor proxy (aplicable a todas las tareas de copia de seguridad que se ejecutan en este servidor proxy)

   a. Abra la clave de registro desde la siguiente ubicación:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

   b. Agregue un valor DWORD con el nombre *ConvertIndependentVMDK* y especifique su valor en 1.

   En el nivel de máquina virtual

   a. Abra la clave de registro desde la siguiente ubicación:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Agregue un valor DWORD con el nombre *ConvertIndependentVMDK* y especifique su valor en 1.

Notas:

- Después de habilitar esta opción, no se puede revertir los discos independientes en caso de que la copia de seguridad termine anormalmente (por ejemplo, cuando se bloque la tarea o se reinicia el equipo proxy).
- Esta opción no funciona cuando la opción para "convertir la plantilla a máquina virtual durante la copia de seguridad" está activada (el valor del registro TemplateDirectBackup se crea con valor 0).

Se produce un error en la tarea de copia de seguridad de la máquina virtual en el recurso compartido de SMB 3.0 con un mensaje de error

Nota: Válido para Hyper-V.

Síntoma

La máquina virtual reside en Hyper-V 2012 o 2012 R2 y tiene archivos en el recurso compartido SMB 3.0. Se continúa produciendo un error en la tarea de copia de seguridad con cualquiera de los siguientes mensajes de error:

Se ha producido un error al tomar la instantánea VSS. Error del sistema= [VSS_E_ VOLUME_NOT_SUPPORTED_BY_PROVIDER]

Se ha producido un error al tomar la instantánea VSS. Error del sistema=[VSS_E_ BAD_STATE]

Solución

1. Si un servidor de archivos de Windows aloja el recurso compartido de SMB, agregue el rol del servicio del Agente de VSS del servidor de archivos al servidor de archivos y asegúrese de que está instalado el servicio del Agente de instantáneas del servidor de archivos de Microsoft.
2. Si el recurso compartido de SMB se aloja en dispositivos de NAS de terceros o en otras soluciones similares, compruebe si tales dispositivos o soluciones son compatibles con SMB 3.0 y con los protocolos de VSS remoto del servidor de archivos. Para obtener más detalles, póngase en contacto con el distribuidor de terceros.

Nota:

- Para la máquina virtual que reside en Hyper-V 2016, no es necesario Microsoft File Server Shadow Copy Agent Service.
- Se debe configurar correctamente el recurso compartido SMB 3.0 antes de que Arcserve UDP pueda realizar una copia de la máquina virtual. Para obtener los requisitos detallados del recurso compartido SMB 3.0, consulte la sección sobre los requisitos y las configuraciones admitidas en la documentación de Microsoft.

Se produce un error en la tarea de recuperación de la máquina virtual al restaurar la máquina virtual en un recurso compartido predeterminado de archivos de Windows

Nota: Válido para Hyper-V.

Síntoma

Al restaurar la máquina virtual especificando el recurso compartido de archivos predeterminado de Windows (por ejemplo, \\nombrehost\C$\abc) como la ruta de destino, se produce un error en la tarea de restauración y aparece el siguiente mensaje de error:

La tarea de recuperación de la máquina virtual no ha podido crear la nueva máquina virtual.

Solución

Se espera el error de la tarea porque los archivos de la máquina virtual no pueden almacenarse en el recurso compartido de archivos predeterminado del sistema de Windows. Solo se admite el recurso compartido de archivos de Microsoft SMB 3.0. Para obtener más detalles, consulte la *documentación de Microsoft*.

La información del volumen no está disponible para el punto de recuperación

Síntoma

En el asistente de restauración de archivos o de la máquina virtual, mientras se monta el punto de recuperación o se copia el punto de recuperación, no se mostrará ningún archivo ni volumen en la pantalla del punto de recuperación. En su lugar, aparece el siguiente mensaje:

La información del volumen no está disponible para este punto de recuperación.

Solución

Este comportamiento es el esperado si la máquina virtual de origen no tiene el sistema operativo Windows. Por lo tanto, Arcservev UDP no puede analizar los discos virtuales de la máquina virtual para obtener la información del volumen. Se puede restaurar toda la máquina virtual o copiar el punto de recuperación. Si la máquina virtual de origen tiene el sistema operativo de la máquina virtual de Linux, también se pueden restaurar archivos desde el punto de recuperación utilizando un servidor de copia de seguridad de Linux.

Convierta las copias de seguridad incrementales en copias de seguridad de verificación porque las instantáneas de la máquina virtual se han modificado desde la última tarea de copia de seguridad o requieren una consolidación

Nota: Válido en plataformas de Windows.

Síntoma

Las copias de seguridad incrementales para máquinas virtuales de VMware se convierten en copias de seguridad de verificación. El registro de actividades muestra el mensaje siguiente:

"Convierta las copias de seguridad incrementales en copias de seguridad de verificación porque las instantáneas de la máquina virtual se han modificado desde la última tarea de copia de seguridad o requieren una consolidación."

Solución

Utilice el cliente de VMware vSphere para consolidar las instantáneas de máquina virtual. Para obtener más detalles sobre la consolidación de instantáneas, consulte el artículo de la base de conocimiento de VMware.

Nota: Es posible que la consolidación de las instantáneas para una máquina virtual pueda producir un error debido a archivos bloqueados. Si la tarea de copia de seguridad utiliza el modo de transporte de HOTADD, verifique que los valores de configuración de la máquina virtual del proxy de la copia de seguridad en el servidor ESXi no contienen los discos duros agregados en caliente. A continuación consolide las instantáneas de la máquina virtual.

Se produce un error en la copia de seguridad sin agente para la máquina virtual de VMware si el dispositivo de CD/DVD de la máquina virtual está conectado a una imagen ISO que se encuentra en un almacén de datos de NFS desconectado

Síntoma

Realice los pasos siguientes para ver la incidencia:

1. Prepare una imagen ISO en un almacén de datos de NFS conectado al host de ESX.
2. Adjunte la imagen ISO al dispositivo de CD/DVD de una máquina virtual.
3. Desconecte el almacén de datos de NFS de la red.
4. Realice la copia de seguridad sin agente para la máquina virtual.

En este caso, se produce un error en la tarea de copia de seguridad con un mensaje de error parecido a "No se puede obtener una instantánea de la máquina virtual. El servidor vCenter/ESX ha informado sobre el siguiente error: Se ha producido un error general del sistema."

Solución

Debido a la limitación de ESX, no es posible realizar instantáneas cuando la máquina virtual desconecta la imagen ISO conectada. Como solución alternativa, quite la imagen ISO del dispositivo de CD/DVD de la máquina virtual antes de la copia de seguridad.

Se produce un error en la copia de seguridad basada en el host sin agente de la máquina virtual de Hyper-V después de actualizar Arcserve UDP

Válido para Hyper-V

Síntoma

Después de actualizar Arcserve UDP desde la versión 5.0 Actualización 2 o anterior a la última versión, ha empezado a producirse un error en la copia de seguridad basada en el host sin agente con el siguiente mensaje de error:

Se cancela la tarea de copia de seguridad. Para una instantánea VSS, el editor de Hyper-V VSS tiene que guardar la máquina virtual y esto no se aplica en el plan actual. Para reiniciar la tarea de copia de seguridad, cambie la configuración del método de instantánea de Hyper-V en el plan. Para obtener más información sobre cómo configurar el método de instantánea de Hyper-V en un plan, consulte la documentación del producto.

La copia de seguridad basada en el host sin agente funcionaba antes de la actualización.

Solución

En Arcserve UDP 5.0 Actualización 2 o anterior, cuando la máquina virtual no admite el método de copia de seguridad en línea, el comportamiento predeterminado es adoptar el método de copia de seguridad sin conexión. El método de copia de seguridad sin conexión guarda la máquina virtual mientras se toma una instantánea. En el estado Guardado, la máquina virtual es inaccesible. Sin embargo, las máquinas virtuales críticas tienen que ser accesibles todo el tiempo.

En la versión 5.0 Actualización 3 y en las versiones posteriores, si la máquina virtual debe colocarse en el estado Guardado, el comportamiento predeterminado es cancelar la tarea de copia de seguridad para evitar cualquier período de inactividad de la máquina virtual. Si no se desea que la tarea de copia de seguridad se cancele, cambie la opción **Método de instantáneas de Hyper-V** del plan. Para obtener más detalles sobre la opción Método de instantánea de Hyper-V del plan, consulte Cómo crear un plan de copia de seguridad de máquina virtual basada en el host.

También puede consultar el artículo de KB de Arcserve para obtener más detalles sobre este problema.

Error en la copia de seguridad sin agente basada en host en VMware ESXi 6.0

Síntoma

Se puede producir un error en las copias de seguridad sin agente de Arcserve UDP cuando se intenta realizar una copia de seguridad de una máquina virtual en VMware ESXi 6.0 si la función de seguimiento del bloque de cambios (CBT) está activada.

Este problema es un problema conocido de VMware. Cuando se produce un error en la copia de seguridad, se pueden producir los siguientes dos comportamientos:

- Es posible que Arcserve UDP no se pueda conectar a la función de seguimiento del bloque de cambios (CBT) del host de ESXi. Como resultado, Arcserve UDP no podrá recibir la información del bloque de datos utilizados o modificados desde la máquina virtual.
- Es posible que se produzca un error en Arcserve UDP al capturar las instantáneas desactivadas de la máquina virtual. (Esto puede ocurrir cada vez que Arcserve UDP captura una instantánea o cuando se captura manualmente una instantánea en el cliente de vSphere).

Solución

VMware ha solucionado esta incidencia en su última generación, ESXi 6.0 Compilación 2715440. Se puede instalar el parche ESXi600-201505001 para solucionar este problema. Para obtener más información sobre cómo descargar e instalar el parche, consulte el artículo de la base de conocimiento de VMware.

Si no se puede aplicar el parche, se puede solucionar el problema realizando los siguientes cambios en la clave de registro:

Solución para el error de conexión del seguimiento del bloque de cambios.

Si Arcserve UDP no se puede conectar al seguimiento del bloque de cambios, en lugar de producirse un error en la tarea de copia de seguridad, Arcserve UDP podrá continuar con la tarea de copia de seguridad. Sin embargo, en lugar de realizar una copia de seguridad incremental, Arcserve UDP realizará de forma predeterminada una copia de seguridad completa del disco de la máquina virtual. Si no se desea realizar una copia de seguridad completa de forma automática, se puede agregar una clave de registro para cambiar este comportamiento predeterminado. Si se agrega la clave y se establece el valor en 1, se producirá un error en la tarea de copia de seguridad de Arcserve UDP cuando se produzca un error del seguimiento del bloque de cambios.

Se puede agregar esta clave de registro al servidor proxy tal y como se indica a continuación:

En el nivel de servidor proxy (aplicable a todas las tareas de copia de seguridad que se ejecutan en este servidor proxy)

1. Abra la clave de registro desde la siguiente ubicación:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

2. Introduzca la siguiente dword:

   "BackupEntireDiskOnCBTBitmapFailure"=dword:00000001

3. Guarde la clave de registro.

En el nivel de máquina virtual

1. Abra la clave de registro desde la siguiente ubicación:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

2. Introduzca la siguiente dword:

   "BackupEntireDiskOnCBTBitmapFailure"=dword:00000001

3. Guarde la clave de registro.

Nota: Si se agrega la clave de registro en el registro tanto en el nivel de la máquina virtual como en el nivel del proxy, la configuración del registro en el nivel de la máquina virtual tiene prioridad sobre la configuración del registro en el nivel del servidor proxy.

Solución para un error de instantánea desactivada

Asegúrese de que la opción **Tomar la instantánea sin inactividad de invitado si se produce un error en la instantánea de inactividad** esté seleccionada en la ficha Origen de la planificación de copia de seguridad sin agente basada en host.

La copia de seguridad basada en el host sin agente se bloquea cuando se utiliza Windows 2003 R2 de 64 bits como servidor proxy de la copia de seguridad

La copia de seguridad basada en el host sin agente para la máquina virtual de VMware se bloquea cuando se utiliza Windows 2003 R2 de 64 bits como servidor proxy de la copia de seguridad.

Válido para VMware

Síntoma

Cuando se utiliza un equipo de Windows 2003 R2 de 64 bits como el servidor proxy de la copia de seguridad para proteger la máquina virtual de VMware, a veces la tarea de copia de seguridad se puede bloquear. Se pueden ver los siguientes mensajes de error en el archivo de registro de depuración de la tarea de copia de seguridad:

[2016/01/21 10:18:11:316 00 03820 03336] [VDDKLOG] VixDiskLib: VixDiskLib_OpenEx: Open a disk. {AFBackend.exe::AFBackupVirtual.dll(1746.0)}
[2016/01/21 10:18:11:316 00 03820 03336] [VDDKLOG] VixDiskLibVim: VixDiskLibVim_GetNfcTicket: Get NFC ticket for [datastore1 (3)] VMname/VMware_1.vmdk. {AFBackend.exe::AFBackupVirtual.dll(1746.0)}
[2016/01/21 10:19:11:691 00 03820 03336] [VDDKLOG] VixDiskLibVim: Error 18000 (listener error GVmomiFaultInvalidResponse). {AFBackend.exe::AFBackupVirtual.dll (1746.0)}
[2016/01/21 10:19:11:691 00 03820 03336] [VDDKLOG] VixDiskLibVim: Login failure. Callback error 18000 at 2439. {AFBackend.exe::AFBackupVirtual.dll(1746.0)}
[2016/01/21 10:19:11:691 00 03820 03336] [VDDKLOG] VixDiskLibVim: Failed to find the VM. Error 18000 at 2511. {AFBackend.exe::AFBackupVirtual.dll(1746.0)}

Solución

En Arcserve UDP versión 7.0, VMware VDDK 6.x está integrado. Pero VDDK 6.x no es oficialmente compatible con Windows 2003 R2. Como solución alternativa, se puede llevar a cabo una de las opciones siguientes:

- Cambiar para utilizar un servidor proxy que VDDK 6.x admite oficialmente. Por ejemplo, el servidor proxy con Windows 2008 R2, Windows 2012 o Windows 2012 R2.
- Reemplazar VDDK 6.x integrado por VDDK 5.5, que también es compatible con UDP 7.0. Para obtener más información acerca de cómo reemplazar VDDK, consulte la sección *Cómo aplicar una versión de VDDK distinta a la versión integrada en Arcserve UDP.*

La copia de seguridad sin agente basada en host no utiliza el modo de transporte HotAdd

Síntoma

Para realizar una copia de seguridad de los datos, la tarea de copia de seguridad basada en el host no utiliza el modo de transporte HotAdd ni siquiera cuando está disponible. Esto sucede cuando la máquina virtual de origen se importa a la Consola de Arcserve UDP desde un host de ESX (en vez de desde vCenter Server) y el servidor de vCenter gestiona el host de ESX.

Solución

Para resolver este error se deben realizar las tareas siguientes:

- Suprima el nodo de la máquina virtual de la Consola de Arcserve UDP. Importe el nodo de nuevo desde vCenter Server, que se encarga de gestionar el host de ESX.
- Desconecte ESX de vCenter Server.

La tarea de copia de seguridad o restauración sin agente basada en host utiliza el modo de transporte NBD o NBDSSL incluso cuando se puede usar el modo SAN

Válido en plataformas de Windows. Válido solo para la máquina virtual de VMware.

Síntoma

Aunque el modo de transporte SAN sea posible, la tarea de copia de seguridad o restauración sin agente todavía utiliza el modo de transporte NBD o NBDSSL.

Solución

Se deben cumplir los siguientes requisitos previos para que las tareas de copia de seguridad y restauración sin agente utilicen el modo de transporte SAN.

- El equipo proxy debe ser una máquina física (no puede ser una máquina virtual).
- El equipo proxy se debe conectar al SAN LUN en el que resida la máquina virtual.
- En el equipo proxy, la política de SAN de un disco SAN se debe establecer en OnlineAll.

  Para configurar el disco, haga lo siguiente:

  1. Conéctese al sistema de proxy de copia de seguridad mediante una cuenta con privilegios administrativos.
  2. Abra la línea de comandos de Windows.
  3. En la línea de comandos, introduzca los comandos siguientes:
     a. Escriba diskpart y, a continuación, pulse la tecla Intro.
     b. Escriba “SAN” y, a continuación, pulse Intro.

        Se mostrará la política de SAN actual.

     c. Escriba SAN POLICY=OnlineAll y, a continuación, pulse la tecla Intro.
- Si desea realizar la recuperación de la máquina virtual mediante el modo de transporte SAN, debe configurarse un disco SAN como editable.

  Para borrar el indicador de solo lectura, realice los siguientes pasos:

1. Conéctese al sistema de proxy de copia de seguridad mediante una cuenta con privilegios administrativos.
2. Abra la línea de comandos de Windows.
3. En la línea de comandos, introduzca los comandos siguientes:
    a. Escriba diskpart y, a continuación, pulse la tecla Intro.
    b. Escriba “list disk” y la pulse Intro.

       Se mostrará la lista de discos.
    c. Escriba “select disk xxx” y, a continuación, pulse Intro para seleccionar el disco SAN que se configurará como editable.
    d. Escriba attribute disk clear readonly y, a continuación, pulse Intro.

- En el caso de la recuperación de la máquina virtual, el modo de transporte SAN ofrece el mejor rendimiento en discos gruesos, pero el peor en discos delgados. La recuperación de la máquina virtual utiliza el modo de transporte NBD o NBDSSL para los discos delgados de forma predeterminada. Si desea utilizar el modo de transporte SAN, incluso para discos delgados, puede agregar un valor de cadena EnforceTransportForRecovery con el valor SAN en HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFRestoreDll (cree la clave AFRestoreDll si no existe).
- Al tomar una instantánea durante la copia de seguridad, se generan archivos adicionales. Por tanto, es necesario cierto espacio libre en el dispositivo de almacenamiento en el que residen los archivos VMDK de la máquina virtual. El modo de transporte SAN necesita más espacio libre en comparación con el modo de transporte NBD/NBDSSL. Por tanto, asegúrese de que haya suficiente espacio libre en SAN LUN si desea utilizar el modo de transporte SAN.

Se ha producido un error al crear una instantánea para las máquinas virtuales de Hyper-V cuando se están ejecutando varias tareas

Síntoma

Al ejecutar varias tareas, la creación de la instantánea para la máquina virtual de CSV de Hyper-V tarda demasiado tiempo y se produce un error. Se produce un error incluso después de varios intentos. Se muestra el siguiente mensaje en el registro de actividades de la máquina virtual respectiva.

La creación de la instantánea está en curso y solo puede haber una operación de creación de instantánea en curso al mismo tiempo.

Reinténtelo después de 600 segundos.

Solución

El problema ocurre porque solo se puede ejecutar una creación de la instantánea a la vez.

Para solucionar la incidencia, se puede aumentar el número de intentos o aumentar el intervalo de tiempo de reintentos. También se puede aumentar el número de tareas simultáneas que se pueden ejecutar.

Nota: El valor predeterminado de reintentos es 3 y el valor predeterminado del intervalo de tiempo es 10 minutos.

Para aumentar el número de reintentos, realice los pasos siguientes en el servidor proxy:

1. Abra el registro de Windows.
2. Vaya a HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Cree una clave llamada **VSSWrap**.
4. Haga clic con el botón secundario del ratón en **VSSWrap**, seleccione **Nuevo** y, a continuación, seleccione el valor **DWORD (32 bits)** y especifique el nombre como **VssAsynchMaxRetryTimes**.
5. Especifique el valor tal y como sea necesario.

Para aumentar el intervalo de tiempo entre cada reintento, realice los pasos siguientes en el servidor proxy:

1. Abra el registro de Windows.
2. Vaya a HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Cree una clave llamada **VSSWrap**.

4. Haga clic con el botón secundario del ratón en **VSSWrap**, seleccione **Nuevo** y, a continuación, seleccione el valor **DWORD (32 bits)** y especifique el nombre como **VssAsynchRetryInterval**.
5. Especifique el valor tal y como sea necesario.

Para aumentar el número de tareas simultáneas, realice los pasos siguientes en el servidor proxy:

1. Abra el registro de Windows.
2. Vaya a HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Haga clic con el botón secundario del ratón en **HyperVMaxJobNum**, seleccione **Modificar** y especifique el valor requerido.

Se ha producido un error en Hyper-V al crear la instantánea VSS

Se ha producido un error al realizar la copia de seguridad de la máquina virtual de Hyper-V basada en un host de Hyper-V y se muestra el mensaje siguiente:

Se ha producido un error al tomar la instantánea VSS.

Síntoma

Las siguientes razones son responsables del error de la copia de seguridad:

- Uno o más volúmenes del host de Hyper-V no está formateado con NTFS/Refs.
- Uno o más volúmenes del host de Hyper-V tiene menos de 100 MB de espacio libre.
- Actividad de disco excesiva durante la copia de seguridad.

Solución

Resuelva los problemas del entorno y realice la copia de seguridad de nuevo.

Se ha producido un error al realizar la copia de seguridad de un disco virtual debido al error del sistema [El dispositivo no está preparado (21)]

Válido en plataformas de Windows.

Síntoma

Cuando se produce un error de red o cuando se reinicia un servidor Hyper-V mientras la copia de seguridad está en curso, el registro de actividades especifica que el error puede ser un error de red o un error del sistema de archivos.

Solución

Reinicie la tarea de copia de seguridad otra vez después de que se reinicie el servidor Hyper-V.

Error en la tarea de copia de seguridad

Síntoma

Una tarea de copia de seguridad ha producido un error con el mensaje de error siguiente en los registros de actividades:

En el estado actual no se puede realizar la reconfiguración de la copia de seguridad. Apague la máquina virtual y vuelva a intentar ejecutar la tarea de copia de seguridad. (La máquina virtual se puede volver a encender durante o después de la fase de instantánea).

Solución

Establezca los valores del registro en no reconfigurar disk.enableUUID.

Siga estos pasos:

Se aplica a nivel del proxy y afecta a todas las máquinas virtuales de VMware.

1. Inicie sesión en el servidor de proxy de la copia de seguridad.
2. Abra el editor del registro y busque la siguiente clave:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll
3. Agregue un valor de DWORD con el nombre DoNotReconfigDiskUUID y especifique 1 como su valor.

Se aplica a nivel de la máquina virtual específica y solamente afecta a la máquina virtual especificada.

1. Inicie sesión en el servidor de proxy de la copia de seguridad.
2. Abra el editor del registro y busque la siguiente clave:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM-InstanceUUID>

   Nota: Reemplace <VM-InstanceUUID> por el valor de UUID de la máquina virtual para la cual se aplica esta configuración. El valor se puede encontrar en la dirección URL de la máquina virtual que se usa cuando se conecta al Agente de Arcserve UDP.
3. Agregue un valor de DWORD con el nombre DoNotReconfigDiskUUID y especifique 1 como su valor.

Tenga en cuenta los siguientes puntos:

- El nivel de máquina virtual tiene preferencia si se han configurado registros a nivel de la máquina virtual como del proxy.
- Si el registro no existe, el valor del registro implica 0, es decir, se debe reconfigurar disk.enableUUID.
- Si se ha especificado que no se debe reconfigurar el parámetro disk.EnableUUID, es posible que los datos de la copia de seguridad no estén en un estado coherente.

Para obtener más información sobre esta incidencia, consulte el artículo de la base de conocimiento de VMware.

Se produce un error al importar máquinas virtuales de VMware desde vCenter

Síntoma

Aunque el servidor vCenter funcione correctamente y se pueda conectar con el explorador y el cliente de vSphere, Arcserve UDP no puede importar máquinas virtuales de VMware desde vCenter. En archivo ARCAPP-Gateway.log del servidor de la Consola de Arcserve UDP, el mensaje de error aparece de la siguiente manera:

com.sun.xml.ws.client.ClientTransportException: HTTP transport error: javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: Certificates does not conform to algorithm constraints

Pero cuando se cambian las dos líneas siguientes en el archivo "C:\Archivos de programa\Arcserve\Unified datos Protection\Common\JRE\lib\security\java.security" y se reinicia el servicio de gestión de Arcserve UDP, podrá conectarse al mismo servidor vCenter mediante Arcserve UDP:

Líneas existentes:

jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024

jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768

Líneas modificadas:

jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 512

jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 512

Causa:

El servidor vCenter tiene un certificado con una clave pública corta o se ha desactivado el algoritmo mediante el JRE en Arcserve UDP. Un certificado con una clave pública menor de 1024 bits no se considera seguro (lo mismo se aplica al algoritmo MD5). Los desactiva el JRE que utiliza Arcserve UDP.

Solución

Genere un certificado nuevo para el servidor vCenter. Garantice que el certificado nuevo tenga una clave pública que tenga un tamaño mayor de 1024 bits y utilice un algoritmo más fuerte.

Se produce un error en las copias de seguridad debido a la licencia de ESXi

Válido en plataformas de Windows.

Síntoma

Se produce un error en las copias de seguridad completas, progresivas o de verificación. Aparecerá el siguiente mensaje en el registro de actividades de Arcserve UDP:

El servidor de máquinas virtuales <server_name> no tiene una licencia de ESX pagada

Solución

Debido a una limitación de VMware, no se pueden realizar copias de seguridad de las máquinas virtuales en ejecución en servidores de ESXi con una licencia gratuita. Para proteger estas máquinas virtuales, aplique una licencia comprada.

El modo de transporte HotAdd no funciona cuando se intenta realizar la copia de seguridad de una máquina virtual de VMware

Síntoma

El modo de transporte de HotAdd no es compatible con esta máquina virtual y, como resultado, se produce un error en la copia de seguridad en el modo de NBDSSL (dispositivo de bloqueo de red cifrado). (La tarea de copia de seguridad se está ejecutando lentamente). La copia de seguridad de una máquina virtual de VMware no está utilizando el modo de transporte de HotAdd. Para obtener más detalles sobre el transporte de HotAdd, consulte este vínculo.

Verifique los siguientes requisitos previos de HotAdd:

- El proxy de la copia de seguridad de HotAdd debe ser una máquina virtual. HotAdd implica adjuntar un disco virtual al proxy de la copia de seguridad, tal y como adjuntar un disco a una máquina virtual.
- El proxy de HotAdd debe tener acceso al mismo almacén de datos que la máquina virtual de destino.
- Los tamaños del bloque de datos y de la versión VMFS para la máquina virtual de destino deben ser iguales al tamaño del almacén de datos donde reside el proxy de HotAdd. Si el proxy de HotAdd es una máquina virtual que reside en un volumen VMFS-3, se debe seleccionar un volumen con un tamaño de bloque adecuado para el tamaño máximo del disco virtual de las máquinas virtuales de las que los clientes van a realizar copias de seguridad, tal y como se muestra en el tamaño del bloque de VMFS-3 para el proxy de copia de seguridad de HotAdd. Esta advertencia no se aplica a los volúmenes de VMFS-5, que siempre disponen de un tamaño de bloque de archivos de 1 MB.

  La tabla siguiente muestra el tamaño de bloque de VMFS-3 para el proxy de copia de seguridad de HotAdd:

Tamaño de bloque de VMFS	Tamaño máximo del disco de destino
1 MB	256 GB
2 MB	512 GB
4 MB	1024 GB
8 MB	2048 GB

- En vSphere 5.1 y anterior, el tamaño máximo admitido de VMDK es de 1,98 TB.
- Los discos que van a ser HotAdd deben ser SCSI. Las unidades de disco IDE no son compatibles con HotAdd.
- Las herramientas de VMware deben estar instaladas y actualizadas en la máquina virtual y en el proxy de la copia de seguridad.
- El almacén de datos necesita espacio suficiente para una instantánea de la máquina virtual.
- Es posible que se produzca un error en HotAdd si se ha creado algún disco con una versión más reciente del hardware que el de la máquina virtual de la se está realizando la copia de seguridad. Por ejemplo, si se ha movido un disco desde la máquina virtual de la versión de hardware 8 a la máquina virtual de la versión de hardware 7. Para solucionar este problema, actualice la versión de hardware de la máquina virtual.
- Un único controlador de SCSI puede tener un número máximo de 15 discos adjuntados. Para ejecutar varias tareas simultáneas con más de 15 discos, es necesario agregar más controladores de SCSI al equipo de proxy de la copia de seguridad.
- En caso de tener una conexión independiente ESX (vCenter no gestiona al servidor de ESX), solo se pueden tener discos HotAdd de las máquinas virtuales que se encuentran en el mismo servidor de ESX que el equipo de proxy de la copia de seguridad.
- Es posible que se produzca un error en HotAdd si se está intentando realizar una copia de seguridad de la máquina virtual a través del servidor de ESX agregado como un servidor independiente en UDP pero que realmente esté gestionado por vCenter.
- Es posible que se produzca un error en HotAdd si la máquina virtual de la que se está intentando realizar una copia de seguridad y el servidor proxy se encuentran en clústeres diferentes.

