Guida alle soluzioni di Arcserve® Unified Data Protection

Versione 8.x

arcserve®

Guida in linea alle soluzioni Arcserve® Unified Data Protection

Versione 8.x

L'elenco dei contenuti viene visualizzato nel riquadro sinistro. Per visualizzare tutti gli argomenti, fare clic sull'icona TOC disponibile nella parte superiore.

arcserve®

Informazioni di carattere legale

La presente documentazione, che include il sistema di guida in linea integrato e materiale distribuibile elettronicamente (d'ora in avanti indicata come "Documentazione"), viene fornita all'utente finale a scopo puramente informativo e può essere modificata o ritirata da Arcserve in qualsiasi momento. Questa Documentazione contiene informazioni proprietarie di Arcserve e non può essere copiata, trasmessa, riprodotta, divulgata, modificata o duplicata per intero o in parte, senza la preventiva autorizzazione scritta di Arcserve.

Se l'utente dispone di una licenza per l'utilizzo dei software a cui fa riferimento la Documentazione, avrà diritto ad effettuare copie della suddetta Documentazione in un numero ragionevole per uso personale e dei propri impiegati, a condizione che su ogni copia riprodotta siano apposti tutti gli avvisi e le note sul copyright di Arcserve.

Il diritto a stampare copie della presente Documentazione è limitato al periodo di validità della licenza per il prodotto. Qualora e per qualunque motivo la licenza dovesse cessare o giungere a scadenza, l'utente avrà la responsabilità di certificare a Arcserve per iscritto che tutte le copie anche parziali del prodotto sono state restituite a Arcserve o distrutte.

NEI LIMITI CONSENTITI DALLA LEGGE VIGENTE, ARCSERVE FORNISCE LA DOCUMENTAZIONE "COSÌ COM'È" SENZA GARANZIE DI ALCUN TIPO, INCLUSE, IN VIA ESEMPLIFICATIVA, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ, IDONEITÀ A UN DETERMINATO SCOPO O DI NON VIOLAZIONE DEI DIRITTI ALTRUI. IN NESSUN CASO ARCSERVE SARÀ RITENUTA RESPONSABILE DA PARTE DELL'UTENTE FINALE O DA TERZE PARTI PER PERDITE O DANNI, DIRETTI O INDIRETTI, DERIVANTI DALL'UTILIZZO DELLA DOCUMENTAZIONE, INCLUSI, IN VIA ESEMPLIFICATIVA E NON ESAUSTIVA, PERDITE DI PROFITTI, INTERRUZIONI DELL'ATTIVITÀ, PERDITA DI AVVIAMENTO O DI DATI, ANCHE NEL CASO IN CUI ARCSERVE VENGA ESPRESSAMENTE INFORMATA IN ANTICIPO DI TALI PERDITE O DANNI.

L'utilizzo di qualsiasi altro prodotto software citato nella Documentazione è soggetto ai termini di cui al contratto di licenza applicabile, il quale non viene in alcun modo modificato dalle previsioni del presente avviso.

Il produttore di questa Documentazione è Arcserve.

Fornita con "Diritti limitati". L'uso, la duplicazione o la divulgazione da parte del governo degli Stati Uniti è soggetto alle restrizioni elencate nella normativa FAR, sezioni 12.212, 52.227-14 e 52.227-19(c)(1) - (2) e nella normativa DFARS, sezione 252.227-7014(b)(3), se applicabile, o successive.

© 2014-2021 Arcserve, incluse affiliate e controllate. Tutti i diritti riservati. Tutti i marchi o i diritti di copyright di terze parti sono di proprietà dei rispettivi titolari.

Riferimenti dei prodotti Arcserve

Questo documento fa riferimento ai seguenti prodotti Arcserve:

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

Contatto del Supporto tecnico di Arcserve

Il team del Supporto tecnico di Arcserveoffre un insieme di risorse per la risoluzione dei problemi tecnici e fornisce l'accesso a importanti informazioni sul prodotto.

Contatto con il supporto tecnico

Con Supporto tecnico di Arcserve:

- È possibile consultare direttamente la stessa libreria di informazioni che viene condivisa internamente dagli esperti del Supporto tecnico di Arcserve. Questo sito fornisce l'accesso ai documenti della Knowledge Base (KB). Da qui, è possibile cercare e trovare facilmente gli articoli della Knowledge Base relativi al prodotto e contenenti le soluzioni testate sul campo a molti problemi principali e comuni.
- È possibile utilizzare il collegamento Chat in tempo reale per avviare una conversazione in tempo reale con il team del Supporto tecnico di Arcserve. Con la Chat in tempo reale, è possibile ottenere risposte immediate alle proprie domande e preoccupazioni, mantenendo al contempo l'accesso al prodotto.
- È possibile partecipare alla Arcserve Global User Community per porre domande e rispondere, condividere suggerimenti e consigli, discutere su procedure consigliate e partecipare a discussioni con i propri colleghi.
- È possibile aprire un ticket di supporto. Quando si apre un ticket di supporto in linea, si verrà contattati da uno degli esperti nell'area del prodotto per il quale si richiede il supporto.
- È possibile accedere ad altre risorse utili relative al prodotto Arcserve.

Contenuti

Guida in linea alle soluzioni Arcserve® Unified Data Protection 2

Chapter 1: Funzionalità e miglioramenti 29

Nuove funzionalità 30

Miglioramenti delle funzionalità 32

Miglioramenti dell'agente Linux 33

Piattaforme e database supportati 34

Miglioramenti della protezione e delle terze parti 35

Miglioramenti apportati all'appliance Arcserve 36

Supporto eliminato 37

Chapter 2: Introduzione a Arcserve UDP 39

Introduzione 40

Funzionamento di Arcserve UDP 42

Computer virtuale istantaneo (IVM) e computer Virtual Standby (VSB) 44

Protezione utente 47

Ruoli per i servizi Arcserve UDP 48

Privilegi dell'utente per le funzioni di Arcserve UDP 49

Chapter 3: Installazione di Arcserve UDP 59

Installazione di Arcserve UDP 60

Verifica delle considerazioni e dei prerequisiti 61

Definizione del tipo di installazione 62

Installazione di Arcserve Unified Data Protection mediante la procedura guidata di installazione 63

Installazione di Arcserve Unified Data Protection mediante la riga di comando 67

Installazione di Arcserve UDP mediante il programma di installazione unificato 72

Verifica dell'installazione 74

Porte di comunicazione utilizzate da Arcserve UDP 75

Impatto del processo di installazione sui sistemi operativi 95

Installazione degli aggiornamenti di Arcserve UDP 101

Revisione delle considerazioni per l'installazione degli aggiornamenti 102

Indicazione delle preferenze di aggiornamento 103

Verifica e installazione degli aggiornamenti 109

Aggiornamento degli agenti sui nodi remoti mediante Gateway 111

Aggiornamento del server RPS sul server remoto mediante gateway 112

(Facoltativo) Installazione degli aggiornamenti di Arcserve UDP in modalità invisibile all'utente 113

Verifica dell'installazione degli aggiornamenti 115
Disinstallazione dell'Arcserve UDP 116
Disinstallazione standard 117
Disinstallazione invisibile all'utente 118
Rimozione dei componenti ignorati dal programma di disinstallazione 120
Chapter 4: Aggiornamento ad Arcserve UDP versione 8.0 123
Versioni supportate per l'aggiornamento 124
Sequenza di aggiornamento sull'appliance Arcserve 125
Aggiornamento dell'appliance Arcserve eseguita come console e server RPS Arcserve UDP 126
Aggiornamento dell'appliance Arcserve eseguita solo come server RPS Arcserve UDP 127
Procedura di aggiornamento per gli ambienti in cui vengono utilizzati due o più appliance Arcserve 128
Aggiornamento dell'agente Arcserve per Linux sull'appliance Arcserve UDP 129
Aggiornamento di Arcserve Backup sull'appliance Arcserve 130
Criterio per il supporto della compatibilità con le versioni precedenti 131
Criterio per il supporto della compatibilità con le versioni precedenti per Arcserve UDP versione 8.0 131
Criterio per il supporto della compatibilità con le versioni precedenti per Arcserve UDP versione 7.x 134
Criterio per il supporto della compatibilità per Arcserve UDP versione 6.5 Aggiornamento 4 137
Supporto della compatibilità con le versioni precedenti del server di backup Linux 140
Sequenza di aggiornamento per console UDP, server RPS e agente 141
Aggiornamento ad Arcserve UDP 8.0 da una release precedente 142
Aggiornamento ad Arcserve UDP 8.0 mediante il programma di installazione unificato 145
Aggiornamento ad Arcserve UDP 8.0 o Arcserve Backup 18.0 per abilitare la copia su nastro 149
Migrazione della console Arcserve UDP da un server a un altro 152
Aggiornamento del gateway alla stessa versione della console registrata 153
Migrazione della Console Arcserve UDP 153
Chapter 5: Esplorazione e configurazione di Arcserve UDP 157
Accesso alla console Arcserve UDP mediante l'autenticazione a più fattori 157
Verifica dei prerequisiti 157
Accesso alla console Arcserve UDP mediante MFA 158
Arcserve Unified Data Protection Interfaccia utente 163
Accesso ad Arcserve UDP 164
Schede 165