Solución

Desactive la opción Automount (Montaje automático) en el equipo de proxy de la copia de seguridad mediante la utilidad diskpart.

Control más detallado de VSS sobre las desactivaciones del sistema operativo invitado de Windows

Síntoma

Deseo especificar un control más detallado de VSS durante la creación de la instantánea de desactivación para los sistemas operativos invitados de Windows.

Solución

En vSphere 6.5, la API del servicio web de vSphere permite los siguientes controles más detallados para VSS cuando se crea la instantánea de desactivación para los sistemas operativos invitados de Windows:

- Se puede configurar en cualquier lugar el tiempo de espera para las máquinas virtuales de desactivación indicando un valor comprendido en un intervalo de cinco minutos a cuatro horas (el valor predeterminado es de 15 minutos).
- Tipo de copia de seguridad de VSS: VSS_BT_COPY se ha utilizado previamente como el valor predeterminado durante la creación de la instantánea. Pero ahora también están disponibles VSS_BT_FULL VSS_BT_INCREMENTAL, VSS_BT_DIFFERENTIAL y VSS_BT_LOG. Se activa el truncamiento del registro de acuerdo con la configuración de la aplicación.
- Se introduce el contexto de la copia de seguridad de VSS para forzar la desactivación de la aplicación (contexto VSS_CTX_BACKUP) o la desactivación del sistema de archivos (contexto VSS_CTX_FILE_SHARE_BACKUP).

Con Arcserve UDP, se pueden especificar los parámetros en el registro para implementar el control.

Nota: Para especificarlos, se requiere VMware Tools 10.1.0 o versión posterior instalado en el sistema operativo invitado de la máquina virtual.

Siga estos pasos:

1. Inicie sesión en el equipo proxy.
2. Cree un valor del registro en el nivel del servidor proxy o en el nivel de la máquina virtual.

   Nota: Si se agrega el valor del registro tanto en el nivel de la máquina virtual como en el nivel del servidor proxy, la configuración en el registro del nivel

de la máquina virtual tiene prioridad sobre la configuración del registro del nivel del servidor proxy.

En el nivel de servidor proxy (aplicable a todas las tareas de copia de seguridad que se ejecutan en este servidor proxy)

a. Abra la clave de registro desde la siguiente ubicación:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

b. Agregue las siguientes valores DWORD con los valores correctos:

   - VssUseEnhancedSnapshot
   - VssTimeoutMinute
   - VssBackupType
   - VssBackupContext
   - VssBootableSystemState
   - VssPartialFileSupport

En el nivel de máquina virtual

a. Abra la clave de registro desde la siguiente ubicación:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Agregue las siguientes valores DWORD con los valores correctos:

   - VssUseEnhancedSnapshot
   - VssTimeoutMinute
   - VssBackupType
   - VssBackupContext
   - VssBootableSystemState
   - VssPartialFileSupport

Valores posibles de los valores del registro:

VssUseEnhancedSnapshot

- 0: No se utiliza el control mejorado y los valores del registro no son efectivos.
- 1: Se utiliza el control mejorado y los valores del registro no son efectivos.

VssTimeoutMinute

Intervalo de 5 a 240

VssBackupType

- 0 - VSS_BT_COPY (valor predeterminado)
- 1 - VSS_BT_FULL
- 2 - VSS_BT_INCREMENTAL
- 3 - VSS_BT_DIFFERENTIAL
- 4 - VSS_BT_LOG

VssBackupContext

- 0 - ctx_auto
- 1 - ctx_backup (valor predeterminado)
- 2 - ctx_file_share_backup

VssBootableSystemState

- 0 – falso
- 1 - verdadero (valor predeterminado)

VssPartialFileSupport

- 0 - ralso (valor predeterminado)
- 1 - verdadero

No se puede configurar la máquina virtual para activar el parámetro Disk.EnableUUID

Síntoma

Se produce un error durante la reconfiguración de la máquina virtual para activar el parámetro Disk.EnableUUID, que es necesario para realizar una copia de seguridad coherente con la aplicación. Este problema se produce cuando el entorno virtual se ha recuperado de un error.

Solución

Este problema es específico del entorno de VMware. Este problema se produce cuando Microsoft VSS intenta realizar una instantánea desactivada por la aplicación pero se produce un error al leer el valor del UUID o del número de serie de uno o más discos de la máquina virtual.

El parámetro disk.EnableUUID de la máquina virtual debe estar activado. Las máquinas virtuales creadas en la versión 4.1 o posterior tienen este parámetro activado de forma predeterminada. La tarea de copia de seguridad se configura

automáticamente para evitar la incoherencia de los datos y para realizar una copia de seguridad coherente de la aplicación. Si se produce un error en la tarea de copia de seguridad al activar el parámetro Disk.EnableUUID, configure manualmente el parámetro mediante los pasos siguientes:

Siga estos pasos:

1. Apague la máquina virtual.
2. Inicie sesión en vCenter Server o en el host de ESX/ESXi a través del cliente de vSphere.
3. Haga clic con el botón secundario del ratón en la máquina virtual y haga clic en Edit settings.
4. Haga clic en la ficha Options.
5. Vaya a Advanced > General > Configuration Parameters.
6. Agregue o modifique la fila del parámetro disk.EnableUUID y establézcalo en True.
7. Haga clic en OK para guardar.
8. Haga clic en OK para salir.
9. Reinicie la máquina virtual para que los cambios entren en vigor.

   Nota: Si el parámetro ya está establecido en True, hay una solución alternativa que no provoca interrupciones y que consiste en editar el archivo .vmx y establecer el valor de disk.enableUUID en False y, a continuación, utilizar el almacenamiento vMotion en la máquina virtual (en cualquier otro host) para volver a cargar el archivo .vmx en la memoria del host. De esta manera se desactiva eficazmente la desactivación a nivel de la aplicación (la desactivación del sistema de archivos todavía está disponible).

Las operaciones de recuperación producen un error al recuperar datos mediante el modo de transporte HotAdd o SAN

Válido en plataformas de Windows.

Síntoma

Las operaciones de recuperación producen un error al recuperar datos mediante el modo de transporte HotAdd o SAN. Aparecerá el siguiente mensaje en el registro de actividad:

Se ha producido un error desconocido. Póngase en contacto con Soporte técnico.

Solución

Las operaciones de recuperación producen un error mediante el modo de transporte HotAdd o el modo de transporte SAN cuando los valores de configuración del disco no se configuran correctamente.

Para configurar el disco, realice los pasos siguientes:

1. Conéctese al sistema de proxy de copia de seguridad mediante una cuenta con privilegios administrativos.
2. Abra la línea de comandos de Windows.
3. En la línea de comandos, introduzca el siguiente comando:

   diskpart

   Pulse la tecla Intro.
4. Escriba SAN y a continuación pulse la tecla Intro.

   Se mostrará la política de SAN actual.
5. Escriba el siguiente comando y pulse Intro:

   SAN POLICY = OnlineAll

   La política de SAN está configurada de manera que no se montan automáticamente volúmenes hospedados de SAN.
6. Para borrar el atributo de solo lectura del disco de SAN específico, seleccione el disco de la lista de discos, escriba el comando siguiente y pulse Intro:

   attribute disk clear readonly
7. Escriba Salir y a continuación pulse la tecla Intro.

   El disco se habrá configurado y se podrá reenviar la tarea.

Si se vuelve a producir un error en la tarea, monte manualmente los discos de HotAdd mediante la gestión de discos en el sistema proxy.

Para montar los discos manualmente, realice los siguientes pasos:

1. Conéctese al sistema de proxy de copia de seguridad mediante una cuenta con privilegios administrativos.
2. Abra Panel de control de Windows y haga doble clic en Herramientas Administrativas.

   Aparece la ventana Herramientas administrativas.
3. De la lista de Favoritos, haga doble clic en Gestión de equipos.

   Aparecerá el cuadro de diálogo Gestión de equipos.
4. Expanda Almacenamiento y haga clic en Gestión de discos.

   Se mostrarán los discos.
5. Haga clic con el botón secundario en el disco que desea montar y haga clic en En línea.

   El disco se habrá montado y se podrá reenviar la tarea.

Error de recuperación de la máquina virtual al especificar un puerto no predeterminado

Síntoma

Cuando se especifica un puerto que no es el predeterminado para el servidor VMware vCenter, se produce un error al ejecutar la recuperación de la máquina virtual.

Solución

Para solucionar el problema, establezca un número de puerto no predeterminado de vCenter para el valor de VDDKport en el registro del equipo del proxy de la copia de seguridad.

Para establecer el número de VDDKport, realice los pasos siguientes en el servidor proxy:

1. Abra el registro de Windows.
2. Vaya a HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Haga clic con el botón secundario del ratón en VDDKport, seleccione Modificar y especifique el valor requerido.

Error en la tarea de copia de seguridad incremental programada o completa para la máquina virtual de Hyper-V

Síntoma

A veces la tarea de copia de seguridad incremental o completa programada produce un error en las máquinas virtuales de Hyper-V y se muestran los errores siguientes en el visor de eventos del host de Hyper-V:

- Se ha producido un error al agregar la operación DM para la máquina virtual <nombre de máquina virtual>: memoria agotada (0x8007000E) (ID de máquina virtual <ID de máquina virtual>)
- No se ha podido crear un punto de control de copia de seguridad para la máquina virtual <nombre de máquina virtual>: esta operación se ha devuelto porque el período de tiempo de espera ha caducado. (0x800705B4). (Virtual machine ID <vm ID>)
- No se ha podido crear un punto de control de copia de seguridad para la máquina virtual <nombre de máquina virtual>: no se ha encontrado el elemento. (0x80070490). (Virtual machine ID <vm ID>)
- Se ha producido un error cuando los editores de VSS de la máquina virtual <nombre de máquina virtual> han intentado realizar la copia de seguridad completa de su conjunto de instantáneas (instantáneas VSS): se realizó una llamada de función cuando el objeto se encontraba en un estado incorrecto para dicha función (0x80042301). (Virtual machine ID)
- El editor de Hyper-V VSS ha encontrado un error al procesar esta máquina virtual. (Para obtener más información sobre errores del editor de Hyper-V VSS, consulte la documentación del producto).

Solución 1

La solución es aumentar el tamaño de RAM en el servidor Hyper-V y, a continuación, reenviar la tarea de copia de seguridad.

Solución 2

Si el editor de VSS que se encuentra en la máquina virtual no funciona correctamente, la tarea de copia de seguridad producirá un error. Para resolver la incidencia, compruebe el registro de eventos tanto del host de Hyper-V como de la máquina virtual. Compruebe las advertencias y errores de VSS, y realice las acciones adecuadas.

Error en el editor VSS de NTDS de Hyper-V al tomar la instantánea VSS en la máquina virtual

Síntoma

En una máquina virtual del controlador del dominio, si la función AutoMount no está activada, el editor de VSS NTDS produce un error mientras se toma la instantánea VSS en la máquina virtual. Como resultado, el editor de Hyper-V VSS produce un error al tomar la instantánea VSS en el host de Hyper-V.

Se produce un error en la tarea de copia de seguridad de HBBU de Hyper-V con el registro de actividades siguiente:

El editor de Hyper-V VSS ha encontrado un error al procesar esta máquina virtual. (Para obtener más información sobre errores del editor de Hyper-V VSS, consulte la documentación del producto).

Solución

Active la función *AutoMount* en la máquina virtual.

Siga estos pasos:

1. Abra la ventana de símbolo del sistema.
2. Abra diskpart y ejecute el comando siguiente:

   automount enable

No se conservarán los cambios de la dirección de MAC después de la recuperación de máquinas virtuales

Válido en plataformas de Windows y máquinas virtuales de VMware

Síntoma

Las direcciones MAC de las máquinas virtuales no se conservan tras recuperar máquinas virtuales.

Solución

Las direcciones MAC no se conservan durante la recuperación para evitar los duplicados. Para conservar la información de dirección MAC, establezca la siguiente clave de registro en el servidor proxy:

Ubicación: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
Nombre de clave: RetainMACForVDDK
Tipo de valor: Cadena

Valor clave: 1

Se produce un error en la recuperación de la máquina virtual con el error No se pueden abrir archivos VMDK.

Síntoma

Se ha producido un error al recuperar la máquina virtual y se muestra el siguiente mensaje de error en los registros:

No se puede abrir el archivo VMDK (nombre de archivo con .vmdk). VMware ha comunicado el error siguiente: No tiene derechos para acceder a este archivo. Para obtener más información, consulte el registro de depuración de la restauración. Si es necesario, póngase en contacto con Soporte de Arcserve.

Los mensajes siguientes se encuentran en los registros de depuración de la restauración:

- [VDDKLOG] CnxAuthdConnect: Returning false because SSL verification requested and target authd does not support SSL
- [VDDKLOG] CnxConnectAuthd: Returning false because CnxAuthdConnect failed
- [VDDKLOG] Cnx_Connect: Returning false because CnxConnectAuthd failed
- [VDDKLOG] Cnx_Connect: Error message: SSL required

Solución

El motivo puede ser que se desactiva la autenticación SSL en el host de ESX. Para solucionar esta incidencia, utilice uno de los métodos siguientes:

Uso del cliente de vSphere

1. Inicie sesión en el servidor vCenter/ESX.
2. Vaya a la configuración del servidor ESX:

   Configuración, Configuración avanzada, Configuración, Valores predeterminados de seguridad

3. Active la siguiente opción:

   config.defaults.security.host.ruissl

Uso de la línea de comandos

1. Conéctese al host de ESX mediante SSH.
2. Abra el siguiente archivo:

/etc/vmware/config

3. Establezca la entrada security.host.ruissl en VERDADERO.
4. Guarde el archivo y reinicie los agentes de gestión.

Problemas causados por UUID de la máquina virtual duplicados

Síntoma 1

El nodo de máquina virtual se sobrescribe después de importar otro nodo de máquina virtual en la Consola.

Por ejemplo, existen 2 máquinas virtuales llamadas VM1 y VM2 con el mismo UUID (que se llama UUID de la instancia para VMware y UUID de la máquina virtual para Hyper-V) en los hosts de ESXi que están gestionados por diferentes vCenter VC1 y VC2. Importe VM1 a la Consola y se mostrará en la vista de lista de nodos de la Consola. Más adelante, importe VM2 a la Consola. En la vista de lista de nodos, VM2 sobrescribe a VM1 (en otras palabras, se agrega VM2 pero VM1 ya no existe).

Síntoma 2

La información del nodo de máquina virtual de la columna Hipervisor cambia constantemente mientras se esté ejecutando la detección automática.

Por ejemplo, existen 2 máquinas virtuales llamadas VM1 y VM2 con el mismo UUID (que se llama UUID de la instancia para VMware y UUID de la máquina virtual para Hyper-V) en los hosts de ESXi que están gestionados por diferentes vCenter VC1 y VC2. Importe VM1 a la Consola. También se puede importar al menos una máquina virtual desde vCenter VC2 para que se agreguen tanto VC1 como VC2 a la lista de detección de nodos (se puede comprobar la lista en la página Configuración de la detección de nodos que se encuentra en la ficha Configuración). Cuando se ejecuta la detección de nodos, primero se conecta con VC1 y se detecta la VM1 utilizando el GUID para que la columna Hipervisor se actualice con la información de VC1. Después, cuando se conecta con VC2, detecta la VM2 utilizando el GUID para que la columna Hipervisor se actualice con la información de VC2.

Solución

Arcserve UDP utiliza el UUID de la máquina virtual (que se llama UUID de la instancia para VMware y UUID de la máquina virtual para Hyper-V) a fin de identificar el nodo de una máquina virtual. Aunque no es habitual que las máquinas virtuales tengan los UUID duplicados, se pueden producir comportamientos problemáticos en Arcserve UDP en este caso.

Para solucionar los problemas, consulte los siguientes pasos para cambiar de forma manual el UUID de la máquina virtual (aplicable para la máquina virtual de VMware solamente). Después de cambiar manualmente el UUID de la máquina virtual, suprima la máquina virtual original de la Consola de Arcserve UDP y vuelva a importar la máquina virtual.

1. Abra la siguiente dirección URL:

   https://<nombre del host de vCenter>/mob/

2. Inicie sesión como administrador.
3. Busque "content" en la columna NOMBRE y haga clic en el vínculo de la columna VALOR en la misma fila.
4. Busque "rootFolder" en la columna NOMBRE y haga clic en el vínculo de la columna VALOR en la misma fila.
5. Busque "childEntity" en la columna NOMBRE. En la columna VALUE en la misma fila, busque el centro de datos en el que se encuentra la máquina virtual y haga clic en el vínculo.
6. Busque "vmFolder" en la columna NOMBRE y haga clic en el vínculo de la columna VALOR en la misma fila.
7. Busque "childEntity" en la columna NOMBRE. En la columna VALUE en la misma fila, haga clic en "más..." para expandir la lista de máquinas virtuales. Busque la máquina virtual que está buscando y haga clic en el vínculo.
8. Busque ReconfigVM_Task en la tabla Métodos y haga clic en el vínculo.
9. En la nueva ventana del explorador abierta, elimine todo el contenido del campo VALUE y escriba el siguiente código:

   ```
   <spec>
   <instanceUuid>2499952a-6c85-480e-b7df-4cb-
   d2137eb69</instanceUuid>
   </spec>
   ```

   Nota: La cadena 2499952a-6c85-480e-b7df-4cbd2137eb69 mencionada anteriormente es un UUID de muestra. Se debe reemplazar por el UUID que se desea aplicar.

10. Haga clic en el vínculo Invocar método para aplicar el UUID nuevo.
11. Para verificar que se ha aplicado el nuevo UUID, cierre el explorador que se acaba de abrir y vuelva a la página donde se hizo el paso 8.
12. Busque "config" en la columna NOMBRE y haga clic en el vínculo de la columna VALOR en la misma fila.
13. Busque "instanceUuid" en la columna NOMBRE. El UUID de la máquina virtual se muestra en la columna VALUE en la misma fila.

Error en la tarea de catálogo del sistema de archivos o error en la comprobación del punto de recuperación para la copia de seguridad sin agente basada en host

Válido en plataformas de Windows. Válido solo para la máquina virtual de VMware.

Síntoma

- Error en la tarea de catálogo del sistema de archivos para los puntos de recuperación de la copia de seguridad sin agente basada en host
- Error en la comprobación del punto de recuperación durante la tarea de copia de seguridad sin agente basada en host y conversión de la siguiente copia de seguridad incremental en una copia de seguridad de verificación

Solución

Esto puede deberse a un problema conocido de VMware (consulte el artículo de la base de conocimiento de VMware). Cuando se desactiva una máquina virtual de VMware, la instantánea contiene datos dañados. La copia de seguridad lee los datos de la instantánea, así que los datos con copia de seguridad también resultan dañados.

Nota: Este problema ocurre con todas las versiones de VMware ESXi y en una máquina virtual con los sistemas operativos invitados Windows 2008 R2 SP1 y Windows 2012. Arcserve UDP no puede detectar el problema de daño de datos, puesto que VMware no devuelve un error en estos casos. Puede que no se dé cuenta del problema hasta que intente restaurar datos.

Puede seguir lo indicado en el artículo de la base de conocimiento de Arcserve para comprobar si el error está provocado por este problema conocido de VMware. La solución alternativa recomendada por VMware consiste en desactivar los editores de VSS, por ejemplo, el editor del servicio de Microsoft Search (ignorarlo, si no se ha instalado) y el editor de optimización de instantáneas VSS (normalmente presente en todas las máquinas virtuales de Windows), en el sistema operativo de la máquina virtual invitada. Puede desactivar manualmente los editores según las instrucciones del artículo de la base de conocimiento de VMware.

Arcserve UDP también ofrece una forma sencilla de desactivar los editores, si se está usando el método de desactivación de instantáneas de VMware Tools. Siga estos pasos para desactivar los editores.

En el nivel de servidor proxy (aplicable a máquinas virtuales protegidas por este servidor proxy)

1. Inicie sesión en el servidor proxy.
2. Abra la clave de registro desde la siguiente ubicación:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]
   ```

3. Cree un valor de varias cadenas con el nombre *DisableSpecificVSSwriters*.
4. Introduzca los nombres del editor de VSS que desea desactivar (el nombre de cada editor ocupa una línea).
5. Guarde la clave de registro.

En el nivel de máquina virtual

1. Inicie sesión en el servidor proxy.
2. Abra la clave de registro desde la siguiente ubicación:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]
   ```

3. Cree un valor de varias cadenas con el nombre *DisableSpecificVSSwriters*.
4. Introduzca los nombres del editor de VSS que desea desactivar (el nombre de cada editor ocupa una línea).
5. Guarde la clave de registro.

Notas:

- Si se agrega la clave de registro tanto en el registro en el nivel de la máquina virtual y del servidor proxy, la configuración del registro en nivel de la máquina virtual tendrá prioridad sobre la configuración del registro en nivel del servidor proxy.
- Esta configuración de registros solo funciona cuando se usa el método de desactivación de instantáneas de VMware Tools en el plan de copia de seguridad.
- Si alguna vez se han configurado editores manualmente en el sistema operativo invitado de la máquina virtual según el artículo de la base de conocimiento de VMware, se sobrescribirá la configuración.
- El nombre del editor distingue entre mayúsculas y minúsculas, y debe coincidir exactamente con el que se muestra en la salida de “vssadmin list writers”.
- Si desea volver a activar todos los editores, no suprima el valor del registro *DisableSpecificVSSwriters*. En su lugar, conserve el valor del registro, pero elimine el contenido incluido en el registro. Si *DisableSpecificVSSwriters* no existe, Arcserve UDP asume que no se debe cambiar nada en cuanto a la activación o desactivación de editores de VSS.

Conversión de la copia de seguridad incremental en copia de seguridad de verificación o incremento del tamaño de copia de seguridad en Hyper-V

Válido en la máquina virtual de Hyper-V.

Síntoma

- He realizado un cambio incremental en una máquina virtual de Hyper-V. Cuando realizo una copia de seguridad incremental, se realiza una copia de seguridad de toda la máquina virtual en lugar de realizar solamente la copia de seguridad de los datos modificados.
- Tengo un servidor proxy con la actualización 7.0 de Arcserve UDP que realiza copia de seguridad de una máquina virtual desde un host de Hyper-V (ejemplo HOST1). Tengo otro servidor proxy con una versión anterior de Arcserve UDP que realiza copia de seguridad de una máquina virtual desde el mismo host de Hyper-V (HOST1). En tales casos, el seguimiento de bloques modificados (CBT) está inactivo y las tareas incrementales no se ejecutan. La copia de seguridad incremental se convierte en la copia de seguridad de verificación.

Solución

Las causas raíz de los síntomas mencionados anteriormente pueden ser una de las razones siguientes:

- La pérdida de los datos del seguimiento de bloques modificados (CBT). Las siguientes circunstancias darán lugar a la pérdida de datos de CBT:
  - El host de Hyper-V se bloquea o se apaga anormalmente.
  - El servicio de CBT se detiene o el servicio abandona anormalmente.
  - El servicio de CBT no ha completado su trabajo mientras el host de Hyper-V se estaba cerrando.
- Las distintas versiones de CBT en el servidor Hyper-V y el servidor proxy.

  Ejemplo: Dispone de dos entornos de Arcserve UDP, uno es Arcserve UDP versión 6.0 y el otro Arcserve UDP versión 7.0. Estos dos entornos de Arcserve UDP realizan las copias de seguridad de diferentes máquinas virtuales en el mismo servidor Hyper-V. El entorno de Arcserve UDP versión 7.0 detecta automáticamente la versión anterior de CBT en el servidor Hyper-V y la actualiza con la última versión. En tales casos, el entorno de Arcserve UDP versión 5 convierte la copia de seguridad incremental programada restante en una copia de seguridad completa.

Si Arcserve UDP detecta distintas versiones de CBT, el registro de actividades mostrará un mensaje de advertencia.

La solución pasa por actualizar todos los servidores proxy que protegen las máquinas virtuales de un host de Hyper-V a la misma versión de Arcserve UDP.

Se produce un error en la copia de seguridad basada en el host para la máquina virtual de Hyper-V que tiene una configuración especial de discos diferentes.

Válido para la máquina virtual de Hyper-V.

Síntoma

Si un disco diferente se configura en una máquina virtual de Hyper-V, se producirá un error en la tarea de copia de seguridad para dicha máquina virtual. Se muestra el mensaje de error siguiente en el registro de actividades:

Se ha producido un error al preparar la copia de seguridad para la máquina virtual.

Se mostrará el siguiente mensaje de error en el archivo de registro de tareas de copia de seguridad en C:\Program Files\Arcserve\Unified Data Protection\Engine\Logs,

El archivo del disco virtual \\?\UNC\<máquina_virtual_dirección_IP>\HYPERV_HBBU_SNAPSHOT@<nombre_instancia>\WIN12-SQL\VIRTUAL duro DISKS\WIN12-SQL-1.VHDX no se muestra.

El problema solo se produce cuando la máquina virtual tiene las siguientes configuraciones de discos diferentes. Se deben aplicar todas las configuraciones.

- La máquina virtual tiene un disco duro virtual normal (con el tamaño fijo o de expansión dinámico) llamado Disco1 que está conectado a un controlador IDE o SCSI de la máquina virtual.
- La máquina virtual tiene un disco duro virtual diferente (llamado Disco2) que también está conectado a un controlador IDE o SCSI de la máquina virtual.
- Se especifica como Disco1 el disco principal del Disco2.

Solución

Este error se produce debido a una configuración anormal o incorrecta. Para solucionar este error, separe el disco diferente o su disco principal de la máquina virtual. Arcserve UDP no admite esta configuración del disco diferente.

Error en la tarea de copia de seguridad para una máquina virtual de VMware

Válido para la máquina virtual de VMware.

Síntoma

Cuando se realiza una copia de seguridad de una máquina virtual de VMware, se produce un error en la tarea de copia de seguridad con cualquiera de los siguientes mensajes de error en el registro de actividades:

Se anula la copia de seguridad porque la tarea de copia de seguridad se ha configurado para utilizar el método de instantánea de Microsoft VSS dentro de máquina virtual. Sin embargo, solo el método de instantánea de las herramientas de VMware es aplicable debido a que se ha producido un error en la copia de seguridad de la máquina virtual basada en el host al implementar las herramientas necesarias en la máquina virtual.

O

Se anula la copia de seguridad porque la tarea de copia de seguridad se ha configurado para utilizar el método de instantánea de las herramientas de VMware. Sin embargo, solo el método de instantánea de Microsoft VSS dentro de la máquina virtual es aplicable debido a que se ha producido un error en la copia de seguridad de la máquina virtual basada en el host al eliminar la implementación de las herramientas necesarias en la máquina virtual.

Solución

El primer error puede producirse por varias razones. Se ha seleccionado la opción **Microsoft VSS dentro de la máquina virtual** pero:

- No se ha actualizado la máquina virtual con las credenciales necesarias.
- Las credenciales no son correctas.
- Las herramientas de VMware no están instaladas ni actualizadas.

En este caso, Arcserve UDP no puede implementar las herramientas necesarias en la máquina virtual para utilizar el nuevo método de instantánea.

Para resolver este error, actualice la máquina virtual con las credenciales correctas. Verifique que las herramientas de VMware están actualizadas y en funcionamiento en la máquina virtual. Después de la verificación, vuelva a enviar la tarea de copia de seguridad.

Solución

El segundo error se puede producir en el siguiente escenario. Se ha utilizado la opción **Microsoft VSS dentro de la máquina virtual** en las tareas de copia de

seguridad anteriores. Ahora se desea utilizar la opción **Herramientas de VMware** pero las credenciales de la máquina virtual han cambiado (por ejemplo, se ha cambiado la contraseña de SO invitado pero no se ha actualizado el nodo de la máquina virtual en la consola) o las herramientas de VMware no funcionan por alguna razón. En tales casos, Arcserve UDP no puede eliminar la implementación de las herramientas (que la tarea de copia de seguridad anterior ha implementado) desde la máquina virtual para utilizar el nuevo método de instantánea.

Para resolver este error se deben realizar los pasos siguientes:

- Actualice la máquina virtual con credenciales correctas. Verifique que las herramientas de VMware se han actualizado y que están en funcionamiento en el SO invitado de la máquina virtual. Después de la verificación, vuelva a enviar la tarea de copia de seguridad.
- Elimine manualmente la implementación de las herramientas de la máquina virtual:
    a. Inicie sesión en la máquina virtual.
    b. Vaya a la siguiente carpeta:

       C:\Archivos de programa\ARCServe\ASVMOperationTools\custom-freeze-vmware-snapshot\auto-deploy

    c. Haga clic con el botón secundario del ratón en el archivo por lotes auto-undeploy.bat y seleccione Ejecutar como administrador.
    d. Suprima las siguientes carpetas:

       C:\Archivos de programa\ARCServe\as-hbbu-vmwarebackup

       C:\Archivos de programa\ARCServe\ASVMOperationTools

    e. Vuelva a enviar la tarea de copia de seguridad.

Desactivación de una nueva exploración de adaptadores HBA durante la copia de seguridad incremental

Aplicable a VMware ESX

Aplicable solo a UDP v6.5, no se aplica a las Actualizaciones de v6.5.

Síntoma

Cuando el nodo de origen y el servidor proxy se encuentran en diferentes servidores ESX de VMware y ejecuto una copia de seguridad incremental, la copia de seguridad tarda más tiempo en ejecutarse. También recibo varios mensajes para realizar una nueva exploración. Quiero desactivar la nueva exploración de todos los adaptadores de bus del host (hba) de otros servidores ESX de VMware durante las copias de seguridad incrementales.

Solución

Se puede desactivar la exploración creando una clave de registro en el servidor proxy y asignándole un valor.

Siga estos pasos:

1. Inicie sesión en la máquina.
2. Vaya a la siguiente carpeta:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
   ```

3. Cree la clave de registro siguiente (DWORD), si no se ha creado ya.

   ```
   DisableAllESXNodeRescan
   ```

4. Establezca el valor de la clave de registro en 1.

Desactivación de la creación de instantáneas consecutivas en máquinas virtuales de VMware para una copia de seguridad

En la versión anterior de Arcserve UDP, cuando varias tareas de copia de seguridad de máquinas virtuales de VMware que se inician al mismo tiempo, las tareas crean instantáneas en el host de ESX en paralelo a dichas tareas. A veces, dichas operaciones de creación de instantáneas en paralelo aumentan la E/S del disco en el host de ESX. Para evitarlo, Arcserve UDP versión 7.0 serializa de forma predeterminada la operación de creación de instantáneas cuando las tareas se ejecutan en el mismo servidor proxy y dicha operación es para el mismo host de ESX. En otras palabras, la operación de creación de instantáneas se lleva a cabo en serie, una tras otra, y lo ideal es que solo se cree una instantánea por vez. Sin embargo, esto no se aplica si las tareas de copia de seguridad se ejecutan en servidores proxy distintos o si son para hosts de ESX distintos.

Para evitar que la creación de instantáneas se bloquee (o tarde mucho tiempo) y también lo hagan las siguientes tareas, la próxima tarea esperará a la operación anterior de creación de instantáneas durante un máximo de **cinco minutos**. Transcurridos cinco minutos, se iniciará el siguiente proceso de creación de instantáneas.

Se puede desactivar la espera de cinco minutos siguiendo estos pasos:

1. Inicie sesión en el servidor proxy.
2. Abra la clave de registro desde la siguiente ubicación:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

3. Cree un valor DWORD con el nombre **CreateSnapshotSequentially**.
4. Establezca el valor en 0.

Además, se puede cambiar el valor del tiempo de espera predeterminado (cinco minutos) siguiendo estos pasos:

1. Inicie sesión en el servidor proxy.
2. Abra la clave de registro desde la siguiente ubicación:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

3. Cree un valor DWORD con el nombre **CreateSnapshotTimeout**.

4. Establezca el valor con un número.

   La unidad está en segundos.

Cuando se restaura desde una versión superior del host de ESXi a una versión inferior del host de ESXi, la máquina virtual se bloquea en la fase de inicio

Cuando se restaura desde una versión superior del host de ESXi a una versión inferior del host de ESXi, la máquina virtual se bloquea en la fase de inicio después de arrancarla.

Válido en plataformas de Windows. Válido solo para la máquina virtual de VMware.

Síntoma

Restaurar una máquina virtual desde una versión superior del host de ESXi a una versión inferior del host de ESXi y arrancar la máquina virtual. La máquina virtual se bloquea en la fase de inicio.

Solución

La versión del SO invitado de esta máquina virtual podría no ser compatible con la versión inferior de ESXi. Como solución alternativa, se puede llevar a cabo una de las opciones siguientes:

- Restaurar la máquina virtual a un ESXi que sea compatible con esta versión del SO invitado o
- Actualizar el host ESXi existente a la versión adecuada.

Por ejemplo, se realiza una copia de seguridad de la máquina virtual de Windows Server 2012 R2 desde un ESXi 5.5 y se restaura a ESXi 5.0 actualización 1. Este problema puede ocurrir debido a que ESXi 5.0 empezó a ser compatible con sistemas operativos invitados de Windows Server 2012 R2 después de la actualización 2.

Se necesita actualizar ESXi 5.0 actualización 1 a la actualización 2 para admitir el sistema operativo invitado de Windows Server 2012 R2. Como solución alternativa, se puede cambiar la versión del sistema operativo invitado de la máquina virtual restaurada a la versión que sea compatible con la versión actual de ESXi (en el ejemplo anterior, a Windows Server 2008 R2).

Nota: Esta solución alternativa podría no resolver el problema.

La utilización de la memoria RAM alcanza el 99 % cuando las tareas de copia de seguridad se envían a la máquina virtual

La utilización de la memoria RAM alcanza el 99 % cuando las tareas de copia de seguridad se envían a las máquinas virtuales en Windows 2012 Hyper-V CSV.

Síntoma

Durante la copia de seguridad de las máquinas virtuales que forman parte del clúster de Hyper-V 2012, la utilización de la memoria RAM aumenta gradualmente y alcanza el 99 % en el host de Hyper-V propietario de CSV. Como resultado, las máquinas virtuales y el host de Hyper-V dejan de trabajar durante la copia de seguridad.

Solución

Este problema se produce debido a errores conocidos en el código de Microsoft.

Para corregir este problema, descargue y aplique la revisión proporcionada por Microsoft en todos los hosts de Hyper-V desde el vínculo siguiente:

https://support.microsoft.com/en-in/kb/2878635

Se produce un error en la tarea de restauración de Hyper-V, no se puede conectar a la utilidad del host

Se produce un error en la tarea de restauración de la máquina virtual de Hyper-V y aparece un mensaje de error.

Síntoma

Al restaurar una máquina virtual de Hyper-V, se produce un error en la tarea de restauración y aparece el siguiente error en el registro de actividades:

Se ha producido un error al intentar conectarse a la utilidad de restauración de Hyper-V en el host xxxxx.

En el registro de depuración de la tarea de restauración, aparecen los siguientes mensajes de error:

Se ha producido un error al conectarse con xxxxx:10218. Error: Se ha excedido el tiempo de espera del intento de conexión sin establecer una conexión (rc =-536805332)

Se ha producido un error al conectarse con xxxxx:10218, error-536805332

Solución

Normalmente, la causa de este problema es que la conexión entre el host de Hyper-V y el servidor proxy de de la copia de seguridad está bloqueada por el cortafuegos. Si es posible, desactive el cortafuegos y vuelva a intentar la restauración. Si no puede desactivar el cortafuegos, registre el puerto (o el intervalo de puertos) utilizado por la tarea de restauración en la excepción del cortafuegos.

De forma predeterminada, la tarea de restauración elige aleatoriamente un puerto disponible en el intervalo de 1024 y 65535. Se puede especificar manualmente el intervalo de los valores del registro establecido en el host de Hyper-V.

Siga estos pasos:

1. Inicie sesión en el host de Hyper-V.
2. Ejecute el comando *regedit* para abrir el editor del registro.
3. Vaya a la siguiente clave del registro (cree las claves si alguna de ellas no existe):

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\HyperVRestoreStub
4. Cree los dos valores del registro siguientes (DWORD):

   PortMin

PortMax

5. Especifique valores con el número de inicio y final del intervalo de puertos.

   Notas:

   - Intervalo obligatorio de valores especificados: 1024-65535
   - Se puede especificar el mismo número para ambos valores del registro. En este caso, se utiliza el número de puerto fijo para la tarea de restauración. Cuando varias tareas de restauración se ejecutan simultáneamente y tan pronto como una tarea de restauración ocupa este puerto, se produce un error en las otras tareas de restauración.

Se produce un error en la protección automática al detectar y proteger la máquina virtual

No se detecta la máquina virtual ni se protege automáticamente como parte de la protección automática.

Síntoma

Aunque una máquina virtual se puede ver en el hipervisor (vCenter/ESX o Hyper-V) mediante una aplicación de cliente nativa (por ejemplo, el cliente de vSphere cliente o el gestor de Hyper-V), la protección automática no detecta la máquina virtual y, como resultado, la máquina virtual no se puede proteger automáticamente.

Razones

- La máquina virtual no tiene un estado válido en el hipervisor. Por ejemplo, la protección automática omite las máquinas virtuales que tienen el estado Disconnected (Desconectado), Orphaned (Huérfano) o Inaccessible (Inaccesible) en vCenter/ESX.
- Las tareas de Arcserve UDP como Virtual Standby (VSB), máquina virtual instantánea (IVM) o recuperación asegurada (AR) crean la máquina virtual (o se clona desde la máquina virtual de Virtual Standby, de la máquina virtual instantánea o de la recuperación asegurada). Arcserve UDP omite intencionalmente dichas máquinas virtuales debido a las siguientes consideraciones:
  - Cuando Arcserve UDP realiza las copias de seguridad de las máquinas virtuales creadas mediante las tareas de Virtual Standby (VSB), máquina virtual instantánea (IVM) o recuperación asegurada (AR) sin limitación, se puede producir una situación de *bucle infinito de copias de seguridad*. Por ejemplo, utilice la protección automática para proteger todo el ESX. En el plan de copia de seguridad, después de agregar una tarea de copia de seguridad, agregue una tarea de Virtual Standby que crea una máquina virtual de Virtual Standby en el mismo servidor ESX. Por lo tanto, después de la primera copia de seguridad se crea una nueva máquina virtual de Virtual Standby en ESX. La protección automática detecta la nueva máquina virtual de Virtual Standby y se agrega al plan de copia de seguridad. A continuación, durante la siguiente copia de seguridad se crea una nueva máquina virtual de Virtual Standby de la máquina virtual de Virtual Standby anterior y se agrega al plan de copia de seguridad. El proceso continúa hasta que el almacenamiento de ESX se queda sin espacio libre.

- Para la máquina virtual de la máquina virtual instantánea o de la recuperación asegurada de Linux, a menos que la migración del almacenamiento la convierta en una máquina virtual normal, Arcserve UDP no podrá realizar una copia de seguridad de la máquina virtual. La tarea de copia de seguridad se puede completar pero el punto de recuperación del que se ha hecho la copia de seguridad no se puede restaurar. Esta situación se produce debido a una limitación técnica de la implementación de la máquina virtual instantánea de Linux.

Solución

Si se desea hacer la copia de seguridad de las máquinas virtuales de Virtual Standby (VSB), de la máquina virtual instantánea (IVM) o de la recuperación asegurada (AR) o si las máquinas virtuales se convierten en máquinas virtuales independientes mediante la clonación o la migración del almacenamiento, siga los pasos indicados a continuación para las máquinas virtuales de vSphere e Hyper-V para permitir que la protección automática las detecte y las proteja.

Para la máquina virtual de vSphere

1. Inicie sesión en el cliente web de vSphere y busque la máquina virtual.
2. Apague la máquina virtual.
3. Haga clic con el botón secundario del ratón en la máquina virtual y seleccione Editar configuración en el menú.
4. Seleccione la ficha **Opciones de VM** ficha y expanda Avanzada.
5. Haga clic en **Editar configuración**.
6. En el cuadro de diálogo Parámetros de la configuración, busque el parámetro con cualquiera de los siguientes nombres:
   - VCM
   - UDP_IVM
   - UDP_ARVM
   - UDP_IVM_LINUX
   - UDP_VSBVM
   - UDP_ARVM_LINUX
   - UDP_ARIVM_LINUX
7. Borre el valor del parámetro y haga clic en **Aceptar** para guardar.

Para la máquina virtual de Hyper-V

1. Inicie sesión en el host de Hyper-V y abra el Gestor de Hyper-V.
2. Busque la máquina virtual.
3. Haga clic con el botón secundario del ratón en la máquina virtual y seleccione Configuración en el menú.
4. En el cuadro de diálogo Configuración, seleccione Nombre en el panel izquierdo.
5. Elimine todas las líneas que comienzan con las siguientes cadenas:
    - VCM
    - UDP_IVM
    - UDP_ARVM
    - UDP_IVM_LINUX
    - UDP_VSBVM
    - UDP_ARVM_LINUX
    - UDP_ARIVM_LINUX
6. Haga clic en **Aceptar** guardar.

Establecimiento del tamaño de bloque de lectura cuando se realiza la copia de seguridad de un archivo VMDK

Síntoma

En un determinado entorno, el rendimiento de la copia de seguridad de la máquina virtual de VMware se ve afectado por el tamaño de bloque de lectura cuando se realiza la copia de seguridad del archivo VMDK.

Solución

De forma predeterminada, el tamaño de bloque de lectura de VMDK es de 2 MB. Se puede modificar el tamaño.

Siga estos pasos:

1. Inicie sesión en el servidor proxy de la copia de seguridad sin agente.
2. Ejecute el comando *regedit* para abrir el editor del registro.
3. Vaya a la siguiente clave del registro:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll
4. Cree los valores del registro (DWORD) utilizando el siguiente nombre:

   ReadVirtualDiskBlockSizeKB
5. Especifique el valor que desea como tamaño de bloque de lectura (la unidad es kB).

Reserva de espacio de LUN heredada mientras se realiza el clon de LUN

Síntoma

Cuando se realiza el clon de LUN durante la copia de seguridad utilizando la instantánea de hardware, la reserva de espacio de forma predeterminada se hereda desde el LUN de origen.

Solución

Se debe utilizar la clave de registro que Arcserve UDP proporciona para desactivar la reserva de espacio. La clave de registro se encuentra en la ubicación siguiente:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

DisableLunSpaceReservation =1

Especifica que se han desactivado las reservas de espacio de LUN.

Nota: Esto solo es aplicable cuando se aplica la licencia de FlexClone.

Para obtener más información, consulte Considerations for NetApp iSCSI/FC Support for VMware.

Relacionados con Virtual Standby

En esta sección se incluyen los siguientes temas de solución de problemas relacionados con Virtual Standby:

- Sistema operativo no encontrado
- Las tareas de Virtual Standby no se pueden realizar debido a errores internos
- Error en las tareas de Virtual Standby al utilizar el modo de transporte hotadd
- Las tareas de Virtual Standby realizadas sobre sistemas Hyper-V producen errores
- Problema relacionado con el UUID de agente duplicado
- No se muestra la opción Finalizar recursos de EC2

Sistema operativo no encontrado

Válido en plataformas de Windows.

Síntoma:

El mensaje siguiente aparece cuando se produce un error en la operación de encendido de una máquina virtual de Virtual Standby:

Sistema operativo no encontrado.

Solución:

El comportamiento descrito se puede dar en máquinas virtuales que contienen dispositivos SCSI e IDE. Si se produce este problema, debe examinar cómo están configurados los discos en la máquina virtual y comprobar que la secuencia de arranque de la máquina virtual recuperada es la misma que la de la máquina virtual de origen. Si la secuencia de arranque es distinta, se debe actualizar la BIOS en la máquina virtual recuperada para que coincida con la de la máquina de origen.

Nota: Utilice (0:1) para representar el primer disco IDE.

Las tareas de Virtual Standby no se pueden realizar debido a errores internos

Válido en sistemas operativos Windows.

Síntoma 1:

Las tareas de Virtual Standby producen errores. Aparece un mensaje en el registro de actividad que indica alguna de las siguientes situaciones:

No se ha podido convertir el disco virtual

Se ha producido un error interno, póngase en contacto con Soporte técnico

Además, VDDK comunica el mensaje de error siguiente:

Error desconocido.

Solución 1:

Para corregir este problema, tenga en cuenta las siguientes soluciones:

- Las operaciones de conversión pueden fallar cuando no hay suficiente espacio libre en disco en el almacén de datos especificado en la política de Virtual Standby. VDDK devuelve el mensaje porque la API de VDDK no admite (actualmente) la funcionalidad para detectar la cantidad de espacio libre en disco en el almacén de datos. Para corregir este problema, libere la cantidad necesaria de espacio en disco en el almacén de datos original, de forma que se pueda completar la operación y, a continuación, vuelva a enviar la tarea.
- Las perturbaciones en la de red y el tráfico elevado pueden causar que se produzcan errores en las operaciones de conversión. Para corregir este problema, compruebe que el nodo de origen y el sistema del servidor de ESX o del servidor de vCenter se pueden comunicar el uno con el otro a través de la red, y a continuación vuelva a enviar una tarea.
- Se pueden producir errores en las tareas debido a la existencia de múltiples conexiones simultáneas compuestas por tareas de copia de seguridad o de recuperación de máquinas virtuales. Esto también incluye las conexiones de vSphere SDK a través del cliente VMware vSphere. Para corregir este problema, cierre todas las conexiones innecesarias y a continuación vuelva a enviar la tarea.

  Este problema está causado por una limitación de conectividad de VDDK de VMware. Se aplican los siguientes límites del protocolo de copia de archivos de red (NFC):

ESXi 5: Limitado por un búfer de transferencia para todas las conexiones de NFC y aplicado por el host; la suma de todo el almacenamiento búfer de la conexión de NFC en un host de ESXi no puede superar los 32 MB. 52 conexiones por servidor de vCenter, lo que incluye el límite por host.

Nota: no se pueden compartir las conexiones entre discos. Los límites máximos no se aplican a conexiones de tipo SAN y HotAdd. Si no se cierra adecuadamente el cliente NFC, las conexiones pueden permanecer abiertas durante diez minutos.

- Examine las secciones Tasks y Events del registro del cliente de VMware vSphere para conocer los errores internos para una máquina virtual específica. Corrija los errores internos y vuelva a enviar la tarea.

  Ejemplo: Otra aplicación u operación está utilizando el archivo VMDK. Para corregir este problema, libere el archivo y a continuación vuelva a enviar la tarea.

Síntoma 2:

Las tareas de Virtual Standby producen errores. Aparece un mensaje en el registro de actividad que indica alguna de las siguientes situaciones:

No se ha podido convertir el disco virtual

Se ha producido un error interno, póngase en contacto con Soporte técnico

Además, VDDK comunica el mensaje de error siguiente:

Se ha producido un error al abrir vmdk. No se ha encontrado el archivo

Solución 2:

Este problema puede surgir en estos casos:

- VDDK no ha procesado la instantánea correctamente.
- VDDK no ha suprimido una instantánea de forma manual o interna para la máquina virtual.

Para corregir este problema, vuelva e enviar la tarea. Si la tarea produce errores de nuevo, suprima la máquina virtual recuperada y vuelva a enviar la tarea.

Síntoma 3:

Las tareas de Virtual Standby producen errores. Aparece un mensaje en el registro de actividad que indica alguna de las siguientes situaciones:

No se puede aplicar <Nombre Plan> al nodo <Nombre Nodo>. El servicio web del Agente de Arcserve UDP en el conversor <Nombre Conversor> está ocupado. Inténtelo de nuevo más tarde.

Además, el archivo de registro de la Consola de UDP (ARCApp.log) comunica el mensaje de error siguiente:

[ERROR] deployVsbTask: Se ha producido un error al invocar la API del servicio web de D2D: Tiempo de espera excedido. javax.xml.ws.WebServiceException: java.-net.SocketTimeoutException: Tiempo de espera excedido de la lectura

Solución 3:

Este problema puede ocurrir debido a un tiempo de espera excedido. Para corregir este problema, realice los siguientes pasos:

1. Inicie sesión en la **Consola de UDP** con las credenciales adecuadas.
2. Abra la interfaz de la línea de comandos y ejecute el siguiente comando:

   regedit

   Se abre el registro.
3. Vaya a ***\SOFTWARE\Arcserve\Unified Data Protection\Engine\WebService***.
4. Compruebe que la clave **timeoutValue** existe. Si la clave no existe, créela manualmente.

   Agregue o modifique la clave tal y como se indica a continuación:

   - **Nombre de clave:** timeoutValue
   - **Valor:** <especifique el valor en minutos>. Por ejemplo, si desea establecer el valor del tiempo de espera en 20 minutos, especifique 20 como el valor de esta clave.
5. Salga de **regedit**.
6. Vaya a la carpeta de instalación de la **Consola de UDP**. Por ejemplo, *C:\Archivos de programa\Arcserve\Unified Data Protection\Management\Configuration*.
7. Abra el archivo **ConsoleConfiguration.xml** utilizando el Bloc de notas.
8. Busque el siguiente texto en la sección **<TimeoutConf>**:

   <webServiceRequestTimeout>600</webServiceRequestTimeout>
9. Modifique el valor de **webServiceRequestTimeout** en segundos. Por ejemplo, si desea establecer el valor del tiempo de espera en 20 minutos, especifique 1200 como el valor de esta clave.
10. **Guarde** el archivo y salga.
11. **Reinicie** el **servicio de gestión de la Consola de UDP** para permitir que se apliquen los valores de configuración.
12. Vuelva a implementar el plan y compruebe el resultado.

Error en las tareas de Virtual Standby al utilizar el modo de transporte hotadd

Válido en plataformas de Windows.

Síntoma:

Se produce un error en las operaciones de recuperación cuando se intenta recuperar datos mediante el modo de transporte hotadd. Aparecerá el siguiente mensaje en el registro de actividad:

Se ha producido un error desconocido. Póngase en contacto con el servicio de Soporte técnico.

Además, VDDK comunica el mensaje de error siguiente:

Error desconocido.

Solución:

Se produce un error en las operaciones de recuperación mediante el modo de transporte hotadd cuando los valores de configuración del disco no se han configurado correctamente.

Para configurar el disco, realice los siguientes pasos:

1. Conéctese al sistema de proxy de copia de seguridad mediante una cuenta con privilegios administrativos.

   Abra la línea de comandos de Windows.

2. En la línea de comandos, introduzca el siguiente comando:

   diskpart

   Pulse la tecla Intro.

   Escriba SAN y a continuación pulse la tecla Intro.

   Se mostrará la política de SAN actual.

3. Escriba el comando siguiente:

   SAN POLICY = OnlineAll

   Pulse la tecla Intro.

   La política de SAN está configurada de manera que no se montan automáticamente volúmenes hospedados de SAN.

4. Para borrar el atributo de sólo lectura del disco de SAN específico, seleccione el disco de la lista de discos y escriba el comando siguiente:

   attribute disk clear readonly

Pulse Intro

5. Escriba Salir y a continuación pulse la tecla Intro.

   El disco se habrá configurado y se podrá reenviar la tarea. Si se vuelve a producir un error en la tarea, monte manualmente los discos Hotadd mediante la gestión de discos en el sistema proxy.

   Para montar los discos manualmente, realice los siguientes pasos:

1. Conéctese al sistema de proxy de copia de seguridad mediante una cuenta con privilegios administrativos.

   Abra Panel de control de Windows y haga doble clic en Herramientas Administrativas.

   Aparece la ventana Herramientas administrativas.

2. De la lista de Favoritos, haga doble clic en Gestión de equipos.

   Aparecerá el cuadro de diálogo Gestión de equipos.

3. Expanda Almacenamiento y haga clic en Gestión de discos.

   Se mostrarán los discos.

4. Haga clic con el botón secundario en el disco que desea montar y haga clic en En línea.