Finestra di dialogo Monitoraggio processi 180
Configurazione di Arcserve UDP 181
Configurazione del protocollo di comunicazione del server 182
Configurazione del database 184
Configurazione della sincronizzazione dati di backup di Arcserve 188
Configurazione di SRM 190
Configurazione rilevamento nodi 192
Configurazione di posta elettronica e avvisi 194
Configurazione delle impostazioni proxy 196
Configurazione aggiornamento 198
Configurazione dell'account di amministratore 200
Impostazioni di distribuzione remota 201
Mapping del piano sull'account utente 202
Gestione utenti 204
Configurazione della durata del timeout per la console 205
Migrazione dei punti di ripristino di Arcserve r16.5 a Arcserve UDP 206
Creazione di un archivio dati per la replica dei dati da un punto di ripristino Arcserve r16.5 207
Replica dei dati di Arcserve r16.5 nell'archivio dati UDP 208
Procedura guidata di configurazione 209
Chapter 6: Utilizzo delle funzionalità principali di Arcserve UDP 211
Nozioni fondamentali sulle funzionalità Nutanix in Arcserve UDP 212
Nozioni fondamentali sulle funzionalità OneDrive in Arcserve UDP 213
Informazioni sulla funzionalità di Exchange Online in Arcserve UDP 214
Informazioni sulla funzionalità di snapshot hardware in UDP 215
Informazioni sulla funzionalità cloud in UDP 216
Informazioni sulla funzionalità di percorso UNC/NFS in UDP 218
Informazioni sulla funzionalità di SharePoint Online in UDP 219
Prerequisiti 219
Chapter 7: Utilizzo dell'amministrazione basata sui ruoli di Arcserve UDP 221
Accesso alla console Gestione utenti 222
Avvio della console di gestione degli utenti Arcserve UDP 222
Configurazione dell'autenticazione a più fattori 223
Aggiunta di un utente, eliminazione di un utente e modifica della password 230
Configurazione della Gestione utenti 231
Ruoli predefiniti 232

Assegnazione di ruoli predefiniti 236
Visualizzazione e annullamento di un ruolo 237
Aggiunta di un nuovo ruolo 238
Ricerca di utenti e ruoli 240
Integrazione di Arcserve UDP con Active Directory 241
Integrazione di Arcserve UDP 8.0 con Active Directory mediante i gruppi di Windows 242
Integrazione di Arcserve UDP 8.0 con Active Directory mediante i gruppi di Active Directory 245
Accesso a Arcserve UDP tramite l'autenticazione integrata di Windows 251
Risoluzione dei problemi relativi all'autenticazione integrata di Windows (IWA) 252
Autenticazione integrata di Windows non supportata dalla Console Arcserve UDP se la connessione al database della Console utilizza la modalità di autenticazione di Windows 254
Risoluzione dei problemi 256
Chapter 8: Aggiunta e gestione dei nodi di origine 257
Aggiunta di nodi alla console 258
Verifica dei prerequisiti 259
Aggiunta di nodi 260
Rilevamento dei nodi 265
Importazione dei nodi 268
Gestione dei nodi 275
Verifica dei prerequisiti 276
Aggiornamento delle informazioni Hypervisor 277
Definizione dell'hypervisor 278
Aggiornamento delle informazioni del computer virtuale 280
Aggiornamento dei nodi 281
Esportazione del nodo 285
Sospensione del nodo 286
Ripresa del nodo 287
Sincronizzazione dei dati 288
Eliminazione di nodi dalla Console 289
Distribuzione dell'agente sui nodi 290
Esecuzione di verifiche preliminari per i processi di backup 291
Aggiunta e gestione del percorso UNC/NFS 309
Aggiunta di un percorso UNC/NFS 310
Aggiornamento del percorso UNC/NFS 313
Eliminazione di un percorso UNC/NFS 314
Aggiunta e gestione di gruppi di nodi 315

Verifica dei prerequisiti 317
Aggiunta di gruppi di nodi 318
Modifica di gruppi di nodi 319
Eliminazione di gruppi di nodi 320
Gestione dei nodi per il cloud 321
Download del punto di ripristino dal cloud 322
Caricamento del punto di ripristino su cloud 324
Copia del punto di ripristino su disco locale o condivisione di rete 327
Aggiunta di un array di archiviazione 330
Aggiunta di un array di archiviazione per NetApp 332
Aggiunta dei dettagli di HPE RMC che gestisce l'array di archiviazione HPE 3PAR StoreServ 338
Aggiunta di un array di archiviazione Nimble 340
Aggiunta e gestione di un sito 342
Definizione del nome del sito 344
Condivisione delle istruzioni di registrazione 345
Verifica e aggiunta del sito 346
Modifica dell'URL della console 347
Modifica del sito 348
Eliminazione di un sito 349
Impostazione di un server proxy per il gateway 350
Gestione dei nodi di Exchange Online 353
Aggiunta di un nodo Exchange Online 354
Aggiornamento di un nodo di Exchange Online 356
Eliminazione di un nodo di Exchange Online 357
Supporto delle caselle di posta delle cartelle pubbliche per la protezione di Exchange Online. 358
Gestione dei nodi SharePoint Online 359
Aggiunta di un nodo di SharePoint Online 360
Aggiornamento di un nodo di SharePoint Online 361
Eliminazione di un nodo di SharePoint Online 362
Come gestire i nodi OneDrive 362
Aggiunta di un nodo di OneDrive 363
Eliminazione di un nodo di OneDrive Online 363
Gestione dei nodi del gruppo di database Oracle 363
Aggiornamento del nodo del database Oracle 363
Esportazione del nodo 364

Backup del nodo del database Oracle 364
Annullamento del processo di backup dei nodi del database Oracle 366
Eliminazione dei nodi del database Oracle 367
Chapter 9: Aggiunta e gestione delle destinazioni 369
Aggiunta di una destinazione 370
Aggiunta di una destinazione 371
Aggiunta dei server Arcserve Backup 385
Aggiunta di una console remota 387
Aggiunta di un account cloud 389
Aggiunta di un account Arcserve Cloud 424
Gestione di un archivio dati 427
Verifica dei prerequisiti 428
Modifica di un archivio dati 429
Avvio di un archivio dati 439
Interruzione di un archivio dati 440
Eliminazione di un archivio dati della Console 442
Eliminazione dei dati del nodo dall'archivio dati 443
Monitoraggio della capacità di spazio disponibile per l'archivio dati 444
Accesso ai punti di ripristino in un archivio dati 452
Supporto FQDN per un archivio dati 454
Esecuzione manuale o su richiesta di un processo di unione 455
Modifica del limite di nodi attivi simultanei per il backup manuale 456
Risoluzione dei problemi: utilizzo di un archivio dati quando una o più cartelle sono piene 457
Gestione di un Recovery Point Server 459
Verifica dei prerequisiti 460
Aggiornamento di un Recovery Point Server 461
Eliminazione di un Recovery Point Server dalla Console 462
Importazione di un archivio dati 463
Installazione/Aggiornamento del Recovery Point Server 465
Gestione dei server Arcserve Backup 466
Aggiornamento del server Arcserve Backup 467
Eliminazione del server Arcserve Backup 468
Gestione di una cartella condivisa 469
Modifica di una cartella condivisa 470
Eliminazione di una cartella condivisa 471
Gestione di una console remota 472

Modifica di una console remota 473
Eliminazione di una console remota 474
Verifica della connessione della console remota 475
Chapter 10: Creazione di piani per la protezione dei dati 477
Presentazione dei piani e delle attività 478
Creazione di un piano di backup di Windows 482
Verifica delle considerazioni e dei prerequisiti 483
Creazione di un piano con un'attività di backup 489
(Facoltativo) Esecuzione di un backup manuale 512
Verifica del backup 514
Creazione di un piano di backup di Nutanix 515
Creazione di un piano di Virtual Standby per Nutanix AHV 516
Creazione di un computer virtuale istantaneo su Nutanix AHV 516
Creazione di un piano Assured Recovery per proteggere Nutanix AHV per un nodo Linux 516
Backup del volume cluster condiviso 516
Modifica delle impostazioni del computer dell'agente sul volume CSV di backup 518
Backup di volumi senza lettera di unità 519
Verifica dei prerequisiti 520
Montaggio del volume senza lettera di unità nella cartella NTFS 520
Definizione di un volume senza lettera di unità nel Registro di sistema. 521
Esecuzione del backup del volume selezionato 521
Creazione di un piano di backup di Linux 523
Verifica delle considerazioni e dei prerequisiti 524
Creazione di un piano di backup 525
(Facoltativo) Esecuzione di un backup manuale 547
Verifica del backup 549
Risoluzione dei problemi 550
Creazione di un piano di backup del computer virtuale basato su host 552
Verifica delle considerazioni e dei prerequisiti 554
Creazione di un piano di backup basato su host 560
(Facoltativo) Esecuzione di un backup manuale 598
Verifica del piano 601
Creazione di un piano di Virtual Standby su AWS EC2 602
Verifica delle considerazioni e dei prerequisiti 603
Creazione di un piano con un'attività di backup 611
Aggiunta al piano di un'attività Virtual Standby su EC2 628