   El disco se habrá montado y se podrá reenviar la tarea.

Las tareas de Virtual Standby realizadas sobre sistemas Hyper-V producen errores

Válido en sistemas operativos Windows.

Síntoma:

Aparecerá el siguiente mensaje en el registro de actividad:

La tarea de Virtual Standby no ha podido obtener la máquina virtual de Hyper-V.

Solución:

Las tareas de Virtual Standby generan errores en estos casos:

- El servicio Web de Virtual Standby no puede recuperar información sobre la máquina virtual desde el sistema Hyper-V. Se producen errores de comunicación entre el servidor de Arcserve UDP y el sistema Hyper-V cuando los servicios necesarios de Hyper-V no se están ejecutando en el sistema de Hyper-V.

  Solución: Compruebe que todos los servicios necesarios de Hyper-V se estén ejecutando en el sistema de Hyper-V.

- El sistema de Hyper-V no tiene suficiente espacio libre en disco para crear la máquina virtual de Virtual Standby o para crear una instantánea de la máquina virtual de Virtual Standby.

  Solución: Valore la posibilidad de volver a configurar el sistema de Hyper-V para permitir que haya suficiente espacio libre en disco en el volumen del sistema.

Nota: Si detecta otras posibles causas, póngase en contacto con el Soporte de Arcserve.

Problema relacionado con el UUID de agente duplicado

Síntoma:

Un controlador que existe en la Consola con el mismo UUID de agente debe sobrescribir el UUID del agente.

Solución:

1. En el equipo, ejecute *regedit*.
2. Vaya a la ubicación: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine*
3. Suprima los datos del valor NodeID.
4. Reinicie el servicio del Agente de Arcserve UDP.

Las modificaciones realizadas en la nube privada virtual en la tarea de Virtual Standby no se reflejan en Amazon EC2

Síntoma:

Después de realizar una tarea de Virtual Standby, si modifico la nube privada virtual (VPC) en la configuración de las redes de la tarea de Virtual Standby para utilizar una nube privada virtual diferente de Amazon para las tareas posteriores, las modificaciones no se actualizarán en Amazon EC2.

Solución

Amazon EC2 no permite la modificación de la nube privada virtual en la Consola de UDP después de ejecutar una tarea de Virtual Standby al menos una vez. Como solución alternativa, ahora Arcserve UDP permite finalizar la instancia anterior y crear una nueva instancia con los datos existentes de las sesiones anteriores.

Siga estos pasos:

1. Configure un plan de copia de seguridad con Virtual Standby para EC2 como tarea secundaria.
2. Realice algunas tareas correctas de VSB a AWS.
3. Modifique la configuración de VPC en la tarea de Virtual Standby [configuración de la red].

La configuración de VPC actualizada se muestra en la instancia después de la siguiente tarea de Virtual Standby realizada correctamente.

Notas:

- Se omite la instancia antigua creada en EC2 y se crea la nueva instancia con la VPC actualizada en EC2 para reflejar los cambios de la red.
- La nueva configuración de la red también se aplica a las instantáneas antiguas.

No se muestra la opción Finalizar recursos de EC2

Síntoma:

Cuando se configuran los nodos con un plan que tiene la tarea de Virtual Standby en EC2 en UDP 7.0 U1, UDP 7.0 o UDP 6.5 U4, y si se actualiza la consola a UDP 7.0 U2, la opción **Finalizar recursos de EC2** no se muestra para los nodos específicos.

Solución:

Haga clic en la opción **Modificar** para el plan relacionado y guárdelo.

Relacionados con la copia de puntos de recuperación

En esta sección se incluyen los siguientes temas de solución de problemas relacionados con la copia de puntos de recuperación:

- Congestión del ancho de banda con las tareas de copia del punto de recuperación a la nube
- Configuración del registro para la tarea de copia del punto de recuperación
- Tarea de combinación omitida

Configuración del registro para la tarea de copia del punto de recuperación

Síntoma

No se ejecuta la tarea de copia del punto de recuperación.

Solución

Se puede controlar el número de reintentos y el intervalo de tiempo entre ellos para la tarea de copia del punto de recuperación utilizando las claves de registro siguientes. La clave de registro se encuentra en el equipo en el que se ha instalado el Agente de UDP.

Reintento de la tarea de copia del punto de recuperación

La clave de registro se encuentra en el Agente de Arcserve UDP en la ubicación siguiente:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession\nodename1

Agregue una nueva clave tal y como se indica a continuación:

Nombre de la clave: MaxRetryCount

Tipo de clave: REG_DWORD

Valor: 1 como valor predeterminado y el valor máximo (10)

Nota: Esta actualización solo es aplicable a un nodo llamado nombrenodo1.

Para las tareas de copia del punto de recuperación en la nube, Arcserve UDP utiliza una ruta temporal que se puede configurar con las claves de registro para la ruta temporal.

Configuración de la ruta temporal

La clave de registro se encuentra en el servidor de Arcserve Backup, en la ubicación siguiente:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession

Nombre de la clave: LocalTempPath

Tipo de clave: REG_SZ

Nota: De forma predeterminada, se almacena en la ruta principal del producto Arcserve.

Congestión del ancho de banda con las tareas de copia del punto de recuperación a la nube

Síntoma

A menudo, la ejecución de las tareas de copia del punto de recuperación pueden ralentizar el equipo del Agente debido a la congestión del ancho de banda.

Solución

Arcserve le ayudará a definir un ancho de banda específico para las tareas de copia de punto de recuperación. Como resultado, incluso si el equipo tiene varias tareas en ejecución, con las tareas de copia del punto de recuperación, el ancho de banda se controla automáticamente en el equipo del Agente solo para las tareas de copia del punto de recuperación. Utilizando un proceso independiente llamado AFCRPBackend.exe para las tareas de copia del punto de recuperación, se puede configurar la calidad del servicio basada en la política para AFCRPBackend.exe y regular el ancho de banda saliente.

Siga estos pasos:

1. Escriba MMC en el cuadro Iniciar y pulse Intro.

   Se abre la Consola de gestión de Microsoft.

2. En la Consola MMC, pulse CTRL + M.

   Aparecerá el cuadro de diálogo Agregar o quitar complementos.

3. En el cuadro de diálogo Agregar o quitar complementos remotos, seleccione Editor de objetos de políticas del grupo bajo Complementos disponibles y haga clic en Agregar.

4. En el cuadro de diálogo Seleccionar objeto de política del grupo, deje la configuración predeterminada del Equipo local y haga clic en Finalizar.

5. Haga clic en Aceptar.

   Se cierra el cuadro de diálogo Agregar o quitar complementos.

6. En el panel izquierdo de la Consola MMC de Windows, expanda Equipo local, Configuración del equipo, Configuración de Windows y haga clic con el botón secundario del ratón en Calidad del servicio basada en políticas y seleccione Crear nueva política en el menú.

7. En la ventana de la calidad del servicio basada en políticas realice las siguientes opciones y haga clic en Siguiente:

   - Introduzca un nombre para la nueva política.

- Establezca el valor de DSCP en 0.

- Seleccione la casilla de verificación de la opción Especificar velocidad de salida del acelerador.

Nota: Se recomienda seleccionar MBps como opción.

8. Para que se aplique la política de la calidad del servicio, seleccione la casilla de verificación Solo aplicaciones con este nombre del archivo ejecutable, especifique la siguiente ruta del archivo .exe y haga clic en Siguiente:

   C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN\AFCRPBackend.exe

   Nota: AFCRPBackend.exe ayuda a garantizar que la restricción del ancho de banda solo sea aplicable a tareas de copia del punto de recuperación incluso si se están ejecutando varias tareas en el equipo del Agente.

9. Continúe con la configuración predeterminada hasta la última pantalla y haga clic en Finalizar.

Tarea de combinación omitida

Síntoma

- La tarea de combinación se ha omitido porque la sesión está bloqueada actualmente por la tarea de copia de punto de recuperación. Compruebe si hay alguna tarea de copia de punto de recuperación pendiente.
- La tarea de combinación se ha omitido porque la sesión está bloqueada actualmente por la tarea de copia de punto de recuperación a petición. La tarea de copia de punto de recuperación a petición está en ejecución o esperando a ejecutarse.

Solución

Para continuar con la tarea de combinación es necesario eliminar los archivos de bloqueo del destino de la copia de seguridad del nodo.

Ejecute la herramienta de supresión del bloqueo *C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN\AFDeleteLockTool.exe*.

Nota: Esta herramienta suprime todos los bloqueos relacionados con la copia de punto de recuperación (programada y ad-hoc) y la combinación se inicia inmediatamente. Las sesiones combinadas no estarán disponibles para que la copia de punto de recuperación realice la copia en el destino.

Uso:

AFDeleteLockTool.exe -path <RutaDestinoCopiaSeguridad> -user <NOMBREUSUARIO> -password <CONTRASEÑA> -type <crp/adhoccrp>

Observaciones:

-path: Especifica la ruta de destino de la copia de seguridad.

-type: Especifica el tipo de tarea para suprimir el bloqueo.

crp: Suprime el bloqueo relacionado con las tareas de copia de punto de recuperación programadas.

adhoccrp: Suprime el bloqueo relacionado con las tareas de copia de punto de recuperación ad-hoc.

-user: Especifica el nombre de usuario para el destino de la copia de seguridad.

-password: Especifica la contraseña para el destino de la copia de seguridad.

-path y -type son obligatorios.

-user y -password son opcionales. (Se deben proporcionar los dos juntos o se deben omitir los dos)

Ejemplos:

- Si solo se desea eliminar los bloqueos de las tareas de copia de punto de recuperación programadas, ejecute la herramienta tal y como se muestra a continuación:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -type crp

- Si solo se desea eliminar los bloqueos de las tareas de copia de punto de recuperación ad-hoc, ejecute la herramienta tal y como se muestra a continuación:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -user User123 -password "**********" -type crp

- Si se desea eliminar todos los bloqueos de la copia de punto de recuperación, ejecute la herramienta tal y como se muestra a continuación:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -user User123 -password "**********" -type crp -type adhoccrp

Información sobre informes de Arcserve UDP

En esta sección se incluyen los siguientes temas de solución de problemas relacionados con los informes de Arcserve UDP:

Cómo mostrar los gráficos para ver informes de Arcserve UDP

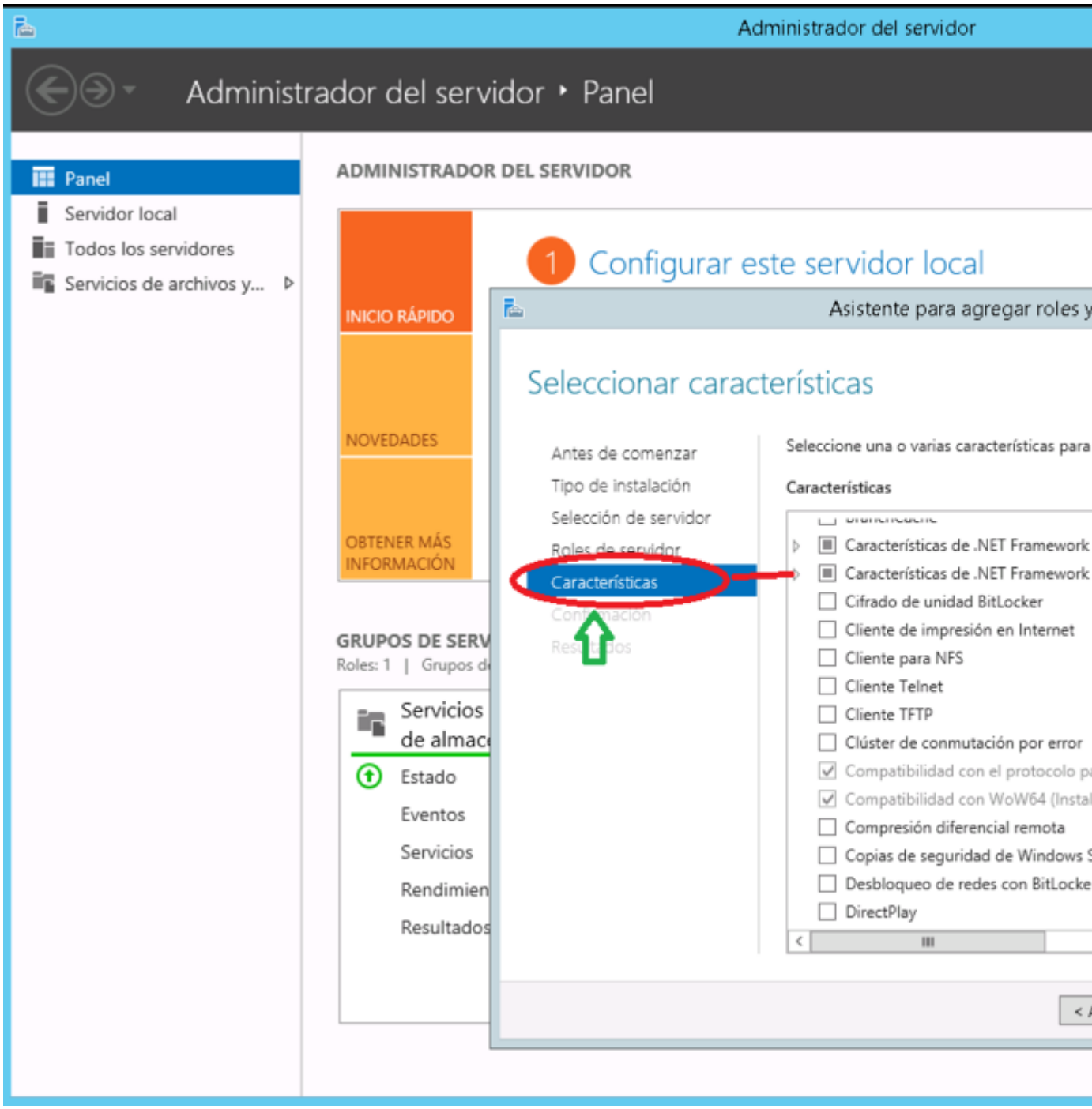
Cómo mostrar los gráficos para ver informes de Arcserve UDP

A veces cuando se desea ver los informes, es posible que los gráficos no puedan mostrarse. Complete el requisito previo siguiente para solucionar el problema de Windows 2012/2012r2.

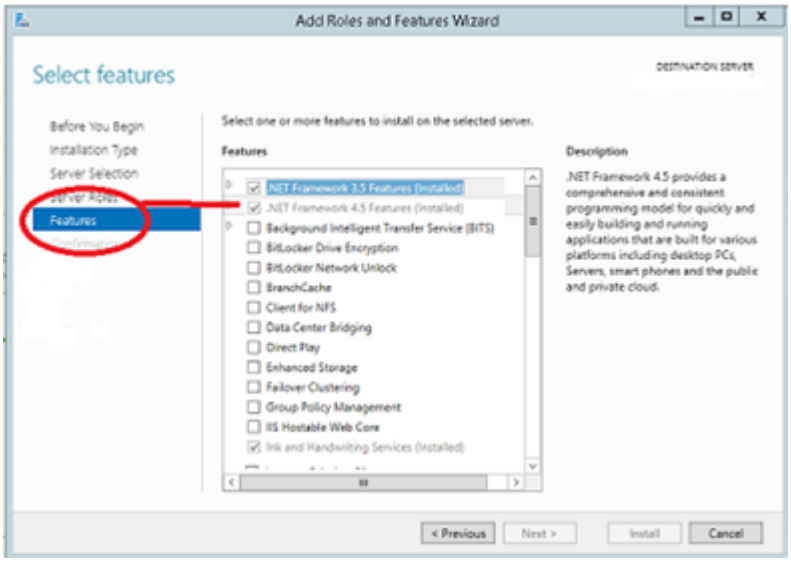
Para ver los gráficos, se debe instalar .NET 3.5 Framework o una versión posterior.

Para instalar .NET Framework, siga estos pasos:

1. Abra el Administrador de servidores.
2. En el cuadro de mandos, en la esquina superior derecha, haga clic en **Administrar** y, a continuación, seleccione la opción **Agregar roles y características**.



3. En el cuadro de diálogo Asistente para agregar roles y características, haga lo siguiente:
   a. En el panel izquierdo, haga clic en **Características**.
   b. En la ficha **Características**, seleccione la casilla de verificación **Características de .NET Framework 3.5 (instaladas)**.
   c. Haga clic en **Siguiente**.



4. En la pantalla Confirmar selecciones de instalación, haga clic en **instalar**.

   La instalación de .NET Framework se ha completado correctamente.

   Importante: Incluso después de implementar el requisito previo, si no se muestran los gráficos con las opciones **Imprimir/Correo electrónico/Guardar**, verifique si el Editor del registro tiene FCImgExportDll. Para verificar la DLL, vaya a la siguiente ruta:

   C:\Archivos de programa\Arcserve\Unified Data Protection\Management\BIN

   Para anular el registro y registrar FCImgExportDLL.dll, siga estos pasos:

   1. Vaya a la siguiente ruta en el símbolo del sistema:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319

   2. Para anular el registro de la DLL, ejecute el siguiente comando:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319>Regasm.exe /u "C:\Archivos de programa\Arcserve\Unified Data Protection\Management\BIN\FCImgExportDLL.dll"

   3. Para registrar la DLL, ejecute el siguiente comando:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319>Regasm.exe "C:\Archivos de programa\Arcserve\Unified Data Protection\Management\BIN\FCImgExportDLL.dll" /codebase

Relacionados con Microsoft Office 365 Exchange Online

Esta sección incluye los siguientes temas de solución de problemas relacionados con Microsoft Office 365 Exchange Online:

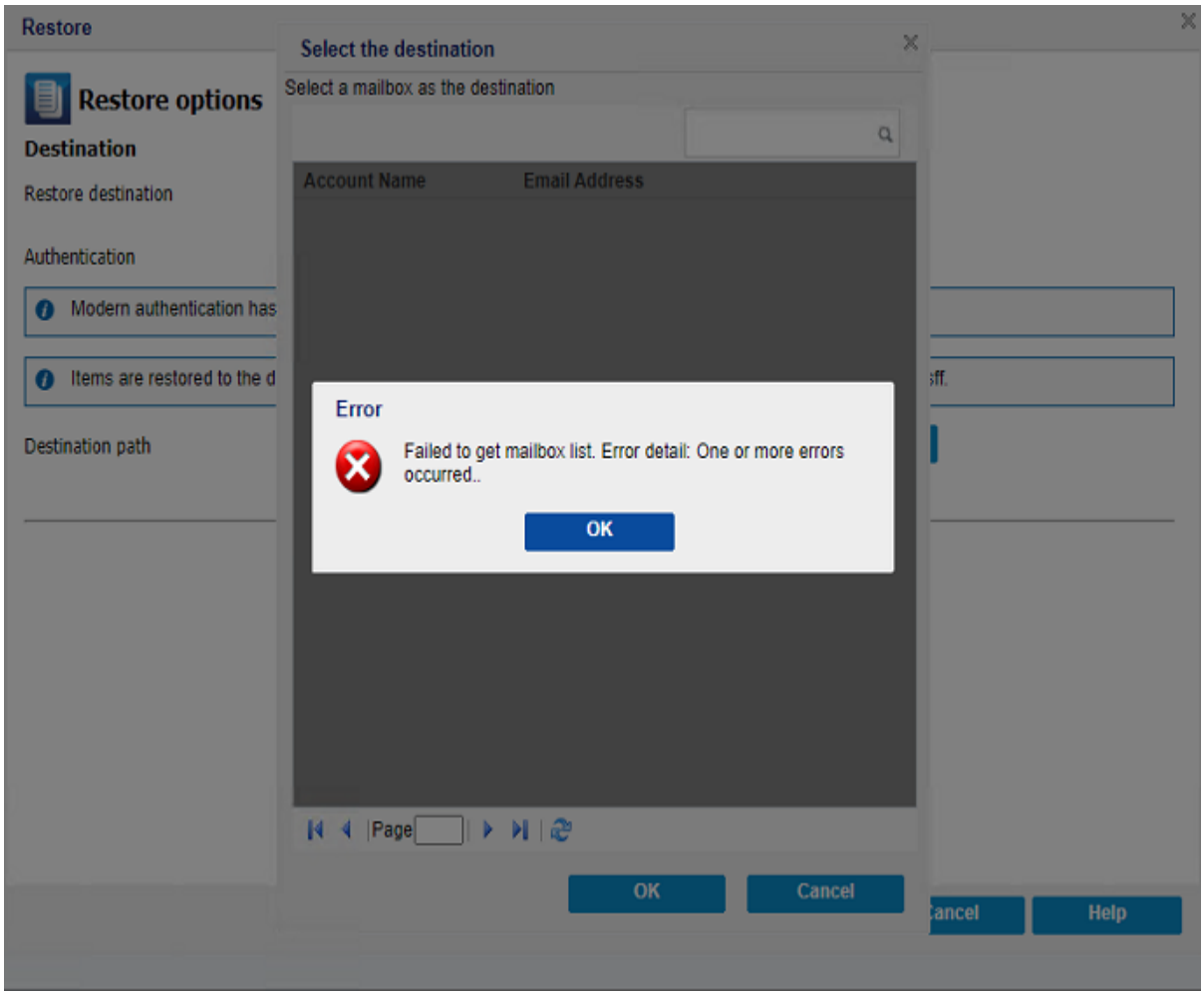
- No se puede ver la lista de buzones en el cuadro de diálogo *Seleccionar el destino*
- Acceso o permiso denegado para el grupo de Exchange Online

No se puede ver la lista de buzones en el cuadro de diálogo *Seleccionar el destino*

Síntoma:

Al definir las opciones de restauración, el cuadro de diálogo Seleccionar el destino no muestra la lista de buzones. Cuando se restauran los datos de correo a una ubicación alternativa utilizando la autenticación existente y se hace clic en el botón Examinar para seleccionar un destino, aparece el siguiente mensaje de error:

Se ha producido un error al obtener la lista de buzones. Detalle del error: Se han producido uno o más errores.



Solución:

Para solucionar este error, cargue un certificado válido en el portal de Azure en el ID de aplicación especificado. Para obtener más información, consulte Cómo utilizar el certificado autofirmado.

Acceso o permiso denegado para el grupo de Exchange Online

Síntoma:

Cuando no hay ningún buzón adjunto al grupo privado de Teams, aparece el siguiente mensaje de error:

Error en el buzón de copia de seguridad [abcd-pvt-group]: Acceso denegado

Solución:

Para solucionar esta incidencia, siga estos pasos:

1. Cree un buzón de correo compartido:
    a. Vaya a la página Inicio de sesión de Microsoft y, a continuación, inicie sesión en la cuenta de administrador de Microsoft Office 365.
    b. Vaya a la página del centro de administración de Exchange Online.
    c. En Panel, vaya a **destinatarios** > **compartido**.
    d. Haga clic en **+** para agregar o crear un buzón de correo compartido.
2. Establezca una contraseña y asigne la licencia de Office 365 para el buzón de correo compartido:
    a. Vuelva a la cuenta de administrador de Office 365.
    b. Vaya a **Usuarios** > **Usuarios activos** y, a continuación, seleccione el buzón de correo compartido.
    c. Establezca la contraseña y asigne la licencia de Office 365.
3. Agregue el buzón de correo compartido como miembro del grupo privado:
    a. Vaya a la página del centro de administración de Exchange Online y, a continuación, haga clic en **Grupos**.
    b. Seleccione el buzón de correo privado y, a continuación, haga clic en **Editar**.
    c. En la página Editar configuración, agregue el buzón de correo compartido como miembro del grupo y, a continuación, haga clic en **Guardar**.
4. Agregue el buzón de correo compartido para el administrador global:
    a. Vaya al portal de Azure.
    b. Vaya a la sección Roles y, a continuación, seleccione el rol Administrador global.
    c. Haga clic en **Agregar asignaciones**, seleccione el buzón de correo compartido y, a continuación, haga clic en **Guardar**.
5. En la Consola de UDP, actualice el nodo con la dirección de correo electrónico del buzón de correo compartido y, a continuación, vuelva a ejecutar la tarea de copia de seguridad.
6. Verifique que la tarea de copia de seguridad ha sido correcta.

Capítulo 13: Apéndice

Esta sección incluye los siguientes temas:

Herramienta de línea de comandos para el almacén de datos de deduplicación

La herramienta de línea de comandos (as_gddmgr.exe) permite comprobar la integridad de los datos en el nivel de punto de recuperación y en el nivel de almacén de datos para los almacenes de datos de deduplicación.

Se puede usar esta herramienta para volver a generar una base de datos de hash en caso de un error de la base de datos de hash. También puede utilizarla para realizar consultas y gestionar el borrado definitivo del servidor y la reclamación del disco de almacenes de datos de deduplicación.

La salida del comando se muestra en la consola de comandos de Windows. La herramienta también genera un archivo de registro en la carpeta Logs. Por ejemplo, as_gddmgr_2014-9-4_11-14-22-655.log es un archivo de registro que contiene todos los detalles.

Nota: Todos los comandos de la herramienta de línea de comandos (as_gddmgr.exe) también admiten el almacén de datos de volumen del GUID. Por ejemplo, *-scan VerifyAll <almacén de datos de volumen del GUID> [-Password <contraseña del almacén de datos>]*.

Ubicación:

Se puede encontrar as_gddmgr.exe en la carpeta Bin de la ruta de instalación de UDP.

Sintaxis:

as_gddmgr.exe

-Scan CheckRecoveryPoint <nombre almacén de datos> -Node [<Todo> |<nombre de nodo del Agente de UDP>] -RecoveryPoint [<más reciente>|<número punto de recuperación>] [-LogLevel <número>]

-Scan VerifyRefCount <nombre almacén datos> [-LogLevel <n>]

-Scan VerifyData <nombre almacén datos> [-Password <contraseña almacén datos>] [-LogLevel <n>]

-Scan VerifyAll <nombre almacén datos> [-Password <contraseña almacén datos>] [-LogLevel <n>]

-Scan RebuildHash <nombre almacén datos> [-NewHashPath <nueva ruta de hash>] [-LogLevel <n>]

-Scan RebuildHashWithIndexPath <ruta del índice> -NewHashPath <nueva ruta de hash> [-LogLevel <n>]

-Purge Start <nombre del almacén de datos>

-Purge Stop <nombre del almacén de datos>

-Purge Status <nombre del almacén de datos>

-Purge StartToReclaim <nombre del almacén de datos>

-Purge StartToIdentifyObsoletedData <nombre del almacén de datos>

Opciones:

CheckRecoveryPoint

Rehidrata los puntos de recuperación especificados como completos y, a continuación, comprueba la integridad de los datos.

Node <Todos> | <nombre nodo agente UDP>

Especifica el nombre del nodo del agente.

RecoveryPoint <Todos> | <número punto de recuperación>

Especifica el punto de recuperación cuya integridad debe comprobarse.

Password <contraseña almacén datos>

Especifica la contraseña del almacén de datos.

LogLevel <n>

Especifica el número del nivel de registro.

VerifyRefCount

Analiza los archivos de índice y de referencia para verificar el número de referencia registrado en la base de datos de hash. Antes de especificar esta opción, detenga manualmente el almacén de datos de deduplicación.

VerifyData

Analiza los archivos de datos y vuelve a generar, a continuación, las claves de hash comparando estos archivos con el de referencia. Antes de especificar esta opción, detenga manualmente el almacén de datos de deduplicación.

VerifyAll

Realiza las dos operaciones de VerifyRefCount y VerifyData. Antes de especificar esta opción, detenga manualmente el almacén de datos de deduplicación.

RebuildHash

Especifique el nombre del almacén de datos y, a continuación, vuelva a generar la base de datos de hash por índice de exploración y archivos de referencia. Antes de especificar esta opción, detenga manualmente el almacén de datos de deduplicación.

RebuildHashWithIndexPath

Especifique la ruta del índice de deduplicación y, a continuación, vuelva a generar la base de datos de hash por índice de exploración y archivos de referencia. Esta opción solo se utiliza cuando el almacén de datos no está presente en ningún servidor de puntos de recuperación.

Iniciar

Permite ejecutar el borrado definitivo y la reclamación del disco en paralelo con otras tareas de Arcserve UDP normales. La ejecución de un borrado definitivo en paralelo podría provocar una disminución del rendimiento de las tareas de Arcserve UDP normales.

Detener

Desactiva la ejecución del borrado definitivo y de la reclamación del disco en paralelo con otras tareas de Arcserve UDP normales.

Estado

Consulta el estado de la reclamación del disco o del borrado definitivo.

StartToReclaim

Permite ejecutar el borrado definitivo y la reclamación del disco en paralelo con otras tareas de Arcserve UDP normales. Esta opción omite la fase de identificación de datos en desuso que identifica el bloque de datos obsoleto y, a continuación, inicia directamente la fase de reclamación del disco, que libera espacio en disco. El inconveniente de esta opción radica en que puede disminuir la eficacia de la reclamación del disco debido a que la fase de identificación de datos en desuso puede identificar más bloques de datos obsoletos en los archivos de datos, pero la recuperación del disco no espera a que la fase de identificación de datos en desuso termine. Además, la ejecución del borrado definitivo en paralelo podría provocar una disminución del rendimiento de las tareas de Arcserve UDP normales.

StartToIdentifyObsoletedData

Permite ejecutar el borrado definitivo y la reclamación del disco en paralelo con otras tareas de Arcserve UDP normales. Esta opción inicia la fase de identificación de datos en desuso. La opción es útil si el usuario desea omitir la fase de reclamación del disco actual.

Nota: Tenga en cuenta que las opciones siguientes podrían ejecutarse durante mucho tiempo porque la operación analiza muchos archivos en el almacén de datos de deduplicación.

- VerifyRefCount
- VerifyData
- VerifyAll

- RebuildHash
- RebuildHashWithIndexPath

Ejemplos:

as_gddmgr.exe -Scan CheckRecoveryPoint GDDDataStore1 -Node myComputer -RecoveryPoint 18

as_gddmgr.exe -Scan CheckRecoveryPoint GDDDataStore1 -Node All -RecoveryPoint Latest

as_gddmgr.exe -Scan VerifyRefCount GDDDataStore1

as_gddmgr.exe -Scan VerifyData GDDDataStore1 -Password 123

as_gddmgr.exe -Scan VerifyAll GDDDataStore1

as_gddmgr.exe -Scan RebuildHash GDDDataStore1

as_gddmgr.exe -Scan RebuildHash GDDDataStore1 -NewHashPath C:\NewHashPath

as_gddmgr.exe -Scan RebuildHashWithIndexPath D:\GDDDataStore\Index -NewHashPath D:\NewHashPath

as_gddmgr.exe -Purge Start GDDDataStore1

as_gddmgr.exe -Purge Stop GDDDataStore1

as_gddmgr.exe -Purge Status GDDDataStore1

as_gddmgr.exe -Purge StartToReclaim GDDDataStore1

as_gddmgr.exe -Purge StartToIdentifyObsoletedData GDDDataStore1

Cómo mostrar la opción Comprobación del punto de recuperación

A partir de Arcserve UDP 7.0, se oculta la función de comprobación del punto de recuperación de forma predeterminada en el asistente del plan. Se recomienda utilizar la tarea de recuperación asegurada para detectar posibles problemas en los datos. Se recomienda utilizar la tarea de recuperación asegurada para detectar posibles problemas en los datos. Para obtener más detalles, consulte la sección Cómo configurar la recuperación asegurada. En caso necesario, todavía se puede utilizar esta opción para realizar la comprobación de los datos y verlos en el asistente del plan.

Siga estos pasos:

1. Inicie sesión en la Consola de UDP.
2. Vaya a la carpeta de instalación de la Consola de UDP. Por ejemplo, *C:\Archivos de programa\Arcserve\Unified Data Protection\Management\Configuration*.
3. Abra el archivo ConsoleConfiguration.xml en cualquier editor de texto.
4. Busque el siguiente texto en la sección <TimeoutConf>:

   <recoveryPointCheck>false</recoveryPointCheck>
5. Modifique el valor de false a true.
6. Guarde el archivo y salga.
7. Reinicie el servicio de gestión de la Consola de UDP para permitir que se aplique el valor de configuración.

   Nota: La versión de Arcserve UDP se actualiza desde la versión anterior y esta opción ya está seleccionada en un plan y no está oculta de forma predeterminada.

   Esta opción le permite detectar problemas de corrupción de datos verificando el sistema de archivos de los volúmenes. Cuando la tarea de copia de seguridad se completa, Arcserve UDP monta el punto de recuperación y ejecuta el comando chkdsk de Windows. Si el comando chkdsk detecta un error, la siguiente tarea de copia de seguridad se convierte en una tarea de copia de seguridad de verificación. Esta opción se aplica tanto en máquinas virtuales de VMware como en máquinas virtuales de Hyper-V con el sistema operativo invitado de Windows. Revise las siguientes consideraciones antes de activar esta opción:

   - No se admiten los siguientes tipos de volumen y la **Comprobación del punto de recuperación** los ignora:

- El volumen cuyo tipo de sistema de archivos no es NTFS.
- El volumen cuyo tipo es seleccionado con paridad.
- El volumen que se encuentra en una agrupación de almacenamiento.

- El comando chkdsk no puede detectar todos los problemas del sistema de archivos. La comprobación del punto de recuperación puede pasar, pero el punto de recuperación todavía puede estar corrupto.
- Dependiendo del tamaño del sistema de archivos del sistema operativo invitado, el comando chkdsk puede tardar más tiempo en ejecutarse. El comando chkdsk utiliza una gran cantidad de memoria del sistema en el servidor proxy de copia de seguridad y afecta al rendimiento del servidor proxy. Esto da como resultado que la tarea de copia de seguridad tarde más tiempo en completarse. *En el peor de los casos, es posible que se agote la memoria del sistema del servidor proxy de copia de seguridad y que el servidor no responda; especialmente cuando haya varias tareas de copia de seguridad simultáneas o cuando se estén comprobando grandes volúmenes de datos.* La comprobación de puntos de recuperación puede controlar el uso de la memoria del sistema y, si el uso de la memoria alcanza un umbral, puede suspenderse a sí misma durante un tiempo y liberar así parte de la memoria del sistema. Sin embargo, se recomienda desactivar esta opción a menos que sea necesaria o se disponga de un servidor proxy de copia de seguridad de alto rendimiento. De forma alternativa, se puede distribuir la carga en varios servidores proxy mediante la creación de varios planes y especificar un servidor proxy distinto para cada plan.
- Si la copia de seguridad es coherente con los bloqueos, hay muchas probabilidades de que chkdsk detectará problemas (debido a la naturaleza de una copia de seguridad coherente con los bloqueos). Como práctica recomendada, no active esta opción para una copia de seguridad coherente con los bloqueos.
- Si se desea activar la opción Comprobación del punto de recuperación pero no se desea que la siguiente tarea de copia de seguridad se convierta en una tarea de copia de seguridad de verificación, cree un valor DWORD llamado CheckRecoveryPointIgnoreError en el registro del servidor proxy y establezca el valor de DWORD en 1. Cree el valor DWORD en la ubicación siguiente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

  El valor DWORD se puede aplicar a todas las tareas de copia de seguridad que se ejecutan en el servidor proxy actual. Si se desea controlar el com-

portamiento de una máquina virtual específica, se puede establecer el valor en la ubicación siguiente:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM GUID>

Nota: Si se agrega la clave de registro en el registro tanto en el nivel de la máquina virtual como en el nivel del proxy, la configuración del registro en el nivel de la máquina virtual tiene prioridad sobre la configuración del registro en el nivel del servidor proxy.

- Si desea que se produzca un error de copia de seguridad si la comprobación de los puntos de recuperación detecta problemas (de manera que se le advierta de problemas de datos de manera inmediata), cree un valor DWORD denominado CheckRecoveryPointDontFailJob en el registro del servidor proxy y establezca el valor DWORD en 0. Cree el valor DWORD en la ubicación siguiente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

  El valor DWORD se puede aplicar a todas las tareas de copia de seguridad que se ejecutan en el servidor proxy actual. Si se desea controlar el comportamiento de una máquina virtual específica, se puede establecer el valor en la ubicación siguiente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM GUID>.

  Nota: Si se agrega la clave de registro en el registro tanto en el nivel de la máquina virtual como en el nivel del proxy, la configuración del registro en el nivel de la máquina virtual tiene prioridad sobre la configuración del registro en el nivel del servidor proxy.

Cómo aplicar una versión diferente de VDDK distinta a la incorporada en Arcserve UDP

VMware Virtual Disk Development Kit (VDDK) 6.7.1 está integrado Arcserve UDP 7.0. Al mismo tiempo, Arcserve UDP 7.0 es compatible con VDDK 5.5. Si desea realizar la tarea de Virtual Standby, de máquina virtual instantánea o de recuperación asegurada en VMware 5.0 o 5.1, utilice VDDK 5.5 en lugar de VDDK 6.7.1.

Importante: Arcserve solo certifica VDDK 6.7.1 y 5.5. No se garantiza que otras versiones de VDDK funcionen con Arcserve UDP versión 7.0.

Para modificar el VDDK manualmente, siga los siguientes procedimientos:

- Modificación del VDDK para la copia de seguridad de Virtual Standby (VSB)
- Modificación del VDDK para la copia de seguridad basada en el host (HBBU)

Modificación del VDDK manualmente para la copia de seguridad de Virtual Standby (VSB)

Se puede modificar el VDDK manualmente o mediante un archivo por lotes de Windows. Este tema explica los procedimientos para ambas opciones.

Consideraciones:

- Para la máquina virtual instantánea y para la prueba de recuperación asegurada, se debe realizar esta acción en el servidor proxy o en el servidor de recuperación.
- Para Virtual Standby a VMware, utilice un servidor dedicado del Agente como controlador de Virtual Standby y configure la tarea de Virtual Standby en modo proxy. A continuación, cambie manualmente el VDDK a la versión 5.5 en el servidor de controlador de Virtual Standby.
- Si la tarea de Virtual Standby está configurada en un plan MSP o en un plan entre sitios, cambie el VDDK que se encuentra en el servidor de puntos de recuperación porque el servidor del controlador no está presente. Como resultado, este servidor de puntos de recuperación no está disponible para utilizarlo como un servidor proxy para la tarea de copia de seguridad sin agente basada en el host.

Para modificar el VDDK manualmente, realice los siguientes pasos:

1. Inicie sesión en el equipo donde está instalado el Agente de Arcserve UDP mediante una cuenta administrativa o una cuenta que tiene privilegios

administrativos.

2. Cambie el nombre de la carpeta *VDDK* a VDDK6.7.
3. Cambie el nombre de la carpeta *VDDK5.5* a VDDK desde la siguiente ubicación predeterminada:

   C:\Archivos de programa\Arcserve\Unified Data Protection\engine\BIN

   Nota: La ubicación de la carpeta BIN puede variar dependiendo de donde se haya instalado el Agente de Arcserve UDP.
4. Ejecute el siguiente comando para comprobar el estado del servicio:

   Nota: Se debe suprimir el servicio solo cuando no esté en estado de ejecución.

   sc query vstor2-mntapi20-shared

   Si el servicio no existe, suprímalo utilizando el siguiente paso. Si se está ejecutando el servicio, antes de suprimirlo utilizando el siguiente paso, ejecute el comando siguiente para detenerlo:

   sc stop vstor2-mntapi20-shared
5. Ejecute el siguiente comando para suprimir el servicio:

   sc delete vstor2-mntapi20-shared
6. Ejecute el siguiente comando para comprobar si el servicio se ha suprimido correctamente:

   sc query vstor2-mntapi20-shared

   Nota: Si el estado del servicio es STOP_PENDING, reinicie el equipo.

   Para modificar el VDDK mediante un archivo por lotes de Windows, siga estos pasos:

1. Inicie sesión en el equipo donde está instalado el Agente de Arcserve UDP mediante una cuenta administrativa o una cuenta que tiene privilegios administrativos.
2. Inicie la herramienta de utilidad *ChangeToVDDK55.bat* desde la ubicación predeterminada siguiente:

   C:\Archivos de programa\Arcserve\Unified Data Protection\engine\BIN

   Nota: La ubicación de la carpeta BIN puede variar dependiendo de donde se haya instalado el Agente de Arcserve UDP.

   VDDK 5.5 se instala después de iniciar una nueva tarea.

Modificación del VDDK manualmente para la copia de seguridad basada en el host (HBBU)

Se puede modificar manualmente el VDDK para la copia de seguridad basada en el host (HBBU).

Modifique VDDK 6.7 para realizar la copia de seguridad de vSphere 5.5 o posterior:

Siga estos pasos:

1. Descargue VDDK del sitio web de VMware.
2. Extraiga todos los archivos en una carpeta temporal.
3. Busque la carpeta llamada ***bin*** que está disponible en la siguiente ruta y cambie el nombre de dicha carpeta (por ejemplo, *bin_old*):

   <Ruta de instalación de Arcserve UDP>\Engine\BIN\VDDK\BIN\VDDK64\

   Ejemplo: C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\VDDK\BIN\VDDK64\bin
4. Busque la carpeta llamada ***bin*** en los archivos extraídos en la carpeta temporal y cópiela en la siguiente ruta:

   <Ruta de instalación de Arcserve UDP>\Engine\BIN\VDDK\BIN\VDDK64\.

   El VDDK se ha modificado correctamente.

Modifique VDDK 5.5 para realizar la copia de seguridad de vSphere 5.0 y 5.1:

Siga estos pasos:

1. Descargue VDDK del sitio web de VMware.
2. Extraiga todos los archivos en una carpeta temporal.
3. Busque la carpeta llamada ***bin*** que está disponible en la siguiente ruta y cambie el nombre de dicha carpeta (por ejemplo, *bin_old*):

   <Ruta de instalación de Arcserve UDP>\Engine\BIN\VDDK5.5\BIN\VDDK64\.

   Ejemplo: C:\Archivos de programa\Arcserve\Unified Data Protection\Engine\BIN\VDDK5.5\BIN\VDDK64\
4. Busque la carpeta llamada ***bin*** en los archivos extraídos en la carpeta temporal y cópiela en la siguiente ruta:

   <Ruta de instalación de Arcserve UDP>\Engine\BIN\VDDK5.5\BIN\VDDK64\.

   El VDDK se ha modificado correctamente.

Cómo migrar datos de copia de seguridad de Arcserve D2D r16.5 de dos servidores con el mismo nombre de host a un almacén de datos del servidor de puntos de recuperación

Existen dos servidores con el mismo nombre de host, pero distinto nombre DNS FQDN y se utiliza Arcserve D2D r16.5 para protegerlos. Si desea migrar los datos al almacén de datos del servidor de puntos de recuperación de Arcserve UDP, siga estos pasos:

1. Detenga el servicio de Arcserve D2D en el servidor 1.
2. Mediante la tarea de JumpStart de Arcserve UDP, migre los datos del servidor 1 al almacén de datos del servidor de puntos de recuperación.
3. Actualice el Agente de Arcserve UDP en el servidor 1.
4. Cree un plan (o use uno existente) para proteger el servidor 1 y elija el mismo almacén de datos del servidor de puntos de recuperación como destino de la copia de seguridad.
5. Implemente el plan.
6. Detenga el servicio de Arcserve D2D en el servidor 2.
7. Mediante la tarea de JumpStart de Arcserve UDP, migre los datos del servidor 2 al almacén de datos del servidor de puntos de recuperación.
8. En el servidor de puntos de recuperación, vaya a la carpeta de destino de la copia de seguridad del almacén de datos y encuentre la carpeta para el servidor 2 buscando el nombre de host de dicho servidor.

   Por ejemplo, si el nombre de host del servidor 2 es “MiServidor2”, el nombre de la carpeta será “MiServidor2”.
9. Actualice el Agente de Arcserve UDP en el servidor 2.
10. En el servidor 2, inicie al Agente de UDP si no se ha iniciado.
11. Abra el registro (en cualquier servidor específico) y busque la siguiente clave:

    HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine”
12. Tenga en cuenta el valor de “NodeID”.

    El valor es un ID único en formato de GUID, como “e856e0ba-66d7-4da5-8b98-2250173e349a”.

13. En el servidor de puntos de recuperación, busque la carpeta de destino de la copia de seguridad del servidor 2 y actualice el ID del nodo a **<nombre_carpeta> [valor NodeID]**.

    Ejemplo: MiServidor2[e856e0ba-66d7-4da5-8b98-2250173e349a]

14. Cree un plan (o use uno existente) para proteger el servidor 2 y elija el mismo almacén de datos del servidor de puntos de recuperación como destino de la copia de seguridad.

15. Implemente el plan.

Cómo implementar Arcserve UDP en Microsoft Azure

Se puede implementar Arcserve UDP en Microsoft Azure cuando se utiliza Arcserve Unified Data Protection v6.5 Actualización 2 o posterior. La función ayuda a implementar las máquinas de Virtual Standby en Microsoft Azure y a proteger los datos. Una máquina de Virtual Standby se crea en Microsoft Azure con los datos relacionados en función de los puntos de recuperación de la copia de seguridad local.

Virtual Standby convierte los puntos de recuperación en formatos de máquina virtual en Microsoft Azure y prepara una instantánea para poder recuperar fácilmente los datos cuando sea necesario.

Esta función también proporciona la capacidad de alta disponibilidad garantizando que la máquina virtual toma el control inmediatamente cuando se produce un error en el equipo de origen. La máquina de Virtual Standby se crea convirtiendo los puntos de recuperación en un formato de máquina virtual de Azure.

¿Qué hacer a continuación?

1. Funcionamiento del flujo del proceso
2. Prácticas recomendadas
3. Consideraciones
4. Planificación de la implementación
5. Implementación de Arcserve UDP en Microsoft Azure

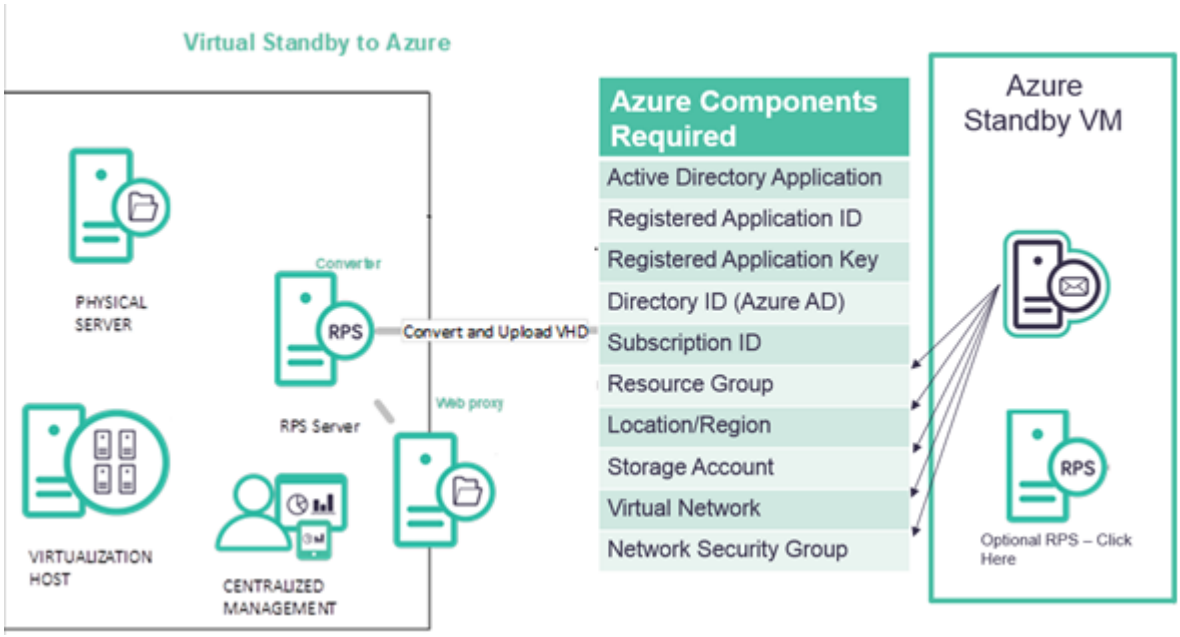
Funcionamiento del flujo del proceso

Arcserve UDP es compatible con las máquinas virtuales de Virtual Standby en Microsoft Azure. Si ya ha implementado la solución de protección de datos localmente, podrá implementar Arcserve UDP en Microsoft Azure.

La solución local está formada por la Consola de Arcserve UDP y el servidor de puntos de recuperación de Arcserve UDP. Se puede realizar la copia de seguridad de

sistemas de Windows en el servidor de puntos de recuperación local. Se puede crear un plan en la Consola de Arcserve UDP para realizar la copia de seguridad de los datos en el servidor de puntos de recuperación local y, a continuación, realizar la tarea de Virtual Standby. La función de Virtual Standby controla el latido del nodo de origen. Si el nodo de origen está desactivado, la máquina virtual en Azure toma el control.

La siguiente imagen muestra el flujo del proceso de Arcserve UDP para Microsoft Azure:



Consideraciones

Revise las siguientes consideraciones antes de implementar Arcserve UDP en Microsoft Azure:

Nota: Para obtener más información sobre las prácticas recomendadas, consulte Implementación de Arcserve UDP en Microsoft Azure.

- En Microsoft Azure, cualquier archivo de VHD único no puede tener un disco del sistema que tenga más de 2048 GB ni que los datos del disco tengan un tamaño mayor de 4095 GB. En Arcserve UDP Virtual Standby, el origen no puede tener un disco del sistema que sea mayor de 2048 GB ni datos del disco que tengan un tamaño mayor de 4095 GB.
- La máquina virtual de Microsoft Azure y Arcserve UDP VSB solo admiten el sistema operativo Windows 2008 R2 o posterior.

- Arcserve UDP no admite la creación de la máquina virtual clásica como máquina virtual de Virtual Standby.
- La máquina virtual de Microsoft Azure necesita que el volumen del sistema y el volumen de arranque estén en el mismo disco.
- Microsoft Azure no admite el inicio del equipo desde el sistema UEFI.
- Microsoft Azure no es compatible con que el equipo de origen sea el servidor Hyper-V.
- Arcserve UDP Virtual Standby no es compatible con el disco del sistema dinámico para el equipo de origen.
- Arcserve UDP en Microsoft Azure solo admite nodos de Windows.

Planificación de la implementación de Arcserve UDP en Microsoft Azure

Debe completar las siguientes tareas antes de implementar Arcserve UDP en Microsoft Azure:

1. Revisión de los requisitos previos
2. Preparación de una cuenta de la nube en Microsoft Azure
3. Preparación de los recursos de Microsoft Azure

Requisitos previos

Revise los siguientes requisitos previos para Arcserve UDP y el servidor de puntos de recuperación antes de implementar Arcserve UDP en Microsoft Azure:

- Revise la Matriz de compatibilidad para obtener los sistemas operativos compatibles, las bases de datos y los exploradores.
- Prepare los servidores de antemano para implementarlos como la Consola de Arcserve UDP y el servidor de puntos de recuperación.
- Los servidores de cada componente deben cumplir con los siguientes requisitos del sistema:
  - **Servidor:** Windows Server 2008 R2 o posterior
  - **CPU:** 4 núcleos como mínimo de 2,7 GHz
  - **Espacio en disco:** 40 GB para la instalación del sistema operativo
  - **RAM:** 8 GB como mínimo

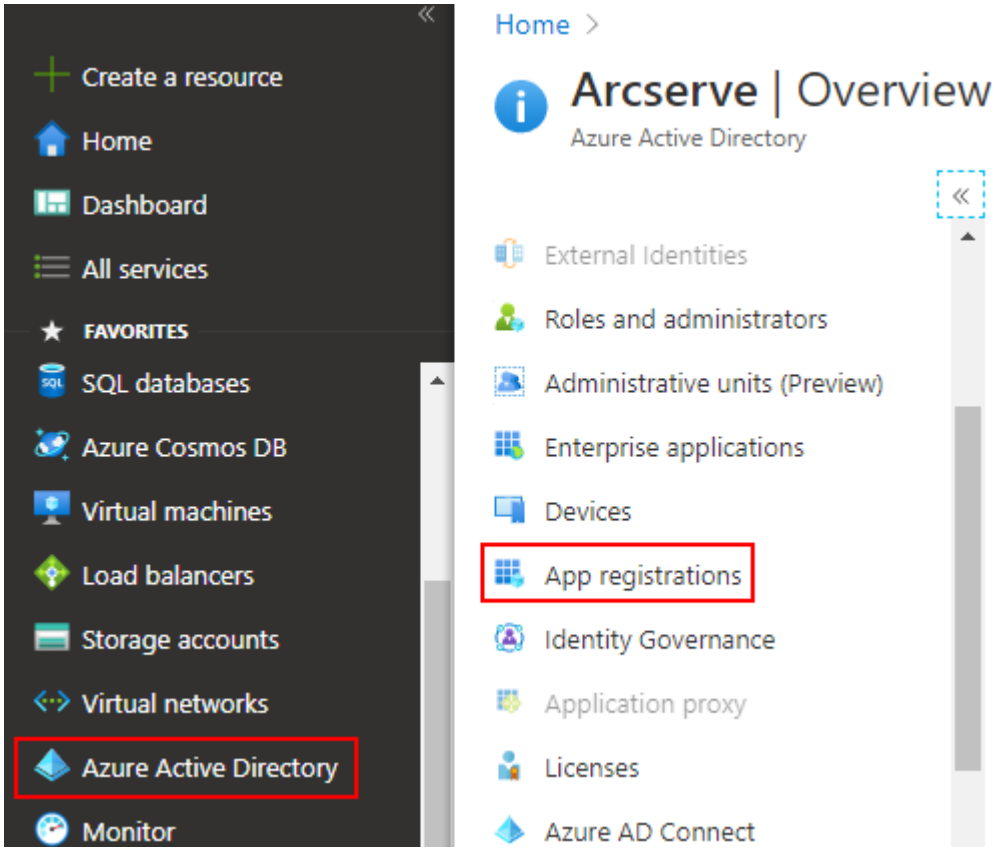
- **Almacenamiento de la copia de seguridad para el servidor de puntos de recuperación:** En función del tamaño de los datos de origen

Preparación de una cuenta de la nube en Microsoft Azure

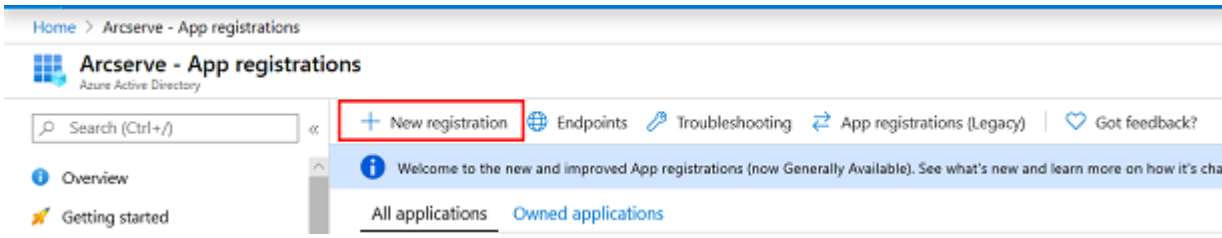
Esta sección proporciona información sobre cómo crear una cuenta de la nube en Microsoft Azure.

Siga estos pasos:

1. Realice los pasos siguientes para registrar la aplicación Azure Active Directory que Arcserve UDP utiliza para comunicarse con Microsoft Azure:
   a. Inicie sesión en el Portal de Azure.
   b. En el panel izquierdo, seleccione **Azure Active Directory** y, a continuación, haga clic en **Registros de aplicaciones**.

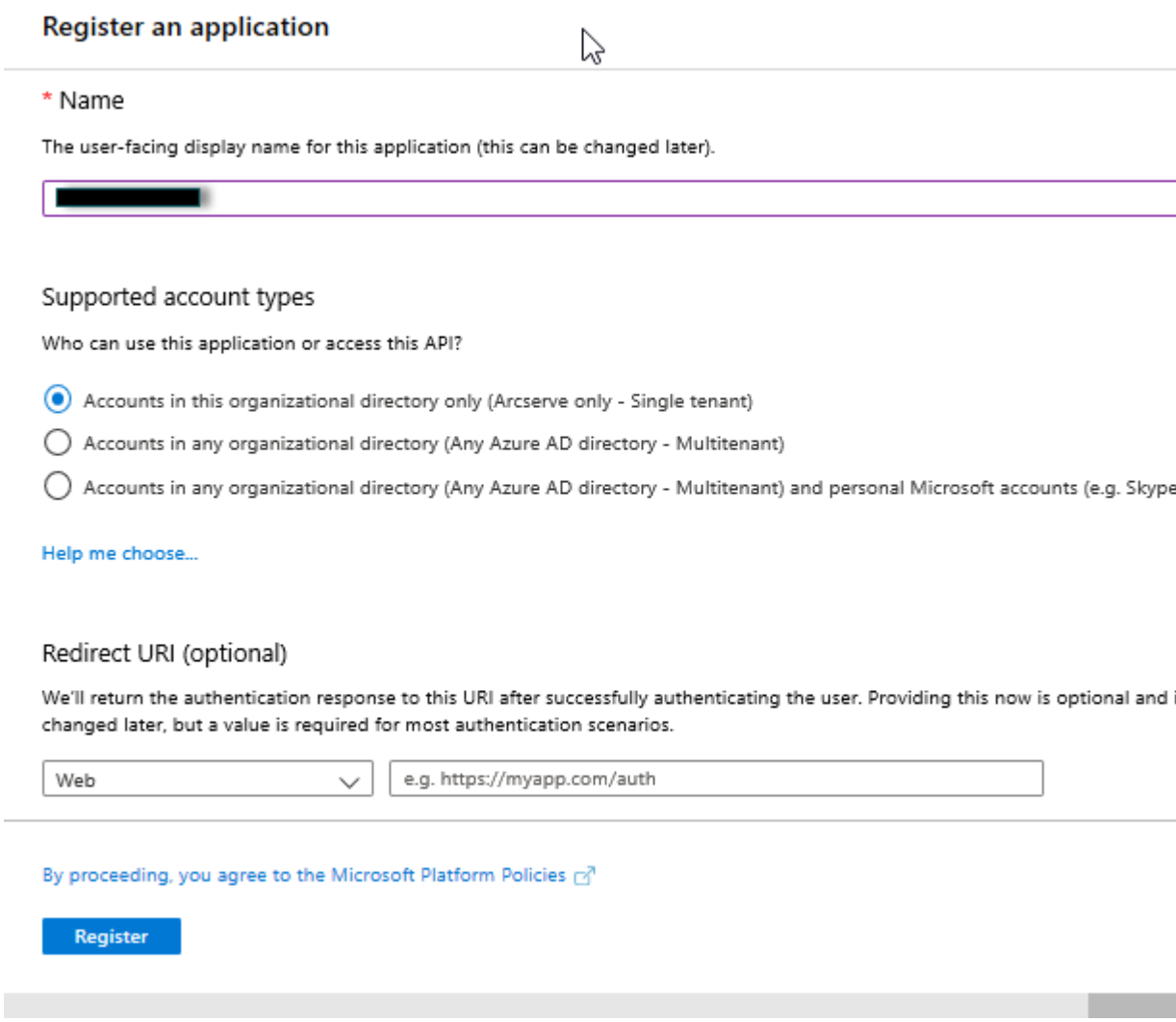


   c. En la página Registro de aplicaciones Arcserve, haga clic en **Nuevo registro**.

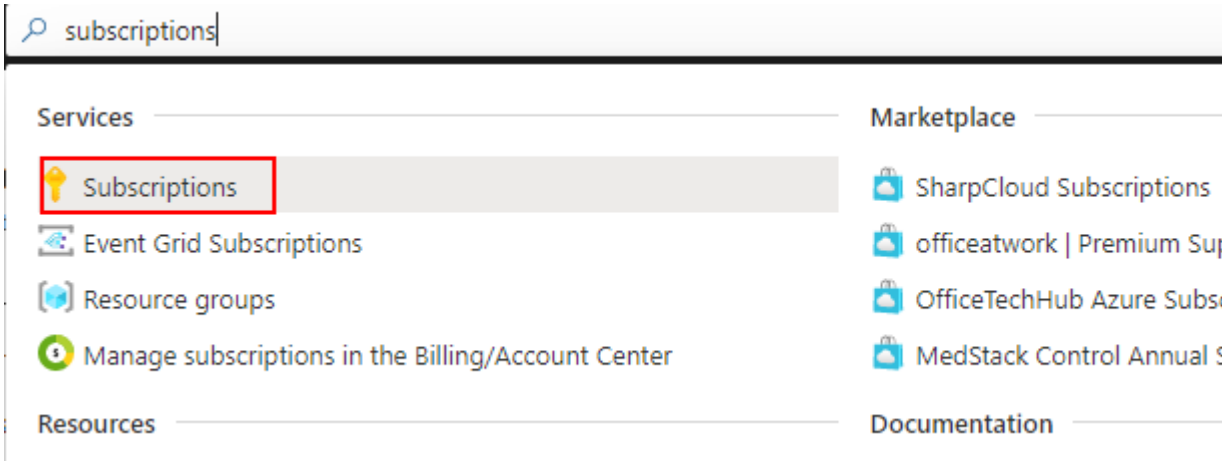


d. En la página Registrar una aplicación, haga lo siguiente y, a continuación, haga clic en **Registrar**.

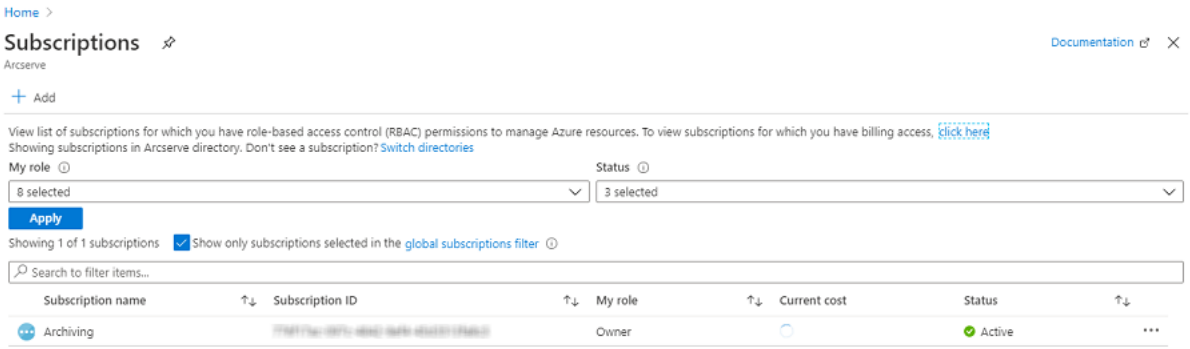
   - Nombre: Introduzca un nombre para la aplicación.
   - Tipos de cuenta compatibles: Seleccione un tipo de cuenta compatible, que determinará quién puede utilizar la aplicación.
   - URI de redirección (opcional): Seleccione el **cliente web o público (dispositivo móvil y escritorio)** para el tipo de aplicación que está creando y, a continuación, introduzca el URI de redirección para la aplicación.



e. En la barra de búsqueda, escriba suscripciones y, a continuación, haga clic en **Suscripciones**.

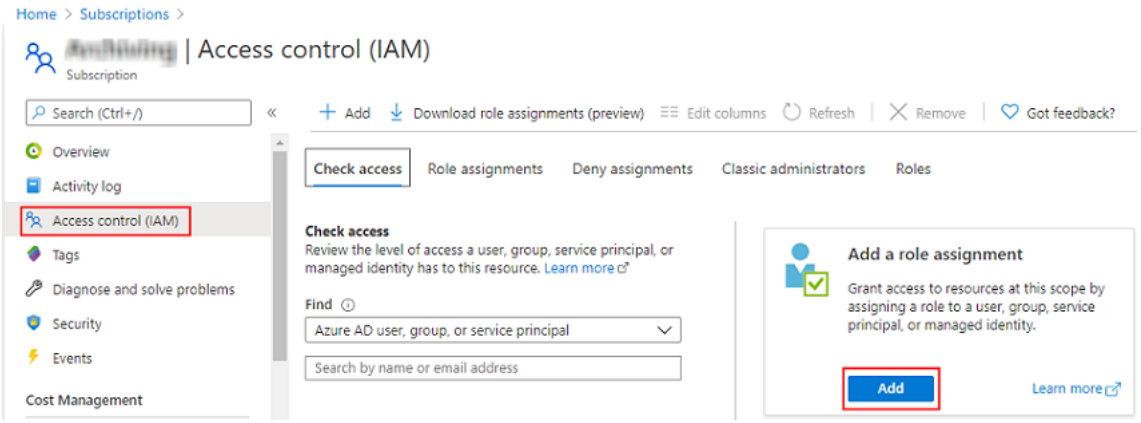


f. En las páginas de Suscripciones, seleccione la suscripción para su aplicación.



Nota: Si la lista de suscripciones no muestra la suscripción necesaria, seleccione el **filtro de suscripciones globales**. Asegúrese de que se ha seleccionado la suscripción que desea para el portal.

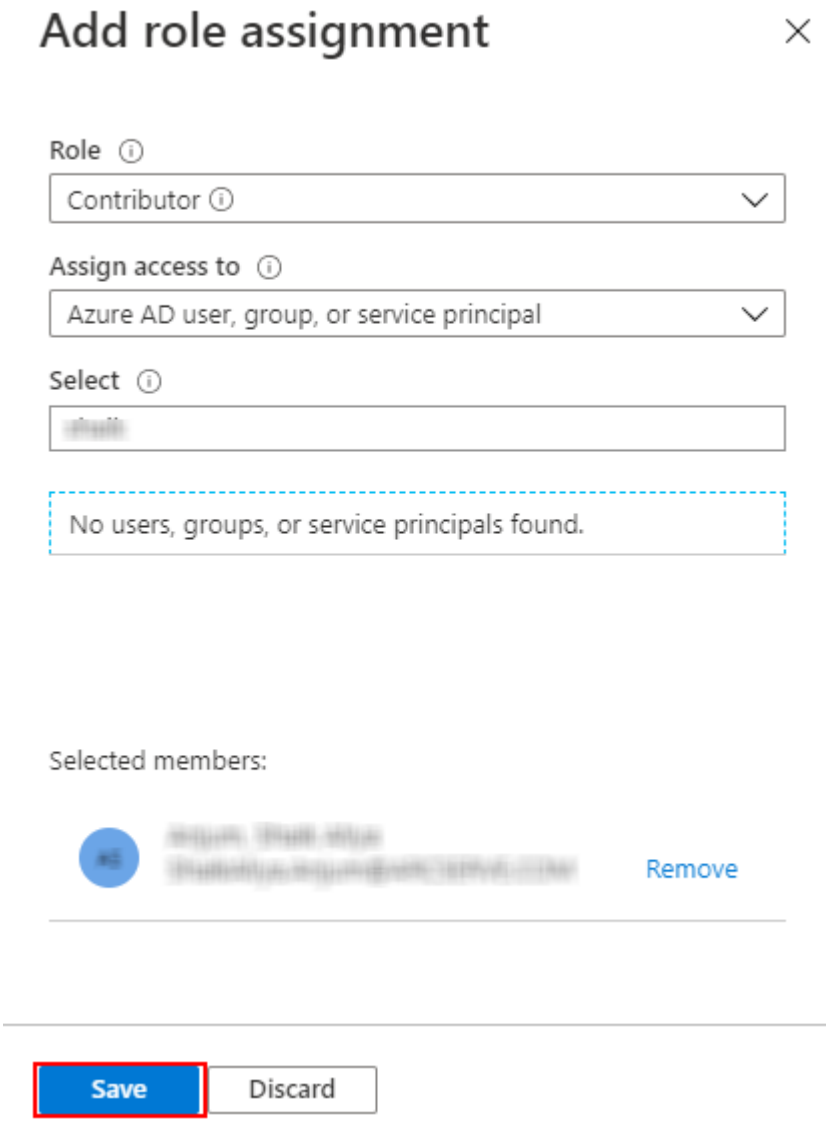
g. En Suscripciones, vaya a **Control de acceso (IAM) > Comprobar acceso** y haga clic en **Agregar** en el cuadro Agregar una asignación de rol.



h. En la página Agregar la asignación de roles, haga lo siguiente y, a continuación, haga clic en **Guardar**.

- Rol: Seleccione el rol que desea asignar a la aplicación.
- Asignar acceso a: Déjela como valor predeterminado.
- Seleccionar: De forma predeterminada, las aplicaciones de Azure AD no aparecen en las opciones disponibles. Para buscar la apli-

cación, busque el nombre y, a continuación, selecciónelo.



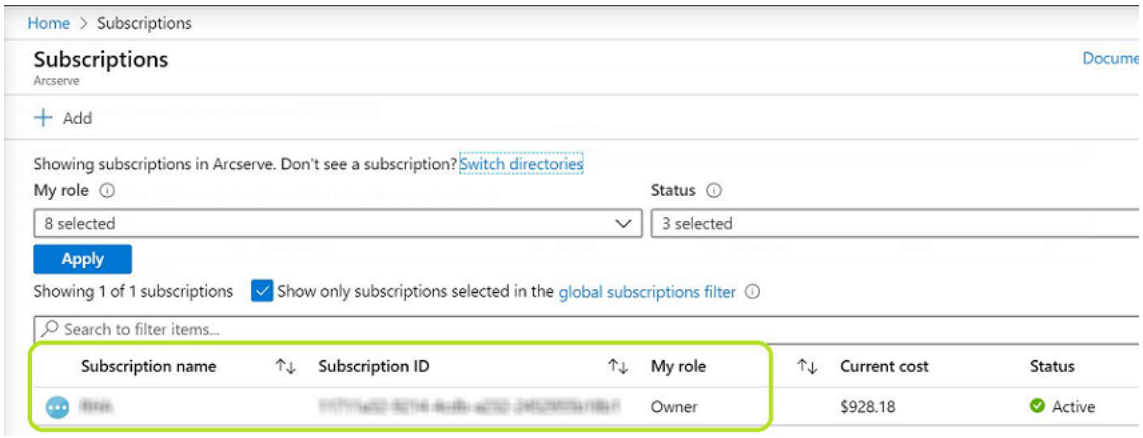
La aplicación Azure Active Directory se registra y se le ha asignado un rol correctamente.

Ahora, se pueden realizar los pasos siguientes utilizando la aplicación registrada para obtener los ID y la clave necesarios.

2. Para obtener el ID de suscripción[1], siga estos pasos:
   a. En el panel de exploración de la izquierda del portal de Azure, haga clic en **Suscripciones**.

      La lista de sus suscripciones se muestra junto con el ID de suscripción.

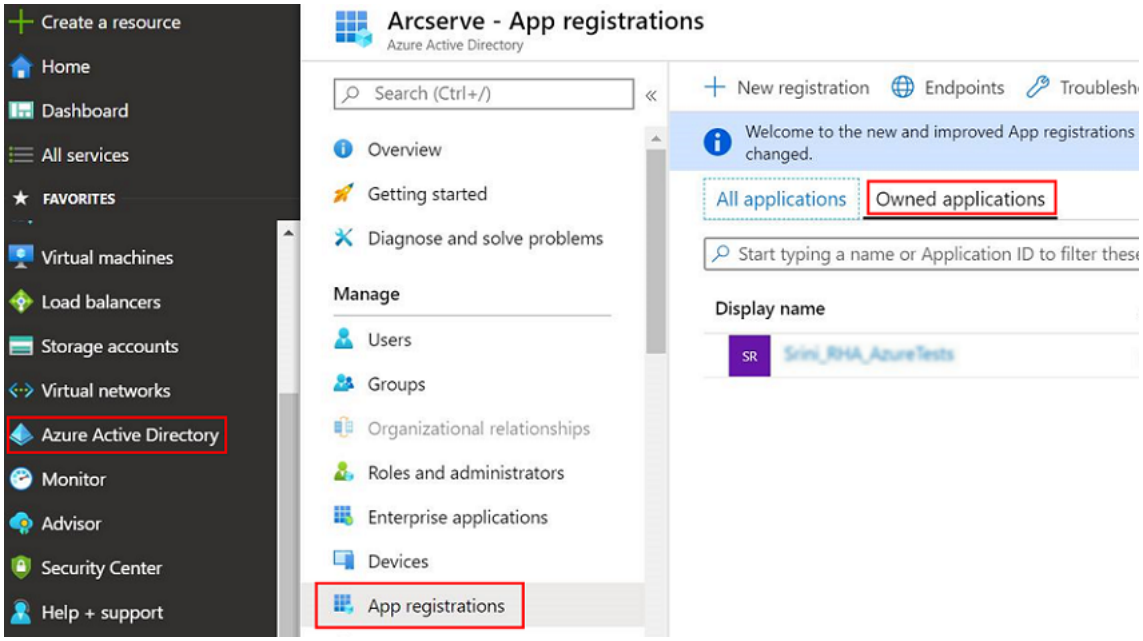
[1]El ID de suscripción hace referencia a un identificador único global (GUID) que identifica de forma exclusiva la suscripción para utilizar los servicios de Azure.



b. Copie y guarde el ID de suscripción que se utiliza al agregar la cuenta de la nube de Microsoft Azure en Arcserve UDP.

3. Para obtener el ID de inquilino[1] y ID de aplicación[2], siga estos pasos:

a. Vaya a **Azure Active Directory** > **App registrations** > **Owned applications** y, a continuación, seleccione la aplicación.

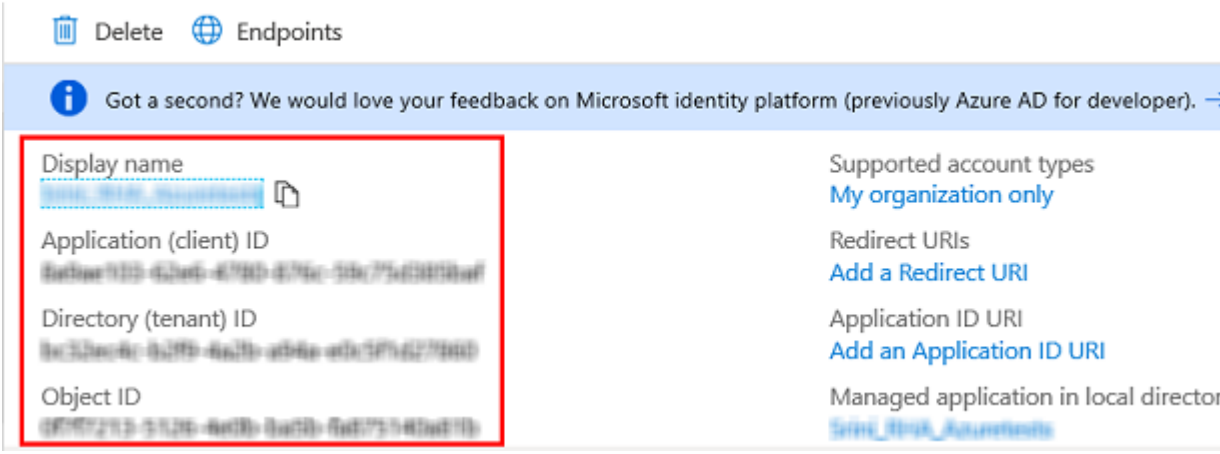


b. Copie y guarde el ID de la aplicación (cliente) y el ID del directorio

[1]Hace referencia al ID de la instancia de Azure Active Directory donde se ha realizado el registro de la aplicación. El ID de inquilino se llama ID de directorio en las propiedades de Azure Active Directory.

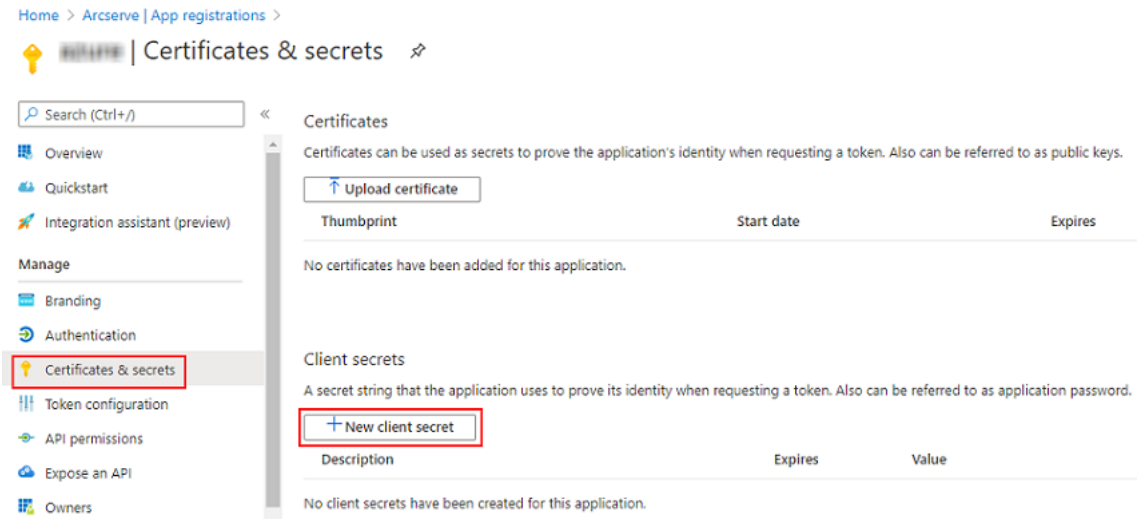
[2]Un ID de aplicación hace referencia a un GUID que identifica de forma única el registro de la aplicación en el inquilino de Azure Active Directory. A veces, también se hace referencia como el ID de cliente.

(inquilino) en una ubicación segura.



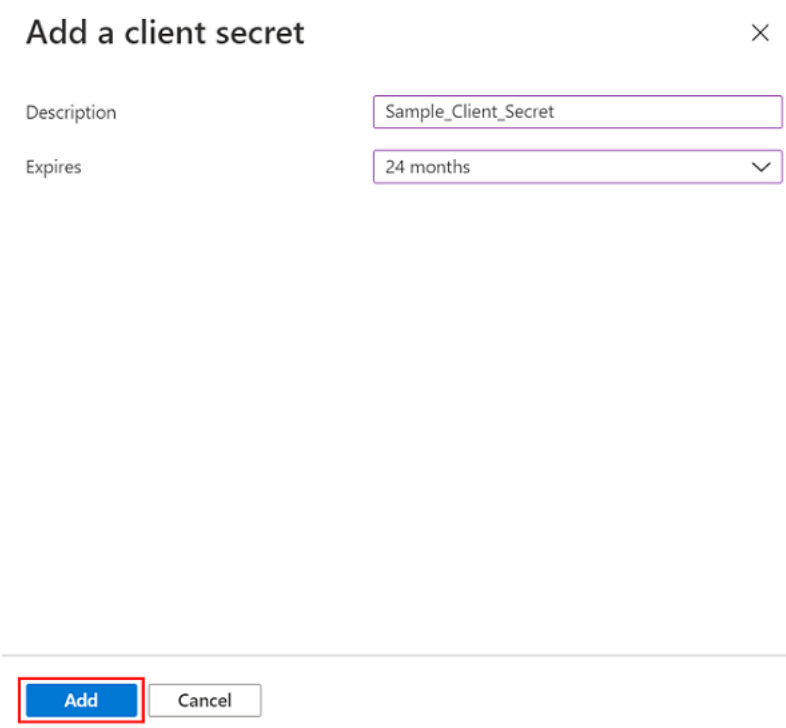
4. Para obtener el Secreto de cliente[1], siga estos pasos:

   a. En la página Registros de aplicaciones, seleccione la aplicación, vaya a **Certificados y secretos** en el panel izquierdo y, a continuación, haga clic en **Nuevo secreto de cliente** para agregar un secreto de cliente.



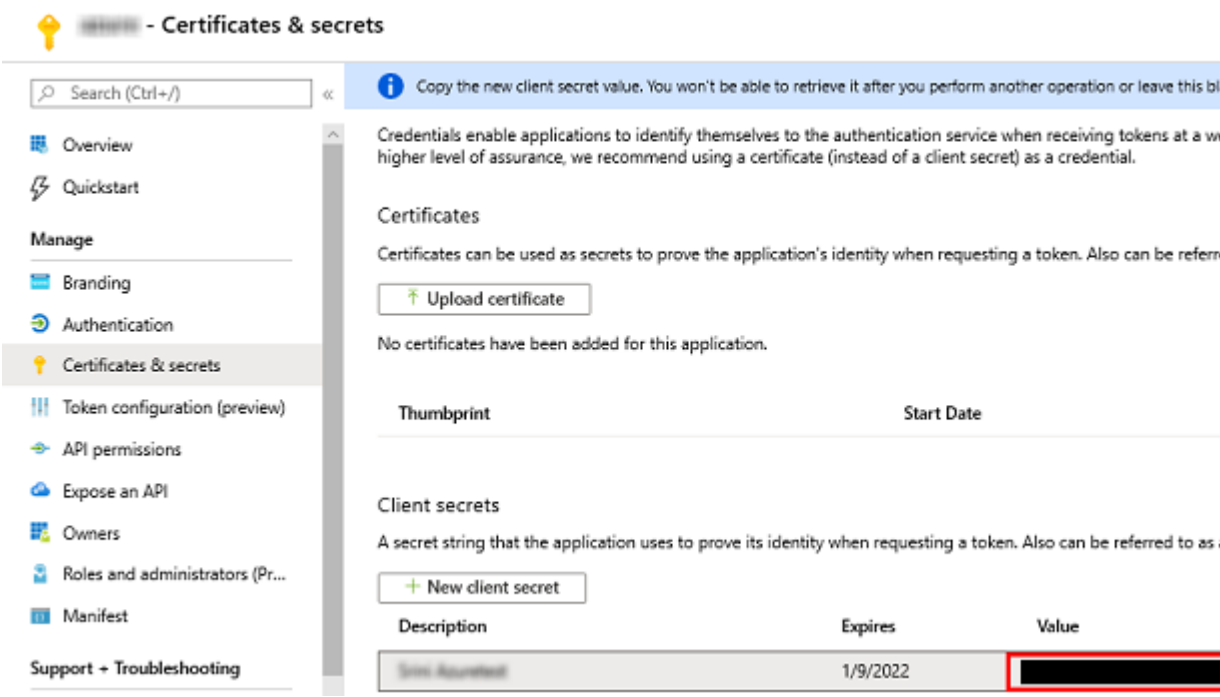
   b. En la página Agregar un secreto de cliente, introduzca una descripción, seleccione un intervalo de caducidad en la lista desplegable según sea necesario y, a continuación, haga clic en **Agregar**.

[1]Se hace referencia al secreto de cliente como una clave de autenticación de Azure.



Nota: Se recomienda seleccionar la opción de **24 meses** como intervalo de caducidad para evitar que se genere el secreto de cliente de forma repetida.

Aparecerá el valor del secreto de cliente.



Importante: Copie y guarde el valor del secreto de cliente porque no podrá recuperarlo más tarde. Si olvida guardar el valor, suprima el

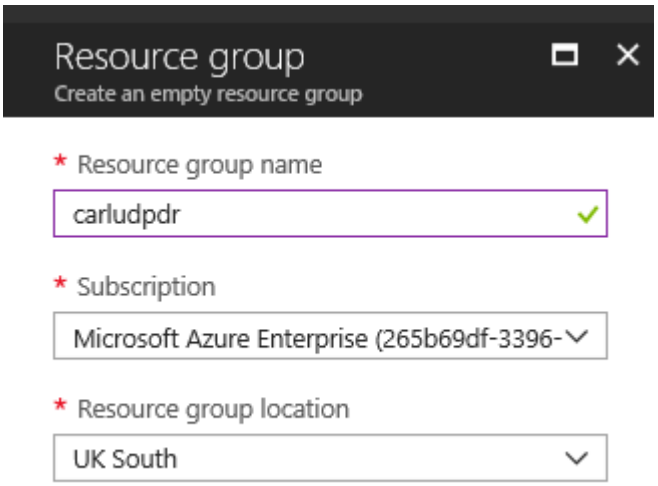
secreto de cliente existente y cree uno nuevo tal y como se menciona en el paso 4.