(Facoltativo) Esecuzione manuale dell'attività Virtual Standby su EC2 634
Sospensione e riattivazione del processo Virtual Standby 635
Verifica del piano 637
Interruzione delle risorse EC2 637
Creazione di un computer Virtual Standby su un piano Microsoft Azure 639
Verifica delle considerazioni e dei prerequisiti 640
Creazione di un piano con un'attività di backup 641
Aggiunta al piano di un'attività Virtual Standby 642
(Facoltativo) Esecuzione manuale del processo Virtual Standby 650
Sospensione e riattivazione dell'heartbeat 651
Sospensione e riattivazione del processo Virtual Standby 652
Verifica del piano 654
Creazione di un piano di Virtual Standby 655
Verifica delle considerazioni e dei prerequisiti 656
Creazione di un piano con un'attività di backup 658
Aggiunta al piano di un'attività Virtual Standby 675
(Facoltativo) Esecuzione manuale del processo Virtual Standby 689
Sospensione e riattivazione dell'heartbeat 690
Sospensione e riattivazione del processo Virtual Standby 691
Verifica del piano 693
Creazione di un piano Assured Recovery 694
Verifica delle considerazioni e dei prerequisiti 695
Aggiunta di un'attività Assured Recovery al piano 697
(Facoltativo) Esecuzione manuale del processo Verifica Assured Recovery 711
Creazione di un piano di backup del percorso UNC/NFS 714
Verifica delle considerazioni e dei prerequisiti 715
Creazione di una condivisione file 715
Creazione di un piano di backup con un'attività del percorso UNC/NFS 720
(Facoltativo) Esecuzione di un backup manuale 740
Altre attività nel piano UNC/NFS 742
Verifica del backup 743
Protezione dei computer Virtual Standby 744
Verifica delle considerazioni e dei prerequisiti 745
Attivazione dei computer Virtual Standby 746
Protezione dei computer Virtual Standby dopo l'attivazione 752
Verifica della protezione del computer Virtual Standby 754

Protezione dei computer virtuali istantanei 755
Verifica delle considerazioni e dei prerequisiti 756
Attivazione di computer virtuali istantanei da un punto di ripristino 757
Protezione di un computer virtuale istantaneo al momento dell'attivazione 758
Verifica della protezione del computer virtuale istantaneo 759
Replica dei dati tra archivi dati gestiti da una console UDP 760
Verifica delle considerazioni e dei prerequisiti 761
Creazione di un'attività di backup 762
Aggiunta al piano di un'attività di replica 763
(Facoltativo) Esecuzione di una replica manuale 766
Verifica del piano 767
Replica dei dati tra archivi dati gestiti da console UDP diverse 768
Verifica dei prerequisiti 771
Creazione di un account utente per la Console di origine 772
Creazione di un piano per definire l'archivio dati di destinazione 773
Mapping del piano sull'account utente 776
Invio del piano e dei dettagli dell'account utente all'amministratore dell'origine 778
Ricezione del piano e dei dettagli dell'account utente dall'amministratore della destinazione 779
Creazione di un piano di replica per l'invio dei dati alla Console di destinazione 780
Verifica della replica dei dati 784
Esecuzione di una replica di dati non in linea utilizzando JumpStart RPS 785
Verifica dei prerequisiti 788
Creazione di un archivio dati temporaneo su una periferica esterna 789
Replica dei dati di origine sull'archivio dati temporaneo 790
Eliminazione dell'archivio dati temporaneo dalla Console di origine 791
Invio della periferica esterna alla posizione di destinazione 792
Ricezione della periferica esterna 793
Importazione dell'archivio dati temporaneo dalla periferica esterna 794
Creazione di un archivio dati di destinazione 795
Replica dei dati dall'archivio dati temporaneo all'archivio dati di destinazione 796
Verifica della replica dei dati 797
(Facoltativo) Impostazione del numero di nodi simultanei per JumpStart RPS 798
Esecuzione della replica inversa 798
Verifica dei prerequisiti 798
Esecuzione della replica ad hoc 799
Esecuzione della replica inversa dalla console remota sul server RPS on-premise 806

Creazione di un piano di copia dei punti di ripristino 814
Verifica delle considerazioni e dei prerequisiti 815
Creazione di un piano con un'attività di backup 816
Aggiunta di un'attività di copia dei punti di ripristino al piano 833
Verifica del piano 842
Creazione di un piano di copia file 843
Verifica delle considerazioni e dei prerequisiti 844
Creazione di un piano con un'attività di backup 845
Aggiunta di un'attività di copia file al piano 863
(Facoltativo) Esecuzione di una copia file manuale 874
Verifica del piano 875
Creazione di un piano di archiviazione file 876
Verifica delle considerazioni e dei prerequisiti 877
Creazione di un piano con un'attività di backup 878
Aggiunta di un'attività di archiviazione file al piano 896
(Facoltativo) Esecuzione di un'archiviazione file manuale 907
Verifica del piano 908
Creazione di un piano di copia su nastro 909
Verifica delle considerazioni e dei prerequisiti 910
Creazione di un piano con un'attività di backup 911
Aggiunta di un'attività di copia su nastro nel piano 912
Creazione e gestione di un computer virtuale istantaneo su Microsoft Azure 921
Verifica dei prerequisiti di un computer virtuale istantaneo su Microsoft Azure 922
Creazione di un computer virtuale su Microsoft Azure 923
Gestione di un computer virtuale istantaneo 932
Creazione e gestione di un computer virtuale istantaneo sui server Hyper-V e VMware ESX 935
Verifica dei prerequisiti per un computer virtuale istantaneo 937
Creazione di un computer virtuale istantaneo 940
Gestione di un computer virtuale istantaneo 956
Modalità di creazione e gestione di un computer virtuale istantaneo su Amazon EC2 962
Verifica dei prerequisiti per un computer virtuale istantaneo su Amazon EC2 963
Creazione di un computer virtuale istantaneo su Amazon EC2 964
Gestione di un computer virtuale istantaneo 973
Creazione di un piano per la replica intersito 979
Creazione di un piano per la replica intersito 981

Protezione dei dati di Microsoft Office 365 983
Autenticazione moderna 983
Creazione di un piano di backup di Exchange Online 990
Creazione di un piano di backup di SharePoint Online 1021
Creazione di un piano di backup per OneDrive Microsoft Office 365 1041
Gestione del backup e del ripristino di Microsoft Teams 1060
Verifica delle considerazioni e dei prerequisiti 1063
Aggiunta di un ruolo e di un gruppo obbligatori all'account di backup di Exchange Online per l'esecuzione di backup e ripristini 1065
Creazione di un piano di backup di Exchange Online 1067
Definizione dell'origine 1069
Definizione della destinazione 1078
Definizione della pianificazione 1079
Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione 1083
Definizione delle impostazioni avanzate 1086
Verifica dei prerequisiti 1108
Creazione di un piano di backup di SharePoint Online 1109
Definizione dell'origine 1111
Definizione della destinazione 1116
Definizione della pianificazione 1117
Definizione delle impostazioni avanzate 1121
Creazione e configurazione di computer virtuali istantanei simultanei su più hypervisor 1138
Selezione di un Recovery point server di origine 1140
Selezione della posizione dei computer virtuali 1141
Selezione dei server di ripristino 1146
Configurazione delle impostazioni dei computer virtuali 1148
Verifica di riepilogo 1153
Configurazione di computer Virtual Standby simultanei 1156
Chapter 12: Utilizzo di una snapshot hardware per il backup 1159
Utilizzo di una snapshot hardware per il backup 1160
Utilizzo della snapshot hardware per il backup senza agente VMware 1161
Considerazioni sul supporto NetApp iSCSI/FC per VMware 1163
Considerazioni sul supporto NFS per VMware 1167
Considerazioni sull'archiviazione Nimble quando è abilitata l'autenticazione CHAP 1170
Utilizzo della snapshot hardware per il backup senza agente Hyper-V 1172

Utilizzo della snapshot hardware per il backup basato sull'agente 1174
Verifica del backup completato utilizzando la snapshot hardware 1175
Chapter 13: Ripristino dei dati protetti 1177
Ripristino da un punto di ripristino 1178
Verifica delle considerazioni e dei prerequisiti di ripristino 1180
Definizione delle informazioni del punto di ripristino da ripristinare 1191
Ripristino del contenuto del punto di ripristino 1204
Verifica del corretto ripristino del contenuto 1205
Ripristino da una copia di file 1206
Verifica delle considerazioni e dei prerequisiti di ripristino 1208
Definizione delle informazioni di copia file da ripristinare 1211
Ripristino del contenuto di copia file 1223
Verifica del corretto ripristino del contenuto 1225
Ripristino da un archivio di file 1226
Verifica delle considerazioni e dei prerequisiti di ripristino 1227
Definizione delle informazioni di copia file da ripristinare 1229
Ripristino del contenuto del punto di ripristino 1241
Verifica del corretto ripristino del contenuto 1243
Ripristino di file/cartelle 1244
Verifica delle considerazioni e dei prerequisiti di ripristino 1246
Definizione delle informazioni di file/cartella da ripristinare 1257
Ripristino di file/cartelle 1275
Verifica del ripristino di file/cartella 1277
Esecuzione di un ripristino bare metal tramite un computer virtuale Virtual Standby o un computer virtuale istantaneo 1278
Verifica delle considerazioni e dei prerequisiti del ripristino bare metal 1280
Definizione delle opzioni di ripristino bare metal 1282
Verifica della corretta esecuzione del ripristino bare metal 1306
Informazioni di riferimento del ripristino bare metal 1307
Risoluzione dei problemi relativi al ripristino bare metal 1315
Ripristino di un computer virtuale 1322
Verifica delle considerazioni e dei prerequisiti di ripristino 1324
Definizione delle informazioni sul computer virtuale da ripristinare 1325
Ripristino del computer virtuale 1345
Verifica del ripristino del computer virtuale 1346
Ripristino di SQL Filestream 1346
Applicazione della patch T00002266 1347