La cuenta de la nube se ha creado correctamente en Microsoft Azure.

Preparación de los recursos de Microsoft Azure

Antes de crear una cuenta de la nube para Microsoft Azure, se deben crear los siguientes recursos de Microsoft Azure:

1. Realice los pasos siguientes para crear un grupo de recursos:
    a. Inicie sesión en el portal de Azure utilizando las credenciales válidas.
    b. Haga clic en **Agregar** para crear un grupo de recursos vacío.
    c. Introduzca un nombre y una ubicación para el nuevo grupo de recursos y haga clic en **Crear**.



2. Realice los pasos siguientes para crear una cuenta de almacenamiento:
    a. Vaya a **Cuentas de almacenamiento** y haga clic en **Agregar**.
    b. Especifique lo siguiente:

    Nota: Asegúrese de que la cuenta de almacenamiento, la red virtual y el grupo de seguridad de red de la máquina virtual de Virtual Standby están en la misma ubicación.

    Nombre

    Especifica el nombre de la cuenta de almacenamiento.

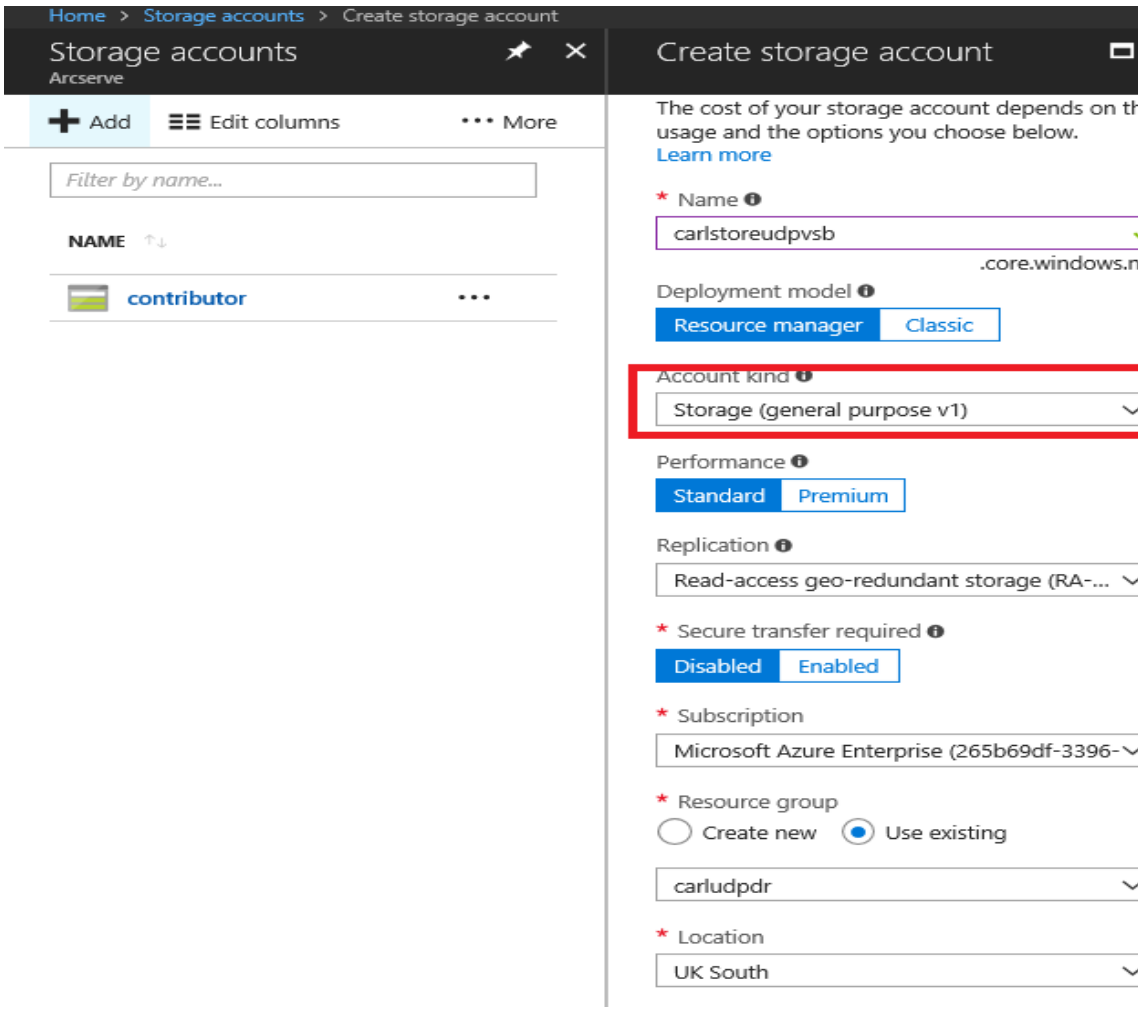
    Modelo de implementación

Seleccione el modelo de implementación en función de sus requisitos.

Tipo de cuenta

Especifique **Storage (general purpose v1)** o **StorageV2 (general purpose v2)** como tipo de cuenta.

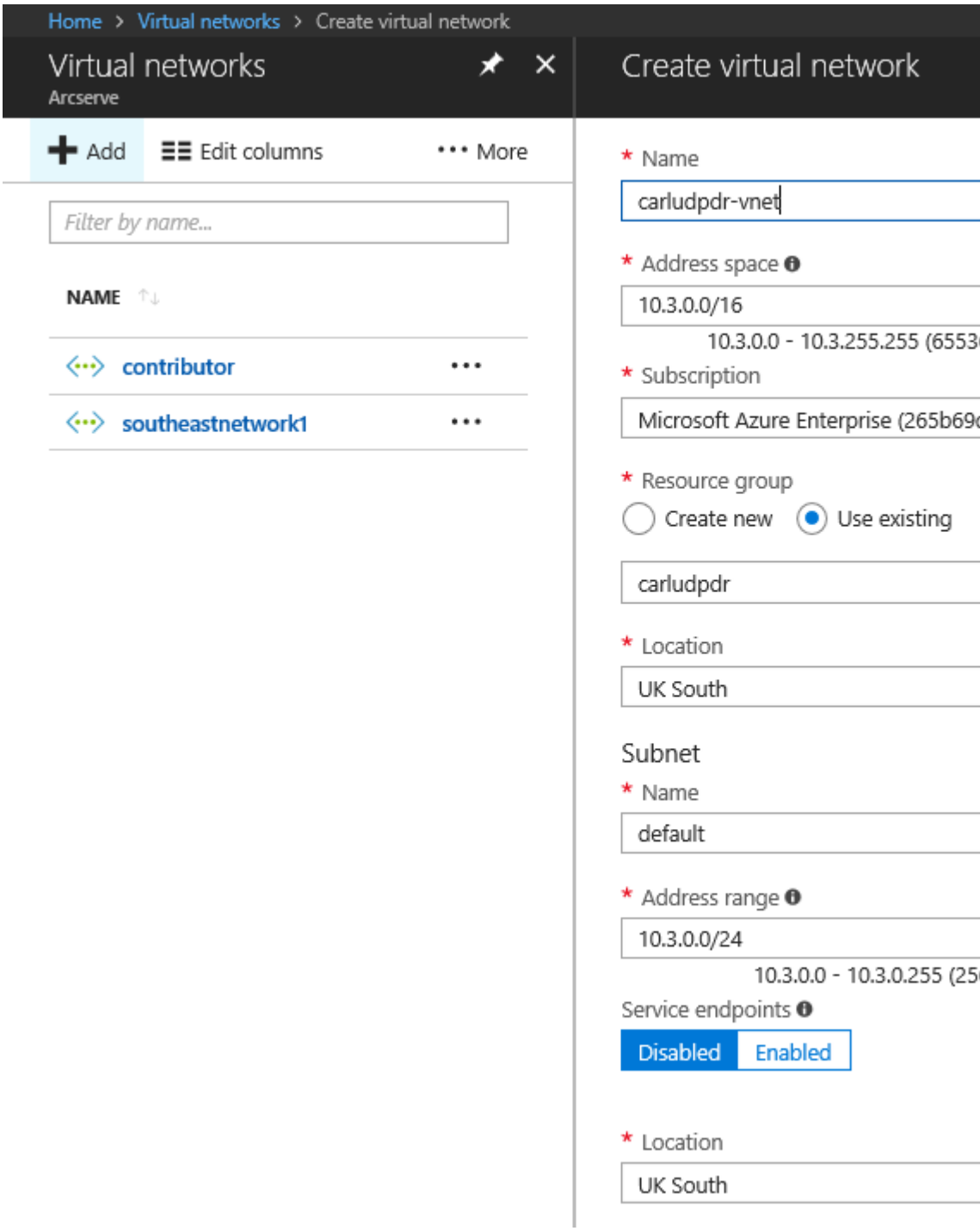
c. Especifique otros detalles según sea necesario y haga clic en **Crear**:



3. Realice los pasos siguientes para crear una red virtual y una subred:

   a. Vaya a la carpeta principal de Microsoft Azure, **Redes virtuales** y haga clic en **Agregar**.

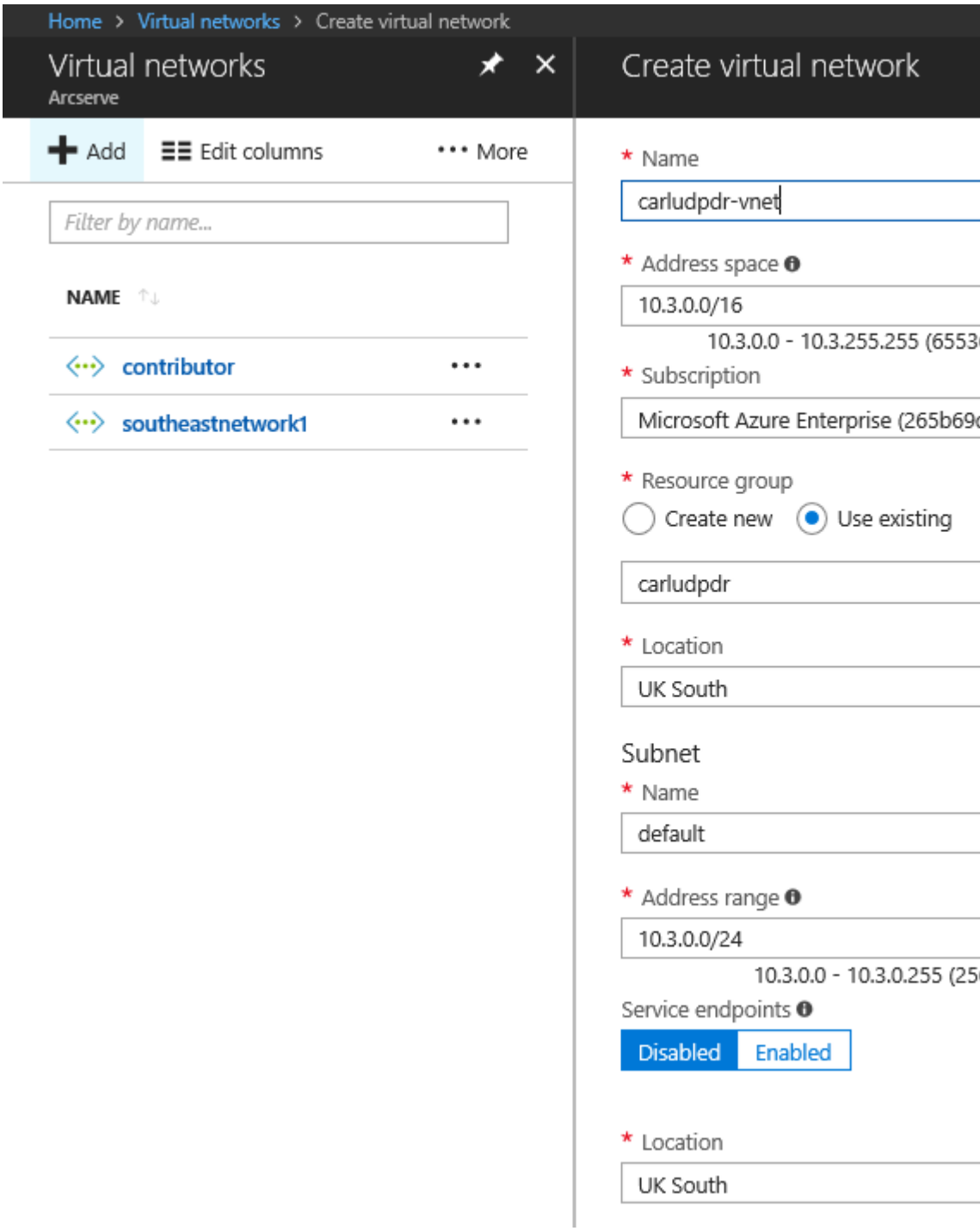
b. Especifique los detalles necesarios y haga clic en **Crear**.



4. Realice los pasos siguientes para crear un grupo de seguridad de red:

   a. Vaya a la carpeta principal de Microsoft Azure, **Grupos de seguridad de red** y haga clic en **Agregar**.

b. Especifique los detalles necesarios y haga clic en **Crear**.



Los recursos de Microsoft Azure se han creado correctamente.

Implementación de Arcserve UDP en Microsoft Azure

Después de completar los requisitos previos, se puede iniciar la implementación de Arcserve UDP en Microsoft Azure.

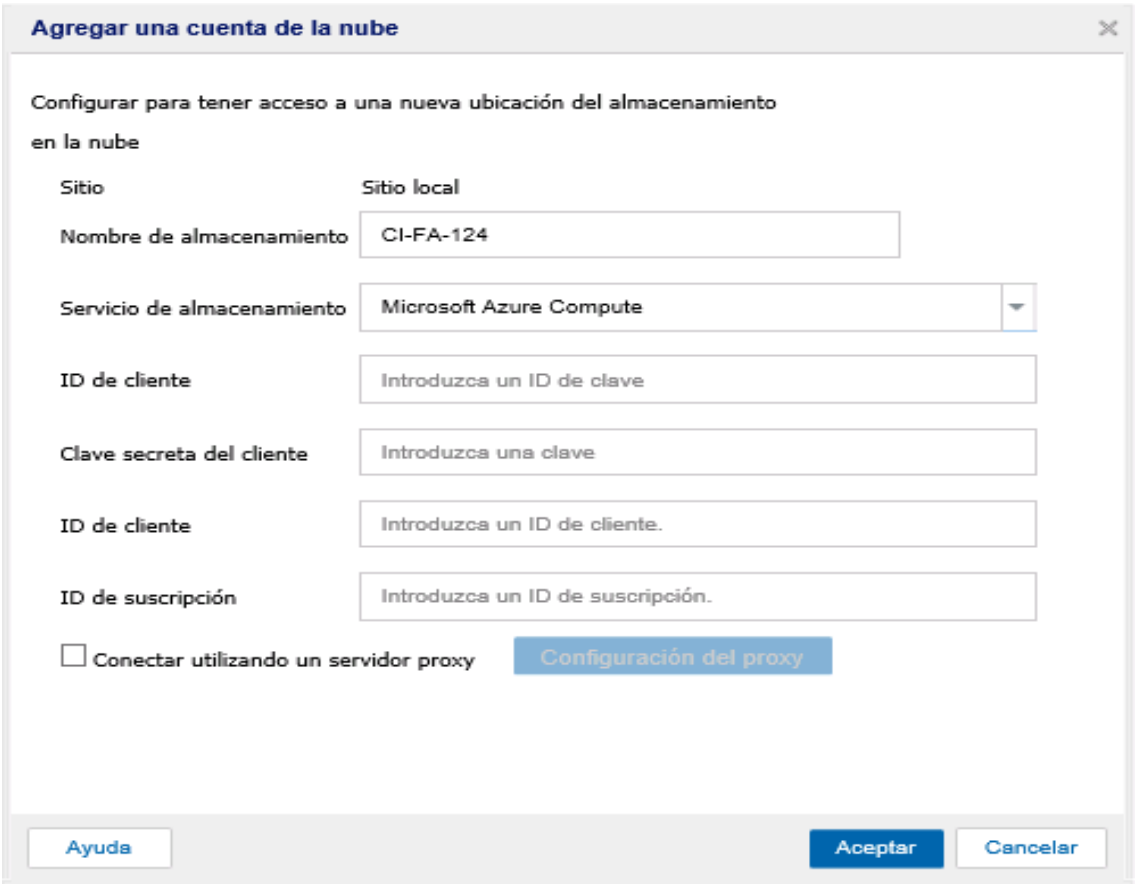
¿Qué hacer a continuación?

1. Adición de una cuenta de la nube de Azure en Arcserve UDP
2. Creación de un plan con una tarea de copia de seguridad
3. Adición de una tarea de Virtual Standby al plan
4. Ejecución de la tarea de Virtual Standby manualmente
5. Encendido de la máquina virtual de Virtual Standby en Azure
6. Comprobación del estado de la máquina virtual de Virtual Standby

Adición de una cuenta de la nube de Azure a Arcserve UDP

Agregue una cuenta de la nube de Microsoft Azure Compute para copiar los archivos o los puntos de recuperación en un almacenamiento en la nube. Se puede utilizar esta cuenta mientras se crean tareas para el plan de Virtual Standby a la nube o para el plan de una máquina virtual instantánea en Microsoft Azure.

Nota: Para agregar una cuenta de la nube para Microsoft Azure, se deben cumplir los requisitos previos. Para obtener más información, consulte Requisitos previos.



Siga estos pasos:

1. Inicie sesión en Arcserve Unified Data Protection y haga clic en la ficha **recursos**.
2. En el panel izquierdo, vaya a **Destinos** y haga clic en **Cuentas de la nube**.

   La página **Destinos: Cuentas de la nube** se muestra en el panel central.
3. Haga clic en **Agregar una cuenta de la nube**.

   Se muestra la página **Agregar una cuenta de la nube**.
4. Para el **Nombre de la cuenta**, proporcione un nombre único.

   El Nombre de la cuenta especifica el nombre del almacenamiento en la nube. Este nombre se agregará a la consola para identificar la cuenta de la nube. Cada cuenta de la nube debe tener un nombre de almacenamiento único.
5. Seleccione la opción de la lista desplegable **Servicio de la cuenta**.

   Aparecen varios campos para la configuración.
6. Especifique los detalles en los siguientes campos para realizar la configuración y haga clic en **Aceptar**:

   ID de cliente

   Hace referencia al ID de aplicación de la aplicación de Azure Active Directory. Copie el ID de cliente preparado en el editor de texto.

   Clave secreta del cliente

   Hace referencia a la clave de autenticación generada para la aplicación de Azure Active Directory que se especifica como ID de cliente. Copie la clave secreta del cliente preparada en el editor de texto.

   Importante: Esta clave secreta es crucial para mantener la seguridad de las cuentas. Se deben mantener las claves y credenciales de la cuenta en una ubicación segura. No incruste la clave secreta en una página web u otro código de origen accesible públicamente ni tampoco transmita a través de canales no seguros.

   ID de inquilino

   Hace referencia al ID de Azure Active Directory donde se ha creado la aplicación de Azure Active Directory. Copie el ID de inquilino preparado en el editor de texto.

   ID de suscripción

   Hace referencia a un identificador único global (GUID) que identifica de forma exclusiva la suscripción para utilizar los servicios de Azure. Copie el ID de suscripción preparado en el editor de texto.

   Configuración proxy

Especifica la configuración del servidor proxy. Seleccione **Conectar utilizando un servidor proxy**para activar esta opción. Si selecciona esta opción, también deberá incluir la dirección IP (o nombre del equipo) del servidor proxy y el número del puerto que utiliza el servidor proxy para las conexiones a Internet. También se puede seleccionar si el servidor proxy requiere autenticación. Se debe proporcionar la información de autenticación correspondiente necesaria para utilizar el servidor proxy.

La cuenta de la nube se agrega a la consola.

Creación de un plan con una tarea de copia de seguridad

Un plan incluye tipos diferentes de tareas que se desea realizar. Para crear una máquina de Virtual Standby, se crea un plan que incluye una tarea de copia de seguridad y una tarea de Virtual Standby. Una tarea de copia de seguridad realiza una copia de seguridad de los nodos de origen y almacena los datos en el destino especificado. La función de Virtual Standby utiliza los datos de la copia de seguridad y los convierte a un formato de máquina virtual.

Siga estos pasos:

1. Haga clic en la ficha **Recursos** en la Consola.
2. En el panel izquierdo, vaya a **Planes** y haga clic en **Todos los planes**.

   Si se han creado planes anteriormente, esos planes se muestran en el panel central.
3. En el panel central, haga clic en **Agregar un plan**.

   Se abre **Agregar un plan**.
4. Introduzca un nombre del plan.
5. (Opcional) Seleccione la casilla de verificación **Pausar plan**.

   El plan no se ejecutará hasta que se desactive la casilla de verificación para reanudar el plan.

   Nota: Si se pausa un plan, cualquier tarea en curso no se pausará pero todas las tareas programadas correspondientes asociadas con ese plan sí que se pausarán. Sin embargo, se puede ejecutar manualmente una tarea. Por ejemplo, se puede ejecutar manualmente la tarea de copia de seguridad y la tarea de replicación para un nodo incluso si el plan correspondiente está en pausa. En tal caso, no se ejecutará la tarea que viene a continuación de la tarea a petición (manual). Por ejemplo, hay una tarea de replicación después de una tarea de copia de seguridad a petición, la tarea de replicación no se ejecuta para la tarea de copia de seguridad a petición. Se

debe ejecutar manualmente la tarea de replicación. Cuando se reanude el plan, las tareas pendientes no se reanudan inmediatamente. Una vez que se haya reanudado el plan, las tareas pendientes se ejecutarán a partir de la próxima programación.

6. En la lista desplegable **Tipo de tarea** seleccione **Copia de Seguridad, Windows basado en el agente**.



Ahora especifique los detalles de los campos Origen, Destino, Programación y Avanzada.

Adición de una tarea de Virtual Standby al plan

Cree una tarea de Virtual Standby a Azure para que los datos de la copia de seguridad se conviertan a un formato de máquina virtual y se cree una máquina virtual. La función de Virtual Standby también controla el latido del nodo de origen para que cuando el nodo de origen esté bloqueado, la máquina virtual tome inmediatamente el control como nodo de origen.

Notas:

- Virtual Standby no puede encender automáticamente las instantáneas de punto de recuperación que se toman de los nodos de máquinas virtuales basadas en el host o replicados de un servidor de puntos de recuperación remoto, y el origen de la tarea de Virtual Standby es el que se replica en un sitio distinto. Se tiene que encender manualmente las instantáneas de punto de recuperación para dichos nodos.
- Cuando se pausa el plan y se vuelve a reanudar, la tarea de Virtual Standby no se reanuda automáticamente. Se debe ejecutar manualmente otra tarea de copia de seguridad para iniciar la tarea de Virtual Standby. También, cuando se pausa el plan, la opción Pausar/reanudar Virtual Standby deja de estar disponible. Si no se desea que la máquina virtual se inicie automáticamente después de pausar el plan, se deberá pausar manualmente el latido para los nodos.

Siga estos pasos:

1. Haga clic en **Agregar una tarea** en el panel izquierdo.

   Una tarea nueva se agrega al panel izquierdo.

2. En el menú desplegable **Tipo de tarea** seleccione **Virtual Standby**.

   La tarea de Virtual Standby se agrega.

3. En la ficha **Origen** seleccione un origen para la tarea de Virtual Standby.

4. Haga clic en la ficha **Servidor de virtualización** e introduzca el servidor de virtualización y los detalles del servidor de control.

   Tipo de virtualización

   Especifique Azure como el Tipo de virtualización.

   Nombre de la cuenta

   Seleccione una cuenta existente de Azure o haga clic en **Agregar** para crear una cuenta.

   Para obtener más información, consulte Cómo agregar una cuenta de la nube.

   Grupo de recursos

   Seleccione un grupo de recursos existente o haga clic en **Agregar** para crear un grupo de recursos.

   Para obtener más información, consulte Resource group in Azure.

   Región

   Seleccione la región en la que desea que la máquina virtual de Virtual Standby funcione en Azure. Para obtener más información, consulte Regions in Azure.

   Control

   Especifique el nombre de host del servidor que controla el estado del servidor de origen.

   Notas:

   - Puede utilizar cualquier equipo físico o máquina virtual como servidor de control.
   - No puede utilizar el servidor de origen de la copia de seguridad como servidor de control.
   - La configuración del servidor de control no es necesaria si los nodos se replican a partir de un servidor de puntos de recuperación remoto o si el origen de la tarea de Virtual Standby es el que se replica en un sitio distinto.

- La configuración del servidor de control no es necesaria si el origen de Virtual Standby es la tarea de replicación y el servidor de puntos de replicación de destino de la replicación se encuentra en Azure.

Nombre de usuario

Especifique el nombre de usuario para iniciar sesión en el sistema de control.

Contraseña

Especifique la contraseña del nombre de usuario para iniciar sesión en el sistema de control.

Protocolo

Especifique HTTP o HTTPS como el protocolo que desea utilizar para la comunicación entre Arcserve UDP y el servidor de control.

Puerto

Especifique el puerto que se desea utilizar para la transferencia de datos entre Arcserve UDP y el servidor de control.

5. Haga clic en la ficha **Máquina virtual** e introduzca los detalles de los siguientes campos: Configuración básica de la máquina virtual, Almacén de datos de la máquina virtual para VMware, Ruta de la máquina virtual para Hyper-V y Red de la máquina virtual.

Prefijo del nombre de la máquina virtual

Especifique un prefijo que se desea agregar al nombre de visualización de la máquina virtual en Azure.

Valor predeterminado: UDPVM_

Instantáneas del punto de recuperación

Especifique el número de instantáneas del punto de recuperación (puntos de recuperación) para la máquina virtual en espera. El número máximo de instantáneas del punto de recuperación es de 29.

Valor predeterminado: 5

Combinar todas las sesiones sin convertir en una instantánea de punto de recuperación única

Seleccione si desea combinar todas las sesiones sin convertir en una instantánea única de punto de recuperación cuando tenga lugar la siguiente tarea de Virtual Standby programada.

Valor predeterminado: Seleccionado

Tamaño de la máquina virtual

Microsoft Azure proporciona una amplia selección de tamaños de la máquina virtual optimizados para adaptarse a distintos casos de uso. Disponen de diversas combinaciones de CPU, memoria, almacenamiento y capacidad de red. Para obtener más información sobre el tamaño de la máquina virtual y sobre cómo satisfacen sus necesidades informáticas, consulte los tamaños de la máquina virtual de Windows en Azure.

Nombre de la cuenta de almacenamiento

Seleccione un nombre de la cuenta de almacenamiento existente o cree una cuenta de almacenamiento en Azure. Cuando se crea una cuenta de almacenamiento en Azure, se debe especificar uno de los siguientes como Tipo de cuenta

- Storage (general purpose v1)
- StorageV2 (general purpose v2)

Para obtener más información, consulte Storage account in Azure.

Red virtual

Seleccione una red virtual existente o cree una red virtual en Azure. Para obtener más información, consulte Virtual Network in Azure.

Subred

Seleccione una subred de la red virtual existente en función de la red virtual seleccionado o agregue una subred en Azure. Para obtener más información, consulte Add Subnet in Azure.

Grupo de seguridad de red

Seleccione un grupo de seguridad de red existente o cree un grupo de seguridad de red en Azure. Configure las reglas del grupo de seguridad para abrir los puertos relacionados, incluido el puerto 3389 para el escritorio remoto, el puerto 8014 y el puerto 8015 para la comunicación de Arcserve UDP. Para obtener más información, consulte Network Security Group.

Activar asignación automática de IP pública

Seleccione esta opción para asignar automáticamente la dirección IP pública a la máquina virtual de Virtual Standby cuando se inicia la máquina virtual de Virtual Standby en Azure.

6. Haga clic en la ficha **Avanzada** y proporcione los detalles siguientes:

Iniciar automáticamente la máquina virtual

Especifique si se desea iniciar la máquina virtual automáticamente.

Nota: Esta opción no se encuentra disponible para nodos de máquinas virtuales basadas en el host ni para nodos replicados desde un servidor de puntos de recuperación remoto, y el origen de la tarea de Virtual Standby es el que se replica en un sitio distinto. El origen de Virtual Standby es la tarea de replicación y el servidor de puntos de recuperación de destino de la replicación en Azure.

Tiempo de espera

Especifique el tiempo que el servidor de control debe esperar a un latido antes de encender una instantánea de punto de recuperación.

Frecuencia

Especifique la frecuencia con la que el servidor de origen comunica los latidos al servidor de control.

Ejemplo: el valor de Tiempo de espera especificado es 60. El valor de Frecuencia especificado es 10. El servidor de origen comunica los latidos en intervalos de 10 segundos. Si el servidor de control no detecta ningún latido en 60 segundos desde el último latido detectado, el servidor de controlador enciende una máquina virtual mediante la última instantánea de punto de recuperación.

Personalizar los parámetros de la tarea

Se pueden personalizar los parámetros de la tarea para las siguientes opciones:

- *Número de subprocesos que se cargan para cada tarea*: Valor predeterminado: 4
- *Tamaño del búfer para cada subproceso*: Valor predeterminado: 4096 kB

Activar Alertas de correo electrónico

Seleccione esta opción para activar las alertas de correo electrónico. Se reciben alertas de correo electrónico en función de los valores de configuración que se proporcionan.

- **Falta el latido del equipo de origen**: Virtual Standby envía notificaciones de alerta cuando el servidor de control no detecta el latido del servidor de origen.

  Nota: Esta opción no está disponible para los nodos de Replicación desde un servidor de puntos de recuperación remoto o si el origen de la tarea de Virtual Standby es el que se va a replicar en un sitio distinto.

- **Máquina virtual encendida para el equipo de origen configurado con encendido automático**: Virtual Standby envía notificaciones de alerta cuando enciende una máquina virtual que está configurada para el encendido automático cuando no se detecta un latido .

Nota: Esta opción no se encuentra disponible para nodos de máquinas virtuales basadas en el host ni para nodos replicados desde un servidor de puntos de recuperación remoto, o si el origen de la tarea de Virtual Standby es el que se replica en un sitio distinto.

- **Máquina virtual encendida para el equipo de origen configurado con encendido manual**: Virtual Standby envía notificaciones de alerta cuando una máquina virtual se enciende manualmente.
- **Errores/bloqueo de Virtual Standby**: Virtual Standby envía notificaciones de alerta si se detecta que se ha producido un error durante el proceso de conversión.
- **Virtual Standby correcto**: Virtual Standby envía notificaciones de alerta cuando una máquina virtual se enciende correctamente.
- **Virtual Standby no se ha iniciado correctamente desde la instantánea del punto de recuperación**: Virtual Standby envía notificaciones de alerta si la opción de recuperación local Iniciar automáticamente la máquina virtual está activada, pero no se ha encendido una máquina virtual de forma automática.

7. Haga clic en **Guardar**.

   Los cambios se guardan y la tarea de Virtual Standby se implementa automáticamente en el servidor de Virtual Standby.

   Nota: Una vez finalizada la tarea de Virtual Standby, se crea el volumen de la máquina virtual en espera. La máquina virtual en espera solo se crea después de la máquina virtual se encienda desde Arcserve UDP.

   Se ha creado e implementado correctamente Virtual Standby al plan de Azure.

Ejecución de la tarea de Virtual Standby manualmente

Para ejecutar manualmente una tarea de Virtual Standby, se tiene que realizar primero una copia de seguridad manual. La tarea de Virtual Standby se asocia con una tarea de copia de seguridad. Si un plan incluye una tarea de copia de seguridad y una tarea de Virtual Standby y se ejecuta manualmente la tarea de copia de seguridad, la tarea de Virtual Standby se ejecuta automáticamente después de la terminación de la tarea de copia de seguridad.

Siga estos pasos:

1. Haga clic en la ficha **Recursos**.
2. En el panel izquierdo, vaya a **Nodos** y haga clic en **Todos los nodos**.

   Muestra los planes que se han agregado.

3. Seleccione los nodos que de los que desea realizar la copia de seguridad. El nodo seleccionado debe tener asignado un plan.
4. En el panel central, haga clic en **Acciones**, **Realizar copia de seguridad ahora**.

   Aparecerá el cuadro de diálogo **Ejecutar ahora una copia de seguridad**.
5. Seleccione el tipo de copia de seguridad y proporcione un nombre para la tarea de copia de seguridad.
6. Haga clic en **Aceptar**.

   Se ejecuta la tarea de copia de seguridad.

   La tarea de Virtual Standby se ejecuta inmediatamente después de que se complete la tarea de copia de seguridad.

   La tarea de Virtual Standby se ejecuta manualmente.

Encendido de la máquina virtual de Virtual Standby en Azure

Los volúmenes de la máquina virtual de Virtual Standby se crean en Azure después de la finalización de la tarea de Virtual Standby. La máquina virtual de Virtual Standby solo se crea cuando se encienden desde Arcserve UDP.

Virtual Standby se puede configurar de manera que encienda máquinas de Virtual Standby a partir de las instantáneas de puntos de recuperación de forma automática cuando el servidor controlador no detecta ninguna pulsación del servidor de origen. Opcionalmente, se pueden encender máquinas de Virtual Standby a partir de las instantáneas de puntos de recuperación de forma manual en el caso de que se produzca una emergencia o un error en el servidor de origen, o en el caso de que sea conveniente dejar sin conexión un servidor de origen para realizar tareas de mantenimiento.

Siga estos pasos:

1. En la ficha **Recursos**, vaya al grupo de nodos de **Virtual Standby**.

   Los nodos de Virtual Standby se muestran en el panel central.
2. En el panel central, seleccione el nodo y haga clic en **Máquina virtual en espera**.

   Se abre el cuadro de diálogo **Máquina virtual en espera**.
3. En el cuadro de diálogo **Máquina virtual en espera**, realice las tareas siguientes:
   - Seleccione una fecha y hora de inicio de la instantánea del punto de recuperación para encender la máquina virtual.
   - Haga clic en **Encender la máquina virtual**.

La máquina virtual se encenderá utilizando los datos de la instantánea del punto de recuperación.

Ahora se puede verificar el estado o apagar la máquina virtual de Virtual Standby. Para obtener más información, consultar lo siguiente:

- Comprobación del estado de la máquina virtual de Virtual Standby
- Apagado de la máquina virtual de Virtual Standby en Azure

Apagado de la máquina virtual de Virtual Standby en Azure

Se puede apagar la máquina virtual de Virtual Standby en Azure utilizando la Consola de Arcserve UDP.

Siga estos pasos:

1. En la Consola, haga clic en **Recursos**.
2. Vaya a **Virtual Standby**.
3. Seleccione y haga clic con el botón secundario del ratón en **Máquina virtual de Virtual Standby** en el panel central.

   Se abre el cuadro de diálogo de la máquina virtual de Virtual Standby y muestra las instantáneas activas.
4. Seleccione una instantánea activa y haga clic en **Apagar máquina virtual**.
5. Haga clic en **Suprimir**.

   Aparecerá un diálogo de confirmación.
6. Si desea suprimir los discos conectados a la máquina virtual de Virtual Standby, seleccione la opción **Suprimir los discos conectados**.
7. Haga clic en **Aceptar**.

   La máquina virtual de Virtual Standby se apaga correctamente.

Comprobación del estado de la máquina virtual de Virtual Standby

Se puede verificar el estado de la máquina virtual de Virtual Standby utilizando la Consola de Arcserve UDP.

Siga estos pasos:

1. En la Consola, haga clic en **Recursos**.
2. Vaya a **Virtual Standby**.
3. Seleccione **Máquina virtual de Virtual Standby** en el panel central.
4. El panel del asistente de configuración mostrará el estado de la máquina virtual de Virtual Standby en el grupo **Estado de Virtual Standby**.

   El estado se muestra como **En ejecución** si la máquina virtual de Virtual Standby está encendida. Si no está encendida, el estado se muestra como **ND** o **Apagada**.

Términos y definiciones de Arcserve UDP

Copia de seguridad basada en el agente