Ripristino del database SQL nella posizione originale 1347
Ripristino del database SQL su un'istanza alternativa dello stesso server 1351
Ripristino del database SQL su un'istanza alternativa di un server diverso 1356
Ripristino del database SQL in una posizione alternativa della stessa istanza 1363
Modalità di ripristino tramite chiave di registro 1366
Uso dell'utilità Exchange Granular Restore (GRT) 1373
Introduzione 1374
Verifica delle considerazioni e dei prerequisiti 1375
Ripristino dei dati di Microsoft Exchange mediante l'utilità Exchange Granular Restore (GRT) 1376
Ripristino di un'applicazione Microsoft Exchange 1382
Verifica delle considerazioni e dei prerequisiti di ripristino 1384
Definizione delle informazioni di Microsoft Exchange da ripristinare 1386
Ripristino dell'applicazione Microsoft Exchange 1392
Verifica del ripristino dell'applicazione Microsoft Exchange 1394
Ripristino dei dati di Exchange su un computer virtuale VMware 1395
Download di file o cartelle senza ripristino 1396
Download di file/cartelle senza ripristino per i nodi Linux 1397
Ripristino di un'applicazione Microsoft SQL Server 1399
Verifica delle considerazioni e dei prerequisiti di ripristino 1401
Definizione delle informazioni di Microsoft SQL Server da ripristinare 1404
Ripristino dell'applicazione Microsoft SQL Server 1410
Verifica del ripristino dell'applicazione Microsoft SQL Server 1412
Ripristino da un percorso UNC/NFS 1413
Verifica delle considerazioni e dei prerequisiti di ripristino 1414
Definizione delle informazioni del percorso UNC/NFS da ripristinare 1415
Ripristino di file e cartelle e del contenuto presente nel percorso UNC/NFS 1425
Verifica del corretto ripristino del contenuto 1427
Ripristino di un database Oracle 1428
Verifica delle considerazioni e dei prerequisiti 1430
Ripristino del file dei parametri per il server 1431
Ripristino del file dei parametri 1432
Ripristino dei registri di ripristino archiviati 1433
Ripristino di spazi tabella o file di dati 1434
Ripristino del sistema o annullamento degli spazi tabella o dei file di dati 1436
Ripristino di tutti gli spazi tabella e i file di dati 1438
Ripristino dei file di controllo 1440

Ripristino del database intero (spazi tabella e file di controllo) 1442
Recupero del database Oracle mediante il ripristino bare metal 1444
Esecuzione di un ripristino a livello di file sui nodi Linux 1445
Verifica dei prerequisiti 1447
(Facoltativo) Ripristino dei dati dal volume iSCSI nel computer di destinazione 1448
Definizione del punto di ripristino per il backup basato sull'agente 1450
Definizione dei dettagli relativi al computer di destinazione 1456
Definizione delle impostazioni avanzate 1460
Creazione ed esecuzione del processo di ripristino 1465
Verifica del ripristino dei file 1467
Esecuzione di un ripristino a livello di file da nodi di backup senza agente basati su host per Linux 1468
Verifica dei prerequisiti 1469
Definizione del punto di ripristino 1470
Definizione dei dettagli relativi al computer di destinazione 1475
Definizione delle impostazioni avanzate 1479
Creazione ed esecuzione del processo di ripristino 1484
Verifica del ripristino dei file 1485
Migrazione di un computer virtuale istantaneo (da un punto di ripristino Linux) da cloud a locale 1486
Verifica dei prerequisiti e considerazioni per la migrazione di un computer virtuale Istantaneo 1487
Migrazione di un computer virtuale istantaneo da cloud a locale 1488
Esecuzione di un ripristino bare metal per computer Linux 1489
Verifica dei prerequisiti di ripristino bare metal 1492
Acquisizione dell'indirizzo IP del computer di destinazione con Live CD 1493
(Facoltativo) Ripristino dei dati nel volume iSCSI del computer di destinazione 1495
(Facoltativo) Ripristino dei dati dal volume iSCSI nel computer di destinazione 1497
Verifica del server di backup 1499
Definizione dei punti di ripristino 1501
Definizione dei dettagli relativi al computer di destinazione 1503
Definizione delle impostazioni avanzate 1505
Creazione ed esecuzione del processo di ripristino 1511
Verifica del ripristino del nodo di destinazione 1519
Esecuzione di un ripristino bare metal di migrazione per computer Linux 1520
Verifica dei prerequisiti per il ripristino bare metal di migrazione 1521
Esecuzione di un ripristino bare metal su un computer temporaneo 1522
Esecuzione del ripristino bare metal di migrazione 1524

Verifica del ripristino del nodo di destinazione 1526
Esecuzione di un ripristino bare metal mediante un backup 1527
Verifica delle considerazioni e dei prerequisiti del ripristino bare metal 1530
Definizione delle opzioni di ripristino bare metal 1532
Verifica della corretta esecuzione del ripristino bare metal 1553
Informazioni di riferimento del ripristino bare metal 1554
Risoluzione dei problemi relativi al ripristino bare metal 1562
Ripristino di dischi condivisi e nodi del cluster Microsoft 1570
Verifica dei prerequisiti 1571
Ripristino di file di un disco condiviso del cluster 1572
Ripristino di un nodo specifico in un cluster 1573
Ripristino di un disco condiviso corrotto del cluster 1574
Ripristino di tutti i dischi condivisi e nodi del cluster 1575
Ripristino di Active Directory 1577
Verifica delle considerazioni e dei prerequisiti di ripristino 1579
Ripristino di Active Directory 1580
Verifica del ripristino di Active Directory 1584
Ripristino dei dati di Active Directory mediante l'utilità di ripristino a livello di oggetto di Active Directory per Arcserve UDP 1584
Ripristino dei dati di Microsoft Office 365 Exchange 1592
Ripristino dei dati della casella di posta di Exchange Online 1593
Ripristino dei dati di una raccolta siti di SharePoint Online 1607
Ripristino dei dati di OneDrive 1618
Accesso al punto di ripristino della copia su nastro per il ripristino 1629
Procedura di ripristino temporizzato 1629
Prerequisiti 1630
Considerazioni 1630
Esecuzione del ripristino temporizzato 1631
Ripristino del volume cluster condiviso 1635
Verifica dei prerequisiti e delle considerazioni 1635
Definizione delle informazioni CSV per il ripristino 1643
Ripristino del contenuto CSV 1653
Chapter 2: Gestione del backup e del ripristino su nastro 1655
Backup di un archivio dati di deduplicazione su un nastro 1656
Ripristino di un archivio dati di deduplicazione da un nastro 1657
Verifica dei prerequisiti 1659
Ripristino da un supporto nastro su una posizione alternativa 1660

Importazione dell'archivio dati ripristinato sul server RPS 1661
Chapter 3: Utilizzo dell'interfaccia PowerShell 1663
Utilizzo dell'interfaccia PowerShell 1664
Revisione del prerequisito 1665
Utilizzo dell'interfaccia PowerShell per Arcserve UDP 1666
Sintassi e parametri di PowerShell 1667
Esempi di PowerShell 1680
File di configurazione e proprietà di PowerCLI 1684
Chapter 4: Protezione del sistema Oracle mediante Recovery Manager (RMAN) 1687
Verifica dei prerequisiti per i database Oracle con RMAN (Windows e Linux) 1688
Creazione di un piano di backup per il database Oracle (Windows e Linux) 1696
Creazione di un piano con un'attività di backup 1697
Aggiunta di un'attività Assured Recovery al piano 1719
(Facoltativo) Esecuzione di un backup manuale 1728
Ripristino di un database Oracle mediante RMAN 1730
Selezione degli elementi del database Oracle da ripristinare 1731
Definizione delle opzioni di ripristino 1739
Limitazioni 1753
Chapter 5: Protezione dell'ambiente Microsoft SharePoint 1755
Considerazioni sull'installazione per l'ambiente Microsoft SharePoint 1756
Esecuzione del backup dei server Microsoft SharePoint 1757
Revisione delle considerazioni 1758
Esecuzione di un backup del server SharePoint 1759
Ripristino di un ambiente SharePoint 1761
Ripristino mediante computer virtuale istantaneo 1762
Ripristino mediante l'interfaccia utente dell'agente Arcserve UDP 1772
Ripristino mediante montaggio del database da un punto di ripristino 1778
Creazione di una rete isolata per il ripristino SharePoint 1802
Creazione di una rete isolata per il ripristino SharePoint per il computer virtuale VMware 1803
Creazione di una rete isolata per il ripristino SharePoint per il computer virtuale Hyper-V 1808
Chapter 6: Generazione di rapporti Arcserve UDP 1811
Introduzione ai rapporti Arcserve UDP 1812
Rapporti Arcserve UDP 1813
Utilizzo di filtri e azioni 1828
Utilizzo dei rapporti Arcserve UDP 1830

Creazione di un profilo SLA 1831
Pianificazione dei messaggi di posta elettronica 1834
Invia rapporto per posta elettronica 1839
Generazione di un rapporto 1841
Personalizzazione dei giorni di conservazione per un rapporto sullo stato del processo 1842
Dimensioni dei dati non elaborati nel rapporto sulla capacità gestita per il backup senza agente basato su host del computer virtuale 1843
Visualizzazione dei valori effettivi di origine e di destinazione per i tipi di processi 1847
Chapter 7: Gestione di High Availability 1851
Funzionamento di High Availability 1852
Gestione dei servizi di controllo High Availability 1853
Gestione delle licenze High Availability 1854
Gestione di scenari 1855
Installazione remota 1869
Rapporti High Availability 1872
Chapter 8: Utilizzo dell'utilità VSphereConfig 1873
Attivazione o disattivazione del tag VSPhereBackupNFC mediante il prompt dei comandi 1873
Chapter 9: Utilizzo dell'utilità di diagnostica 1881
Raccolta di informazioni diagnostiche 1882
Acquisizione delle informazioni diagnostiche da un agente standalone 1884
Caricamento delle informazioni diagnostiche sul sito Web di Arcserve mediante FTP 1885
Estrazione dei registri dell'agente 1887
Estrazione dei registri della console 1888
Contenuti della cartella della cronologia dei registri ignorati tramite il Registro di sistema 1889
Raccolta di registri dal computer Gateway tramite la riga di comando 1889
Raccolta di registri dai server RPS mediante la riga di comando 1890
Raccolta di registri Stub da Hyper-V con l'agente installato 1891
Raccolta dei messaggi dal Visualizzatore eventi Hyper-V 1892
Raccolta della cartella Ca_lic e dei file OLF 1892
Raccolta degli elenchi di directory dalla destinazione di backup o dalle directory dell'archivio dati 1893
Chapter 10: Installazione manuale di Sophos Intercept X Advanced for Server su Arcserve UDP 1895
Chapter 11: Procedura consigliata 1901
Procedure consigliate per la protezione del server Arcserve UDP 1902
Esclusione di file dalla scansione antivirus 1903

Configurazione dei parametri di multistreaming 1904
Problemi correlati a Exchange Online 1905
Configurazione per prestazioni ottimali 1906
Procedure consigliate per il backup 1907
Procedura consigliata per il ripristino 1909
Domande frequenti su Exchange Online 1910
Problemi correlati a Microsoft Azure 1911
Procedure consigliate per un computer virtuale istantaneo su Microsoft Azure 1911
Distribuzione di Arcserve UDP su Microsoft Azure 1911
Chapter 12: Risoluzione dei problemi 1913
Problemi di comunicazione relativi ad Arcserve UDP 1914
Errore di comunicazione tra Arcserve UDP e i nodi Windows 1915
Impossibile ricevere gli avvisi di posta elettronica da account di Gmail 1916
Errore di comunicazione di Arcserve UDP con il server di backup di Linux di Arcserve UDP sui nodi remoti 1917
Errore di comunicazione di Arcserve UDP con il Recovery Point Server di Arcserve UDP sui nodi remoti 1918
Errore di comunicazione di Arcserve UDP con il server di backup di Arcserve sui nodi remoti 1920
Errore di comunicazione di Arcserve UDP con il sito remoto 1921
Problemi correlati a piano, processo e impostazioni 1922
Errore del processo di backup in seguito alla modifica del nome host/indirizzo IP della console 1923
Aggiunta di una password di crittografia per una destinazione crittografata esistente 1924
Errore di applicazione delle impostazioni di backup a un nodo 1925
Errore durante la distribuzione del piano in seguito alla modifica della password del computer proxy di backup senza agente 1926
Impostazioni disattivate durante l'apertura dell'interfaccia utente dell'agente 1927
Mancata sospensione e ripresa quando l'agente non è connesso alla rete 1928
Esecuzione rallentata del servizio dell'agente Arcserve UDP 1929
Configurazione del Registro di sistema per ripetere un processo di copia su nastro 1931
Configurazione del Registro di sistema per la copia di più punti di ripristino dello stesso tipo su un nastro dello stesso processo 1932
File/cartella ignorati dal backup della cartella NFS condivisa o nome del file o della cartella convertiti in elementi indesiderati 1933
Errore di backup della cartella NFS condivisa 1933
Reimpostazione della console UDP abilitata per MFA quando TOTP non è disponibile 1933
Problemi correlati al computer virtuale istantaneo 1940
Impossibile creare un computer virtuale istantaneo in VMware a causa del nome duplicato per l'archivio dati NFS 1941

Impossibile creare un computer virtuale istantaneo utilizzando Windows 2008 R2 come server di ripristino per i server VMware o Windows 2008 R2 Hyper-V 1942

Errore di avvio di un computer virtuale istantaneo nel caso di un server Windows AD 2008/2012/2016 1943

Non è possibile attivare il computer virtuale dopo il ripristino di Hyper-V 1945

Processo del computer virtuale istantaneo non riuscito a causa di un errore del servizio Windows NFS 1946

Impossibile accedere o eliminare la cartella del file del computer virtuale istantaneo pur disponendo dei privilegi di amministratore. 1947

Mancato avvio del computer virtuale istantaneo in Hyper-V dopo il riavvio del server di ripristino 1948

Impossibile creare l'archivio dati NFS VMware. Errore visualizzato: Impossibile risolvere il nome host 1949

Impossibile distribuire il servizio di integrazione al computer virtuale guest in Hyper-V 1951

Errore del computer virtuale istantaneo Linux su un server Hyper-V in lingua non inglese 1952

Utilizzo di altre licenze per i percorsi UNC che si trovano in un computer virtuale Hyper-V su licenza 1953

Visualizzazione di un errore di licenza se si modifica l'edizione o il tipo di licenza e si crea un computer virtuale istantaneo 1953

Problemi correlati all'agente Linux 1955

Impostazioni della destinazione di backup disattivate durante l'apertura dell'interfaccia utente dell'agente Linux 1956

Lo stato del processo, la cronologia del processo e il Registro attività non sono visibili 1957

Non è possibile ripristinare il volume di sistema di SUSE15 con file system XFS 1958

Problemi correlati al ripristino 1959

Errore di ripristino dei file 1960

Aggiunta del database del contenuto ripristinato all'applicazione Web originale 1961

Impossibile eseguire il montaggio del database durante il ripristino del database di Microsoft Exchange 1964

Il campo Da non viene visualizzato correttamente nei messaggi di posta elettronica inviati dagli utenti che dispongono delle autorizzazioni per conto di altri per una casella di posta condivisa 1966

Processi di ripristino non riusciti dopo backup di integrazione leggeri 1967

Modifica del nome del file in un elemento indesiderato causata dal ripristino sulla cartella NFS condivisa 1967

Problemi correlati a gateway, server RPS, archivio dati, console e database 1969

Il nome dell'archivio dati è già in uso 1970

Impossibile connettersi all'archivio dati a causa di un problema DNS 1971

Passaggio dell'archivio dati alla modalità di solo ripristino 1972

Errore in caso di versione RPS precedente alla versione della console 1974

Aggiunta della stessa risorsa in siti diversi non supportata 1975

Abilitazione dei troncamenti di registro quando il database SQL è in modalità di ripristino Estesa ... 1976

Punti di ripristino disponibili non mostrati con Sfoglia punti di ripristino quando il server RPS è configurato con il nome FQDN ... 1978

Accesso negato durante l'aggiunta del server RPS ... 1979

Assegnazione di privilegi e ruoli di amministratore a un utente di dominio ... 1980

Impossibile passare alla visualizzazione UDP per il punto di ripristino ... 1983

Errore di accesso negato durante l'aggiunta o l'aggiornamento dei nodi ... 1984

Errore di apertura della console UDP in caso di modifica della password dell'amministratore di SQL ... 1986

Impossibile montare i punti di ripristino a causa del timeout ... 1987

Aggiornamento delle credenziali del server gateway ... 1988

Aggiornamento del gateway in caso di modifica delle credenziali per il proxy gateway ... 1990

Messaggio "Avvio del server di identità in corso" mostrato nella console ... 1992

Problemi correlati a backup e ripristino del computer virtuale ... 1993

Aggiunta delle autorizzazioni per VDDK a livello del server vCenter ... 1996

Il processo di backup per il modello di computer virtuale viene sempre convertito in backup completo e la dimensione dei dati di backup corrisponde alla dimensione di provisioning del disco virtuale ... 2003

I dischi indipendenti vengono ignorati dal processo di backup del modello del computer virtuale ... 2005

Processo di backup per computer virtuale su condivisione SMB 3.0 non riuscito con messaggio di errore ... 2007