Una copia de seguridad basada en agentes es un método para realizar la copia de seguridad de los datos mediante un componente de agente. El agente está instalado en el nodo de origen.

Compresión

Se utiliza la compresión para las copias de seguridad. La compresión se realiza muchas veces para reducir el uso de espacio en disco, pero también tiene un efecto contrario en la velocidad de la copia de seguridad dado el incremento del uso de la CPU.

A continuación se especifican las opciones disponibles:

Sin compresión

Esta opción utiliza menor cantidad de CPU (velocidad más alta), pero también utiliza más espacio en disco para la imagen de copia de seguridad.

Compresión estándar

Se realiza algún tipo de compresión. Esta opción proporciona un buen equilibrio entre el uso de la CPU y el uso de espacio en disco. Se trata de la configuración predeterminada.

Compresión máxima

Se realiza la compresión máxima. Esta opción utiliza mayor cantidad de CPU (velocidad más baja) pero también utiliza menos espacio en disco para la imagen de copia de seguridad.

Notas:

- Si la imagen de copia de seguridad contiene datos que no pueden comprimirse (como imágenes JPG, archivos ZIP, entre otros), deberá adjudicarse espacio de almacenamiento adicional para tratar estos datos. Como resultado, si ha seleccionado la opción de realizar cualquier tipo de compresión y dispone de datos que no pueden comprimirse en la copia de seguridad, puede resultar en un incremento del uso de espacio en disco.
- Si se modifica el nivel de compresión de Sin compresión a Compresión estándar o a Compresión máxima, o si cambia de Compresión estándar o Compresión máxima a Sin compresión, la primera copia de seguridad que se realiza después de este cambio de nivel de compresión es automáticamente una copia de

seguridad completa. Al finalizar la copia de seguridad completa, todas las copias de seguridad futuras (completa, incremental o de verificación) se realizarán según lo programado.

Esta opción está disponible solamente para los destinos de recursos compartidos locales o remotos. Si la copia de seguridad del Agente de Arcserve Unified Data Protection se realiza en el almacén de datos, no se puede cambiar el valor de configuración de la compresión.

- Si el destino no tiene suficiente espacio libre, considere el aumento del modo de compresión de la copia de seguridad. Esta opción está disponible solamente para los destinos de recursos compartidos locales o remotos. Si la copia de seguridad del Agente de Arcserve Unified Data Protection se realiza en el almacén de datos, no se puede cambiar el valor de configuración de la compresión.

configuración

Una ficha en la consola de Arcserve UDP para definir parámetros de configuración como, por ejemplo, las alertas de correo electrónico, la configuración de la base de datos y las preferencias de instalación.

cuadro de mandos

Una ficha en la consola de Arcserve UDP que permite ver el estado de la última copia de seguridad y el estado de almacenamiento. Se puede ver el almacenamiento de datos real, sin formato y restaurable más reciente.

Almacén de datos

Un almacén de datos es una zona de la memoria física en un disco. Se puede crear un almacén de datos en cualquier sistema Windows donde esté instalado el servidor de punto de recuperación. Los almacenes de datos pueden ser locales o estar en un recurso compartido remoto al que puede acceder el sistema Windows.

Destino

El destino es un equipo o servidor donde se almacenan los datos de la copia de seguridad. Un destino puede ser una carpeta local en el nodo protegido, una carpeta compartida remota o un servidor de punto de recuperación (RPS).

Nodos detectados

Los nodos detectados son sistemas físicos o virtuales que se agregan a la consola de Arcserve UDP detectándolos en Active Directory o en el servidor de vCenter/ESX,

importándolos desde un archivo o agregándolos manualmente mediante la dirección IP.

Cifrado

La solución Arcserve Unified Data Protection proporciona una función de cifrado para los datos.

Cuando el destino de la copia de seguridad es un servidor de puntos de recuperación, los cifrados disponibles son Sin cifrado y Cifrar datos con AES-256. Se puede establecer para crear un almacén de datos. Cuando el destino de la copia de seguridad es el recurso compartido local o remoto, las opciones de formato de cifrado disponibles son Sin cifrado, AES-128, AES-192 y AES-256. La opción se puede establecer mientras se crea un plan para realizar una copia de seguridad a una carpeta local o compartida, o desde la configuración de la copia de seguridad del Agente de Arcserve Unified Data Protection independiente.

Funciones clave del cifrado

1. El método de cifrado AES256 se aplica a lo siguiente:
   - Almacén de datos
   - Contraseña guardada (en el plan de protección, el registro, el archivo de configuración, etc.)
2. *Para la tarea de copia de seguridad:* Si el cifrado está activado, los datos se cifran antes de enviarlos fuera del servidor.
3. *Para la tarea de replicación:* Si el destino de la replicación tiene activado el cifrado, los datos se cifran antes de enviarlos fuera del servidor.

Configuración del cifrado

a. Seleccione el tipo de algoritmo de cifrado que desea utilizar para las copias de seguridad.

   El cifrado de datos es la traducción de los datos a una forma que resulte ininteligible sin un mecanismo de descifrado. La solución Arcserve Unified Data Protection utiliza algoritmos de cifrado seguros AES (Estándar de cifrado avanzado) para lograr la máxima seguridad y privacidad de los datos especificados.

b. Cuando se selecciona un algoritmo de cifrado, se debe proporcionar, y confirmar, la contraseña de cifrado.
   - La contraseña de cifrado puede tener un máximo de 23 caracteres.

- Las copias de seguridad completas y todas las copias de seguridad incrementales y de verificación relacionadas deben utilizar la misma contraseña para el cifrado de datos.
- Si se modifica la contraseña de cifrado de una copia de seguridad incremental o de verificación, se deberá realizar una copia de seguridad completa. Esto significa que la primera copia de seguridad que se realizará después de modificar la contraseña de cifrado será completa, independientemente de cuál fuera el tipo de copia de seguridad original.

Por ejemplo, si se cambia la contraseña de cifrado y se envía una copia de seguridad personalizada de verificación o incremental ésta se convertirá automáticamente en una copia de seguridad completa.

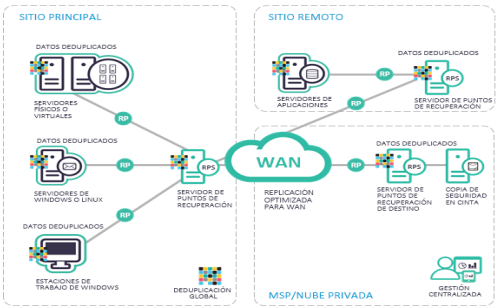
Nota: Esta opción está disponible solamente para los destinos de recursos compartidos locales o remotos. Si la copia de seguridad del Agente de Arcserve Unified Data Protection se realiza en el almacén de datos, no se puede desactivar el valor de configuración del cifrado.

c. La solución Arcserve Unified Data Protection tiene una contraseña de cifrado y una contraseña de sesión.
   - La contraseña de cifrado se requiere para el almacén de datos.
   - La contraseña de sesión se requiere para el nodo.
   - Si se cifra el almacén de datos, la contraseña de sesión es obligatoria. Si no se cifra el almacén de datos, la contraseña de sesión es opcional.

   No será necesaria ninguna contraseña si la restauración se realiza en el equipo desde donde se ha realizado la copia de seguridad. Sin embargo, sí será necesaria una contraseña si se intenta realizar la restauración en otro equipo. De forma predeterminada, solo se necesita una contraseña para el primer inicio de sesión. Para introducir la contraseña incluso después del primer inicio de sesión, el administrador debe detener manualmente el servicio de extensión del explorador del Agente de Arcserve UDP.

Deduplicación global

La deduplicación global de Arcserve UDP reduce sustancialmente la cantidad de datos transferidos realmente durante los ciclos de copia de seguridad. La capacidad para la deduplicación en todos los clientes limita el almacenamiento innecesario y la transferencia de datos existentes, lo que hace que sea una capacidad global porque los datos se deduplican en todos los nodos, tareas y sitios.



Copia de seguridad sin agente basada en host

Una copia de seguridad sin agente y basada en el host es un método para realizar una copia de seguridad de los datos sin utilizar un componente de agente en el equipo de origen.

Modo de transporte HOTADD

El modo de transporte HOTADD es un método de transporte de datos que permite realizar copias de seguridad de máquinas virtuales configuradas con discos SCSI. Para obtener más información, consulte la guía titulada Virtual Disk API Programming Guide en el sitio Web de VMware.

Tarea

Una tarea es una acción de Arcserve UDP para realizar una copia de seguridad, restaurar, crear Virtual Standby o replicar nodos.

tareas

Una ficha en la Consola de Arcserve UDP donde se puede controlar el estado de todas las tareas como, por ejemplo, la copia de seguridad, la replicación y la restauración. Los detalles incluyen las tareas, los tipos de tarea, los ID de nodo, los puntos de recuperación y los nombres de plan.

Modo de transporte NBD

El modo de transporte del dispositivo de bloqueo de red (NBD), también conocido como modo de transporte de LAN, utiliza el protocolo de copia de archivos de red (NFC) para comunicarse. Cuando se utiliza el modo NBD, hay diversas operaciones de VDDK y VCB que utilizan una conexión por cada disco virtual al cual éstas acceden para cada host de ESX/ESXi Server.

Modo de transporte NBDSSL

El modo de transporte de capa de sockets seguros del dispositivo de bloqueo de red (NBDSSL) utiliza el protocolo de copia de archivo de red (NFC) para la comunicación. NBDSSL transfiere datos cifrados mediante redes de comunicación TCP/IP.

Nodos

Un nodo es un sistema físico o virtual protegido por Arcserve UDP. Arcserve UDP puede proteger nodos físicos y máquinas virtuales en un servidor vCenter/ESX o Microsoft Hyper-V.

Plan

Un plan es un grupo de tareas para gestionar la copia de seguridad, la replicación y la creación de equipos de Virtual Standby. Un plan está formado por una única tarea o por varias. Las tareas son un conjunto de actividades para definir el origen, el destino, la programación y los parámetros avanzados.

Nodos protegidos

Los nodos protegidos son los nodos que han programado planes de copia de seguridad para realizar la copia de seguridad de los datos en intervalos regulares.

Evento reciente

Los eventos recientes son las tareas que todavía se están ejecutando o las tareas que se han completado recientemente.

Punto de recuperación

Un punto de recuperación es una instantánea de la copia de seguridad en un momento dado de un nodo. Un punto de recuperación se crea cuando se realiza la

copia de seguridad de un nodo. Los puntos de recuperación se almacenan en el destino de la copia de seguridad.

Servidor de puntos de recuperación

Un servidor de puntos de recuperación es un nodo de destino donde se instala el servidor. Se pueden crear varios almacenes de datos a un servidor de puntos de recuperación. El servidor de puntos de recuperación (RPS) actúa como un repositorio de copias de seguridad para las imágenes del disco y ofrece un conjunto exclusivo de tecnologías que proporcionan los bloques de creación fundamentales de la solución de Arcserve UDP. Entre las funciones clave del servidor de puntos de recuperación se encuentran las siguientes: Deduplicación global verdadera de origen, Replicación incorporada probada de las imágenes del disco, Servidor de puntos de recuperación Jumpstart, Sincronización sin conexión y Almacenamiento multicliente.

Replicación

La replicación es una tarea que duplica los puntos de recuperación de un servidor a otro servidor.

Recursos

Recursos es una ficha en la consola de Arcserve UDP. En la ficha **Recursos** se pueden gestionar los nodos de origen, los destinos y los planes.

Modo de transporte SAN

El modo de transporte de red de área de almacenamiento (SAN) permite transferir datos de copias de seguridad de sistemas proxy conectados con la SAN a dispositivos de almacenamiento.

Sistemas

Los sistemas son todos los tipos de nodos, dispositivos y máquinas virtuales que Arcserve Unified Data Protection puede gestionar. Esto incluye máquinas de Linux, virtuales, físicas y máquinas de Virtual Standby.

Tareas

Una tarea es un conjunto de actividades para definir diversos parámetros para realizar la copia de seguridad, la replicación y la creación de máquinas de Virtual Standby. Estos parámetros incluyen el origen, el destino, el plan y algunos parámetros

avanzados. Cada tarea se asocia con un plan. Se puede tener más de una tarea en un plan.

Nodos desprotegidos

Los nodos desprotegidos son los nodos que se agregan a Arcserve Unified Data Protection pero que no tienen ningún plato asignado. Cuando no se asigna un plan, no se puede realizar la copia de seguridad de los datos y el nodo permanece desprotegido.

Deduplicación de datos

La deduplicación de datos es una tecnología que elimina copias duplicadas de los mismos datos, reduciendo por esa razón el espacio de almacenamiento. En una organización, puede haber diversos motivos para duplicar datos como un archivo adjunto de correo electrónico específico enviado a varios usuarios. Cuando se realiza la copia de seguridad de estos datos, se acaban guardando varias copias de los mismos datos en los medios de almacenamiento de la copia de seguridad.

La deduplicación de datos elimina los datos redundantes y guarda solamente una instancia de los datos. Todas las otras instancias se reemplazan por una referencia a esa instancia. Este método puede reducir considerablemente el espacio de almacenamiento que se requiere para almacenar datos de la copia de seguridad.

Por ejemplo, puede haber un mismo archivo de 10 MB que 100 usuarios diferentes han almacenado en sus sistemas locales. Cuando se realiza la copia de seguridad de todos estos sistemas o nodos locales, se necesitarían 1000 MB de espacio de almacenamiento. Con la deduplicación de datos, se puede reducir el espacio de almacenamiento a aproximadamente 10 MB porque solamente se almacenará una instancia del archivo en el disco. Las 99 instancias restantes hacen referencia a esa instancia.

Beneficios de la deduplicación de datos

- Almacena más datos de la copia de seguridad en un espacio de almacenamiento.
- Reduce la cantidad de datos que se envían por la red.
- Realiza una copia de seguridad rápida ya que se almacena la información de referencia en vez de los datos reales.
- Reduce el coste del ancho de banda de la red y de los medios de almacenamiento.

Tipos de deduplicación de datos

Arcserve UDP es compatible con los dos tipos siguientes de deduplicación de datos.

Deduplicación de datos de origen

Asegura que solamente los datos únicos del agente se envían a un servidor de punto de recuperación para la copia de seguridad de los datos.

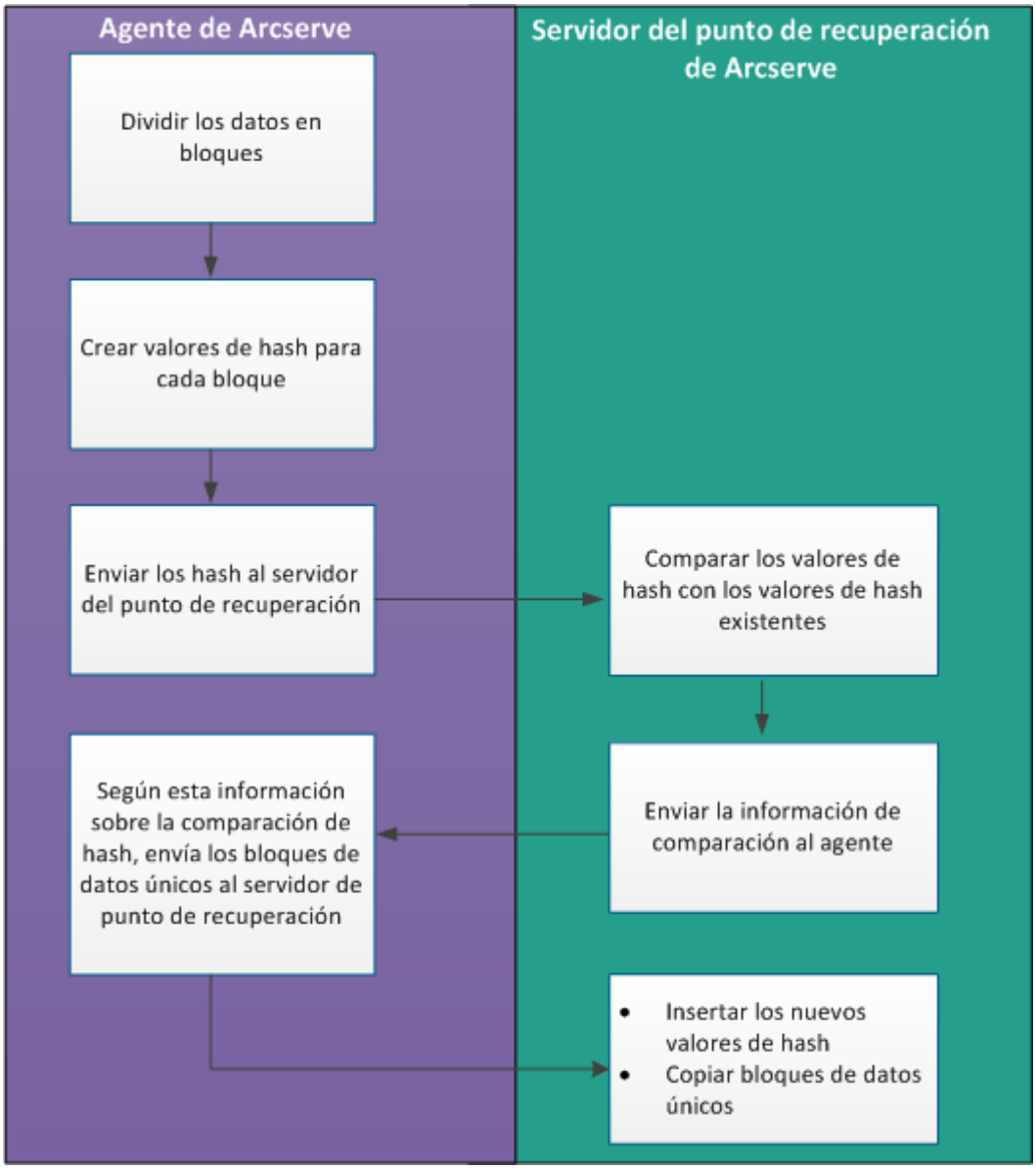
Deduplicación global

Asegura que solamente se realiza la copia de seguridad de los datos únicos de varios gentes en un servidor de punto de recuperación. Si los bloques de datos similares están presentes en varios nodos, solamente se realiza la copia de seguridad de una copia en el servidor de punto de recuperación.

Cómo funciona la deduplicación de datos

El proceso de deduplicación de Arcserve UDP divide los datos en bloques de datos y a cada bloque se le asigna un identificador único llamado hash. Hash se calcula basándose en el clúster de volúmenes. El tamaño del bloque de deduplicación predeterminado es de 4 kB (el tamaño del clúster de volúmenes predeterminado es de 4 kB para la mayor parte de los nodos). Estos valores de hash se comparan con los valores de hash de los datos de copia de seguridad existentes y si se encuentran referencias duplicadas, no se realizará la copia de seguridad de esos bloques de datos. Solamente se realiza la copia de seguridad de los bloques de datos con referencias únicas.

El diagrama siguiente muestra cómo funciona la deduplicación en Arcserve UDP.



Cuando una copia de seguridad se activa, el proceso de deduplicación en el agente primero divide los datos en bloques y asigna una clave de hash o valor únicos a cada bloque. Los valores de hash se envían a continuación al servidor de punto de recuperación. En el servidor de punto de recuperación, estos valores de hash se comparan con los valores de hash existentes y se filtran los hash duplicados. Los resultados de la comparación se devuelven al agente. Según esta información de hash duplicada, el agente envía los bloques de datos únicos al servidor de punto de recuperación para realizar la copia de seguridad. Los valores de hash nuevos de estos bloques de datos también se insertan en la lista de hash existentes en el servidor de punto de recuperación.

Cuando hay varios agentes, el proceso de deduplicación permanece el mismo, pero los datos duplicados de varios agentes se filtran. Esto elimina cualquier duplicación de los datos incluso de varios agentes.

A continuación se muestran los beneficios de utilizar la deduplicación de datos en Arcserve UDP:

- **Copia de seguridad completa más rápida**
- **Tarea de combinación más rápida**
- **Compatibilidad con la deduplicación global**
- **Replicación optimizada**

Cuándo se debe utilizar la deduplicación

A continuación se muestran algunos de los escenarios donde la utilización de un almacén de datos de deduplicación puede ser más efectiva:

- Cuando se tienen varios nodos con datos similares. En este escenario, si se realiza la copia de seguridad de los datos de todos los nodos a un almacén de datos, se puede obtener una buena reducción en la cantidad de datos que se almacenan realmente en el servidor de punto de recuperación. El espacio de almacenamiento necesario puede ser considerablemente menor.
- Cuando se tiene que realizar frecuentemente una copia de seguridad completa de un nodo. En este escenario, la mayor parte de los datos de la copia de seguridad ya existen, así que la duración de la copia de seguridad puede ser menor.
- Cuando el ancho de banda de la red es valioso. Como solamente los bloques de datos únicos viajan a través de la red, se puede reducir el uso de la red.
- Cuando los datos de los que se ha realizado la copia de seguridad frecuentemente cambian de un nodo a otro. En este escenario, cuando se intenta realizar la copia de seguridad del nodo nuevo (donde los datos se mueven desde el nodo original), el destino ya contiene la copia y solo se realiza la copia de seguridad de la información de referencia.

Configuración de almacenes de datos de deduplicación en Arcserve UDP

Los parámetros siguientes son importantes para configurar un almacén de datos de deduplicación:

Destino de los datos

Se utiliza para almacenar los datos protegidos. Es mejor utilizar un disco mayor para el destino de los datos porque contiene los bloques de los datos originales del origen.

Destino del índice

Se utiliza para almacenar los archivos de índice y es mejor usar un disco diferente para mejorar el rendimiento del procesamiento de la deduplicación.

Destino del hash

Se utiliza para almacenar los archivos de hash y es mejor utilizar la unidad de SSD de velocidad alta que pueda mejorar la capacidad de deduplicación con una adjudicación de memoria inferior obligatoria.

Si destino del hash se configura en una unidad de SSD de velocidad alta, se puede utilizar para ampliar la capacidad de deduplicación con un requisito de adjudicación de memoria inferior.

Carpeta de destino de la copia de seguridad

La carpeta de destino dónde residen los archivos .D2D y los archivos del catálogo.

Tamaño de bloque

El tamaño de bloque de la deduplicación también afecta a la estimación de la capacidad de la deduplicación. El valor predeterminado del tamaño de bloque de deduplicación es de 16 KB. Si se establece en 32 KB, se doblará la estimación de la capacidad de la deduplicación. El impacto de aumentar el tamaño del bloque de deduplicación es la posible reducción del porcentaje de deduplicación y, al mismo tiempo, la disminución del requisito de memoria.

Adjudicación de memoria

Para calcular el requisito de memoria, use la herramienta Estimación de los requisitos de memoria y almacenamiento. Si la memoria adjudicada no es suficiente y si esta se ha utilizado completamente, los datos nuevos no pueden insertar un hash nuevo en la base de datos de hash. Así, los datos de los cuales se ha realizado una copia de seguridad posteriormente no podrán duplicarse, causando un descenso de la tasa de deduplicación. Si no se puede aumentar la

memoria por cualquier tipo de motivo, intente aumentar el tamaño de bloque de deduplicación del mismo modo que reduciría el requisito de memoria.

Nota: No se puede cambiar el tamaño de bloque para un almacén de datos existente.

Tenga en cuenta que no está permitido que una tarea de copia de seguridad nueva se inicie después de que la memoria hash se haya completado. Sin embargo, para la tarea de copia de seguridad en curso (que se ha iniciado antes de que la memoria de hash se complete), sí que está permitido continuar hasta que la memoria esté llena. En este caso, no insertaría claves hash nuevas a la base de datos de hash. Como resultado, hay un gran impacto en el porcentaje de deduplicación.

El motivo es que todos los bloques de datos en la tarea de copia de seguridad en curso se comparan todavía con las claves hash existentes en la base de datos de hash.

• Si se ha duplicado con la clave hash existente, ya no se podrá escribir en el disco.

• Si no se ha duplicado con la clave hash existente, se escribirá en el disco. Pero la nueva clave hash no se insertaría en la base de datos de hash puesto que la base de datos de hash está completa. Como resultado, los bloques de datos resultantes no se podrían comparar con estas claves de hash nuevas.

Deduplicación, cifrado y compresión

Además de la deduplicación de datos, se puede aplicar también la compresión y el cifrado en un almacén de datos.

Si se activa el cifrado, el Agente de Arcserve Unified Data Protection para Windows consume los recursos de la CPU para cifrar los datos. Como que el cifrado se aplica solamente a los datos únicos, los recursos de la CPU necesarios para el cifrado pueden ser mínimos cuando el porcentaje de deduplicación sea alto.

- Con la compresión y la deduplicación, el uso de la CPU es menor para la tarea de compresión y los datos almacenados tienen un formato no comprimido.
- Con la compresión y deduplicación estándar, el uso de la CPU es óptimo para la tarea de compresión y los datos almacenados tienen un formato comprimido y el requisito para el espacio de almacenamiento es menor.
- Con la compresión y deduplicación máxima, el uso de la CPU es máximo para la tarea de compresión, se almacena un 2-3 % más de datos y el requisito para el espacio de almacenamiento es menor.

Limitaciones de la deduplicación

Una vez que se haya creado un almacén de datos de deduplicación, no se podrá modificar el tipo de compresión, la configuración de cifrado y el tamaño del bloque de la deduplicación.