Processo di ripristino per computer virtuale non riuscito in caso di ripristino del computer virtuale su una condivisione di file predefinita di Windows ... 2008

Informazioni sul volume non disponibili per il punto di ripristino ... 2009

Conversione del backup incrementali in backup di verifica in quanto le snapshot del computer virtuale sono state modificate dopo l'ultimo processo di backup o richiedono il consolidamento ... 2010

Errore del backup senza agente per il computer virtuale VMware se la periferica CD/DVD del computer virtuale viene associata a un'immagine ISO contenuta in un archivio dati NFS non connesso ... 2011

Errore del backup senza agente basato su host per computer virtuale Hyper-V dopo l'aggiornamento di Arcserve UDP ... 2012

Errore del backup senza agente basato su host in VMware ESXi 6.0 ... 2013

Arresto anomalo del backup senza agente basato su host quando si utilizza Windows 2003 R2 a 64 bit come proxy di backup ... 2015

Modalità di trasporto HotAdd non utilizzata dal backup senza agente basato su host ... 2016

Modalità di trasporto NBD o NBDSSL utilizzata dal processo di backup o ripristino senza agente basato su host anche quando è disponibile la modalità SAN ... 2017

Impossibile creare una snapshot per computer virtuali Hyper-V quando sono in esecuzione più processi ... 2019

Snapshot VSS non creata con Hyper-V ... 2021

Impossibile eseguire il backup del disco virtuale a causa di un errore di sistema=[la periferica non è pronta (21)] 2022

Errore del processo di backup 2023

Errore di importazione dei computer virtuali VMware da vCenter 2025

Backup non riusciti a causa della licenza ESXi 2026

Modalità di trasporto HotAdd non funzionante durante il backup di un computer virtuale VMware 2027

Controllo più granulare per VSS su un sistema operativo guest Windows disattivato 2029

Non è possibile configurare il computer virtuale per abilitare il parametro "Disk.EnableUUID" 2031

Errore delle operazioni di recupero durante il recupero dei dati mediante la modalità di trasporto HOTADD o SAN 2033

Operazione di recupero del computer virtuale non riuscita se è selezionata una porta non predefinita 2035

Errori del processo di backup incrementale o completo pianificato per il computer virtuale Hyper-V 2036

Errore del writer Hyper-V VSS NTDS durante l'acquisizione di snapshot VSS nel computer virtuale 2037

Le modifiche all'indirizzo MAC non vengono memorizzate dopo il ripristino del computer virtuale 2038

Errore di ripristino del computer virtuale - Impossibile aprire i file VMDK 2039

Problemi causati da UUID duplicati del computer virtuale 2041

Errore del processo di catalogo file system o della verifica del punto di ripristino per il backup senza agente basato su host 2043

Conversione del backup incrementale per verificare il backup o aumento delle dimensioni di backup in Hyper-V 2045

Il backup basato su host non riesce per un computer virtuale Hyper-V con una speciale configurazione del disco di differenziazione 2047

Backup Job Fails for a VMware Virtual Machine (Il processo di backup non riesce per un computer virtuale VMware) 2048

Disabilitazione della ripetizione della scansione delle schede HBA durante il backup incrementale 2050

Creazione di snapshot consecutive disabilitata in un computer virtuale VMware per il backup 2051

Blocco in fase di avvio del computer virtuale in seguito al ripristino da una versione successiva dell'host ESXi a una versione precedente dell'host ESXi 2052

RAM utilizzata al 99% durante l'inoltro dei processi di backup al computer virtuale 2053

Errore del processo di ripristino Hyper-V. Errore di connessione dell'utilità sull'host 2054

Errore della protezione automatica durante il rilevamento e la protezione del computer virtuale 2056

Impostazione della dimensione del blocco di lettura durante il backup del file VMDK 2059

Prenotazione dello spazio LUN acquisita tramite l'esecuzione del clone Lun 2059

Problemi correlati a Virtual Standby 2061

Sistema operativo non trovato 2062

Errore dei processi di standby virtuale causato da errori interni 2063
Errore dei processi Virtual Standby mediante la modalità di trasporto HotAdd 2066
Errore dei processi Virtual Standby verso sistemi Hyper-V 2068
Problema relativo alla duplicazione dell'agente UUID 2069
Le modifiche apportate a Virtual Private Cloud nell'attività Virtual Standby non vengono riportate in Amazon EC2 2069
Opzione Risorse Terminal EC2 non visualizzata 2070
Problemi correlati alla copia del punto di ripristino 2071
Configurazione del registro per il processo di copia del punto di ripristino 2072
Congestione della larghezza di banda con i processi di copia del punto di ripristino su cloud 2073
Processo di unione ignorato 2075
Problemi correlati ai rapporti Arcserve UDP 2077
Visualizzazione dei grafici a barre per visualizzare i rapporti Arcserve UDP 2078
Problemi correlati a Microsoft Exchange Online Office 365 2081
Errore di visualizzazione dell'elenco delle caselle di posta nella finestra di dialogo Seleziona destinazione 2081
Accesso o autorizzazione negata per il gruppo Exchange Online 2082
Chapter 13: Appendice 2085
Strumento della riga di comando per l'archivio dati di deduplicazione 2086
Visualizzazione dell'opzione di verifica del punto di ripristino 2090
Applicazione di una versione differente di VDDK rispetto alla versione integrata in Arcserve UDP 2093
Modifica manuale di VDDK per il backup di Virtual Standby (VSB) 2093
Modifica manuale di VDDK per il backup basato su host (HBBU) 2094
Migrazione dei dati di backup di Arcserve D2D r16.5 per due server con nome host identico nell'archivio dati RPS 2096
Distribuzione di Arcserve UDP in Microsoft Azure 2097
Informazioni sul flusso di processo 2097
Considerazioni 2098
Pianificazione della distribuzione di Arcserve UDP in Microsoft Azure 2099
Distribuzione di Arcserve UDP in Microsoft Azure 2111
Termini e definizioni relativi ad Arcserve UDP 2123
Backup basato su agente 2123
Compressione 2123
configurazione 2124
Dashboard 2124
Archivio dati 2124

Destinazione 2124
Nodi rilevati 2124
Crittografia 2125
Deduplicazione globale 2127
Backup senza agente basato su host 2127
Modalità di trasporto HOTADD 2127
Processo 2127
Processi 2127
Modalità di trasporto NBD 2128
Modalità di trasporto NBDSSL 2128
Nodi 2128
Piano 2128
Nodi protetti 2128
Evento recente 2128
Punto di ripristino 2128
Recovery Point Server 2129
Replica 2129
Risorse 2129
Modalità di trasporto SAN 2129
Sistemi 2129
Attività 2129
Nodi non protetti 2129
Deduplicazione dei dati 2131
Tipi di deduplicazione dei dati 2132
Funzionamento della deduplicazione dei dati 2133
Scenari in cui è consigliabile l'utilizzo della deduplicazione 2135
Configurazione degli archivi dati di deduplicazione in Arcserve UDP 2136
Deduplicazione, crittografia e compressione 2138
Limitazioni della deduplicazione 2139

Chapter 1: Funzionalità e miglioramenti

In questa sezione sono illustrati le funzionalità o i miglioramenti forniti in ogni release di Arcserve UDP. La soluzione Arcserve UDP fornisce una soluzione inclusiva per i problemi di archiviazione di ultima generazione delle organizzazioni che provano a proteggere i propri dati in un mondo virtuale, cloud e di servizi in continua evoluzione. Tutto ciò è possibile grazie a una singola interfaccia utente per una vasta gamma di funzionalità che forniscono continuità alle imprese con più sedi e una soluzione rapida ai problemi in caso di emergenza.

In questa sezione vengono fornite informazioni su nuove funzionalità, miglioramenti e supporto.

La presente sezione descrive i seguenti argomenti:

Nuove funzionalità

Importante! Per informazioni sulle funzioni più recenti, consultare UDP 8.1.

Di seguito vengono elencate le nuove funzionalità disponibili in Arcserve UDP 8.0.

- **Backup e ripristino da volumi nascosti**: è consentito eseguire il backup e il ripristino dei dati da volumi nascosti. Il volume nascosto è un volume montato senza una lettera di unità o un percorso di cartella nel sistema operativo. È possibile accedere ai volumi nascosti utilizzando il GUID del volume corrispondente.
- **Impostazioni di esportazione e importazione**: è consentito esportare e importare le impostazioni utilizzando il file JSON nell'agente Windows.
- **Supporto OneDrive**: opzioni di ripristino consentite nelle posizioni originali o alternative.
- **Supporto SharePoint Online**: le seguenti funzionalità sono disponibili per il Supporto SharePoint Online:
  - È consentito eseguire il backup di elenchi e librerie da siti personali.
  - È consentito aggiungere più raccolte di siti contemporaneamente.
  - È consentito aggiungere automaticamente le raccolte di siti appena aggiunte al piano.
- **Supporto Oracle RMAN**: Arcserve UDP fornisce ora un metodo di protezione del sistema Oracle mediante Recovery Manager (RMAN). RMAN è un'utilità di Oracle che consente di eseguire attività di backup, ripristino e recupero sui database, nonché automatizzare l'amministrazione delle strategie di backup. Per ulteriori informazioni, consultare la sezione Protezione del sistema Oracle mediante Recovery Manager (RMAN).
- **Supporto di gruppo Office 365**: supporto di gruppo attivato per gli utenti di Office 365.
- **Replica inversa**: replica dei dati abilitata (punto di ripristino) da RPS cloud, MSP o gestito in remoto sul server UDP locale o sul server RPS on-premise. Per ulteriori informazioni, consultare la sezione Esecuzione della replica inversa.
- **Nutanix Files**: Arcserve UDP fornisce ora una modalità per proteggere Nutanix Files utilizzando l'opzione UNC/NFS di Arcserve UDP. Nutanix Files è una soluzione di archiviazione di file con scalabilità orizzontale definita dal software che fornisce un repository per i dati non strutturati, quali home directory, profili utente, condivisioni dipartimentali, registri delle applicazioni,

backup e archivi. Per ulteriori informazioni, consultare la sezione Protezione del percorso UNC/NFS.

- **Supporto di Teams**: il supporto per il backup e il ripristino dei dati è abilitato per MS Teams, una piattaforma di comunicazione aziendale basata su chat. Per ulteriori informazioni, consultare la sezione Gestione del backup e del ripristino di Microsoft Teams.
- **Supporto dell'archiviazione non modificabile per la copia del punto di ripristino**: è consentito creare l'archiviazione non modificabile su Amazon S3 utilizzando la funzione di blocco degli oggetti.
- **Sostituzione di Adobe Flash**: Adobe Flash non è più necessario e l'installazione di .NET Framework consente di visualizzare i grafici.

Miglioramenti delle funzionalità

Importante! Per informazioni sui miglioramenti più recenti delle funzionalità, consultare UDP 8.1.

- **Modifiche a PowerCLI**: le seguenti opzioni sono abilitate per i file di registro UDPPowerCLI.log:
  - È consentito modificare la posizione dei file di registro UDP PowerCLI.
  - È consentito verificare la dimensione massima dei file di registro mediante la circolazione dei registri.
  - Il timestamp nei file di registro viene modificato nel formato 24 ore.
  - Criterio di conservazione consentito basato sul periodo di conservazione per i file di registro UDP PowerCLI.
  - Criterio di conservazione consentito basato sul numero di file conservazione per i file di registro UDP PowerCLI.
- **Miglioramento della snapshot**: è stato attivato il piano di backup dell'agente Arcserve UDP (Windows/Linux) e il piano di backup senza agente basato su host (Nutanix/ESXI/Hyper-V) per eseguire lo script di snapshot successivo anche quando la snapshot produce un errore.
- **Autenticazione moderna**: l'autenticazione moderna è stata abilitata per il backup e il ripristino di Office 365.
- **Definizione della rete per il ripristino e la replica**: è stato attivato il ripristino e la replica mediante una rete per stabilire la comunicazione tra l'agente Windows e il Recovery Point Server.
- **Definizione della rete per Linux**: backup e ripristino abilitati utilizzando una rete per stabilire la comunicazione tra l'agente Linux e il Recovery Point Server.
- **Computer virtuale istantaneo simultaneo**: è consentito creare e configurare computer virtuali istantanei simultanei su più hypervisor utilizzando la console Arcserve UDP.
- **VSB simultaneo**: è consentito configurare computer virtuali di standby simultanei utilizzando la console Arcserve UDP.

Miglioramenti dell'agente Linux

Importante! Per informazioni sui miglioramenti più recenti dell'agente Linux, fare riferimento a UDP 8.1.

- Nuove piattaforme supportate:
  - 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
- **Definizione della rete per Linux**: backup e ripristino abilitati utilizzando una rete per stabilire la comunicazione tra l'agente Linux e il Recovery Point Server.
- **Computer virtuale istantaneo simultaneo**: è consentito creare e configurare computer virtuali istantanei simultanei su più hypervisor utilizzando la console Arcserve UDP.
- **Miglioramento della snapshot**: è stato attivato il piano di backup Linux dell'agente Arcserve UDP per eseguire lo script successivo alla snapshot anche quando la snapshot non riesce.
- **Sostituzione di Adobe Flash**: Adobe Flash non è più necessario per visualizzare i grafici sull'agente Linux.

Piattaforme e database supportati

Importante! Per informazioni sul supporto più recente per database e piattaforme, consultare 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 Aggiornamento 1
- Database Oracle 19c
- Nutanix Files 3.8.z, 3.7.z, 3.6.z

Miglioramenti della protezione e delle terze parti

Importante! Per informazioni sui miglioramenti più recenti della protezione e di terze parti, fare riferimento a UDP 8.1.

- **Supporto Open JDK**: la versione di Open JDK è stata aggiornata alla 1.8.0.265.b01
- **Supporto di VMware Virtual Disk Development Kit:** la versione di VDDK è stata aggiornata alla 7.0. 1.40833
- **Supporto SDK per i servizi Web VMware vSphere:** la versione SDK è stata aggiornata alla 6.7.1
- **Supporto WSO2**: la versione di WSO2 è stata aggiornata alla v5.7.0
- **Supporto Apache:** la versione di Apache è stato aggiornata alla 2.4.46
- **Supporto OpenSSL:** la versione di OpenSSL è stata aggiornata alla 1.1.1i
- **Supporto Tomcat:** la versione di Tomcat è stata aggiornata alla 9.0.37
- **Supporto SQLite**: la versione di SQLite è stata aggiornata alla 3.26
- **SDK AWS for Java**: la versione di AWS SDK for Java è stata aggiornata alla 1.11.852
- **SDK AWS for C++**: la versione di SDK AWS for C++ è stata aggiornata alla 1.6.53

Miglioramenti apportati all'appliance Arcserve

Importante: Per informazioni sui miglioramenti più recenti apportati all'appliance, fare riferimento a UDP 8.1.

I clienti dell'appliance esistente possono eseguire l'aggiornamento ad Arcserve UDP 8.0. Per ulteriori informazioni, consultare la sezione Installazione.

Supporto eliminato

Importante: Per informazioni sugli elementi di supporto eliminati, fare riferimento a UDP 8.1.

- Supporto di vSphere 5.5. Si consiglia di aggiornare l'ambiente (vCenter/ESXi) alla versione più recente supportata da VMware. Per ulteriori informazioni sulla fine del supporto generale per vSphere 5.5, consultare l'articolo della Knowledge Base.
- Nutanix AHV 5.5.3.1.

Chapter 2: Introduzione a Arcserve UDP

La presente sezione descrive i seguenti argomenti:

Introduzione

Arcserve Unified Data Protection è una soluzione completa per la protezione di ambienti IT complessi. La soluzione protegge i dati presenti in vari tipi di nodi, ad esempio Windows, Linux e computer virtuali su server VMware ESX, Microsoft Hyper-V o Nutanix AHV. È possibile eseguire il backup dei dati su un computer locale o su un Recovery Point Server. Un Recovery Point Server è un server centrale in cui vengono archiviati i backup da più origini.

Arcserve UDP fornisce le seguenti funzionalità:

- Consente di proteggere vari tipi di nodi di origine, tra cui quelli basati sull'agente, quelli senza agente, CIFS, Exchange Online, SharePoint Online, OneDrive e così via.
- Esecuzione del backup dei dati su Recovery Point Server
- Replica dei dati di backup su Recovery Point Server locali e remoti
- Monitoraggio di Arcserve High Availability
- Archiviazione dei dati
- Copia di:
  - file di origine selezionati in una posizione di backup secondaria
  - punti di ripristino in posizioni cloud e locali, quali ad esempio la cartella condivisa e AWS EC2
  - punti di ripristino su nastro
- Creazione di:
  - Computer Virtual Standby dai dati di backup nell'hypervisor locale (Hyper-V, ESX, Nutanix), AWS EC2 o Microsoft Azure
  - Computer virtuale istantaneo nell'hypervisor locale (Hyper-V, ESX, Nutanix) per Windows
  - Computer virtuale istantaneo nell'hypervisor locale (Hyper-V, ESX, Nutanix), AWS EC2 o Microsoft Azure for Linux
- Ripristino di:
  - dati di backup ed esecuzione del ripristino bare metal (BMR)
  - Oggetti di posta elettronica e non di Microsoft Exchange che utilizzano l’utilità Exchange Granular Restore di Arcserve UDP.

Nota: per ulteriori informazioni sulle specifiche e sulle altre funzionalità supportate, consultare la Guida per l'utente di Exchange Granular Restore (esr.pdf).

- Supporto di:
  - amministrazione basata sui ruoli
  - Snapshot hardware
  - Verifica Assured Recovery per i punti di ripristino
  - Rapporto SLA per RTO e RPO

Arcserve UDP consente di replicare i dati di backup salvati come punti di ripristino da un server a un altro del Recovery Point Server. Dai dati di backup è anche possibile creare computer virtuali utilizzabili come computer di standby in caso di errore del nodo di origine. Il computer virtuale di standby viene creato mediante la conversione dei punti di ripristino nel formato del computer virtuale VMware ESX, Microsoft Hyper-V o Nutanix AHV.

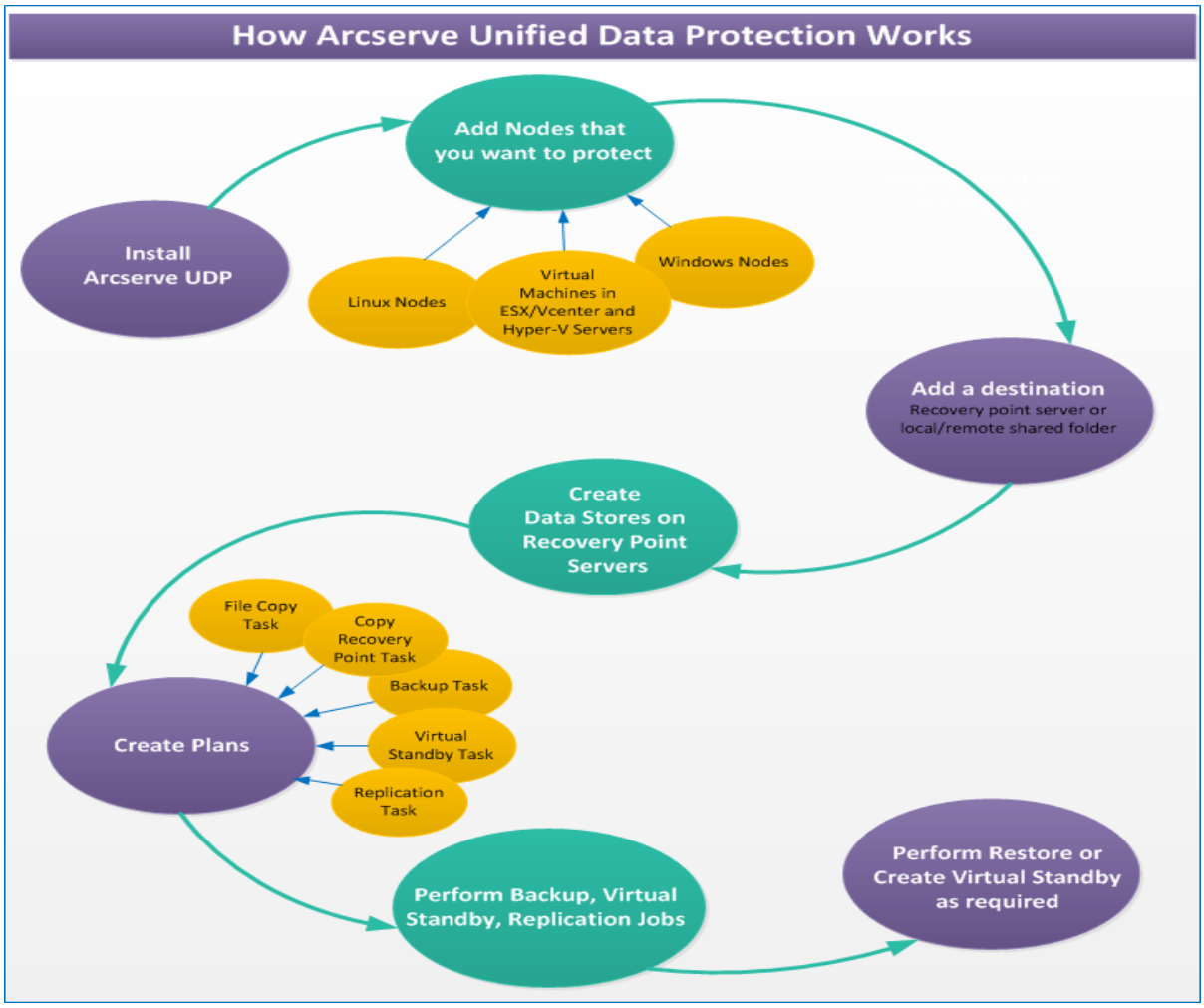
La soluzione Arcserve UDP fornisce l'integrazione con Arcserve High Availability. Dopo la creazione degli scenari in Arcserve High Availability, è possibile gestire e monitorare i propri scenari ed eseguire operazioni quali l'aggiunta o l'eliminazione di computer di destinazione.

Funzionamento di Arcserve UDP

Arcserve UDP è una soluzione di protezione dei dati unificata che consente di proteggere i sistemi informatici. Attenersi alla seguente procedura generica per la protezione dei sistemi mediante Arcserve UDP.

1. Installare Arcserve Unified Data Protection.
2. Aggiungere i nodi che si desidera proteggere. È possibile aggiungere i nodi Windows o Linux e i computer virtuali ai server ESX/vCenter, Hyper-V e Nutanix AHV.
3. Aggiungere una destinazione. Per destinazione si intende un Recovery Point Server, una cartella locale o una cartella condivisa remota.
4. Creare archivi di dati sul Recovery Point Server. Un archivio dati è un'area fisica su un disco. È possibile creare archivi dati di deduplicazione e di non deduplicazione.
5. Creare un piano. Un piano è un gruppo di attività per la gestione di attività di backup, di replica, di copia del punto di ripristino, di copia su nastro, di creazione di computer Virtual Standby o di test di Assured Recovery. È inoltre possibile aggiungere un percorso UNC, Office 365 Exchange Online, un nodo SharePoint Online o un nodo OneDrive e creare attività correlate.
6. Eseguire processi di backup, di creazione Virtual Standby e di replica.
7. Eseguire un ripristino semplice o un ripristino bare metal.

   Il diagramma seguente mostra le operazioni di livello superiore che è necessario eseguire per la protezione dei dati:


How Arcserve Unified Data Protection Works
Add Nodes that you want to protect
Install Arcserve UDP
Linux Nodes
Virtual Machines in ESX/Vcenter and Hyper-V Servers
Windows Nodes
Add a destination
Recovery point server or local/remote shared folder
Create Data Stores on Recovery Point Servers
File Copy Task
Copy Recovery Point Task
Backup Task
Virtual Standby Task
Replication Task
Create Plans
Perform Backup, Virtual Standby, Replication Jobs
Perform Restore or Create Virtual Standby as required

Computer virtuale istantaneo (IVM) e computer Virtual Standby (VSB)

In fase di ripristino dei dati dopo un'emergenza o durante un corso di Disaster Recovery, potrebbe essere necessario avviare le istanze virtualizzate dei server protetti in precedenza con Arcserve UDP.

Arcserve UDP offre le seguenti due funzionalità per l'avvio del computer virtuale dai punti di ripristino:

- **Computer virtuale istantaneo (IVM)**: consente di creare un computer virtuale immediatamente da un punto di ripristino. Utilizzando un computer virtuale istantaneo è possibile ottenere accesso immediato ai dati e alle applicazioni presenti nelle sessioni di backup di Arcserve UDP. Un computer virtuale istantaneo elimina i tempi di inattività associati a un ripristino tradizionale o alla conversione della sessione di backup in un computer fisico o virtuale.

  Per ulteriori informazioni sul computer virtuale istantaneo, consultare la sezione Creazione e gestione di un computer virtuale istantaneo.

- **Computer Virtual Standby (VSB)**: converte i punti di ripristino in formati di computer virtuale e prepara una snapshot per recuperare facilmente i dati qualora necessario. Questa funzionalità fornisce anche la capacità High Availability e garantisce che il computer virtuale possa intervenire immediatamente quando si verifica un errore nel computer di origine. Il computer Virtual Standby viene creato convertendo i punti di ripristino in un formato di computer virtuale VMware, Hyper-V o Nutanix AHV qualsiasi.

  Per ulteriori informazioni su Virtual Standby, consultare la sezione Creazione di un piano Virtual Standby.

Per determinare qual è la funzionalità più adatta, è necessario tener conto degli obiettivi desiderati in materia di tempo di ripristino (RTO) e del proprio scenario. La seguente tabella permette di confrontare le funzionalità IVM e VSB:

FUNZIONALITÀ	IVM	VSB
Attivazione dei computer virtuali di standby dal punto di ripristino più recente	Sì (conversione non necessaria)	Sì, SOLO se è stata aggiunta un'attività VSB al piano di backup. Ad esempio, è richiesta la pianificazione avanzata
Richiede l'elaborazione dei tempi di backup	Non obbligatorio	Obbligatorio. È necessario aggiungere un'attività VSB al piano utilizzato per il backup del computer di origine.
Tempi di avvio del com-	Elaborazione più lenta (fino al	Stessi tempi degli altri computer

puter virtuale	30%) a causa del reindirizzamento I/O.	virtuali sullo stesso hypervisor.
Requisiti di spazio su disco	È richiesto uno spazio di archiviazione minimo per ospitare un disco secondario o per archiviare le modifiche apportate durante l'esecuzione di un computer virtuale.	Sì, lo spazio di archiviazione viene utilizzato nell'hypervisor di destinazione in cui è gestito il computer virtuale di standby VSB. È richiesto uno spazio di archiviazione uguale o superiore alle dimensioni del computer di origine.
Opzione High Availability (HA)	N/D	DISPONIBILE Consente di monitora il computer di origine e di avviare il computer virtuale VSB se quello di origine non è più disponibile.
Prestazioni del computer virtuale	L'elaborazione potrebbe essere più lenta rispetto ai normali computer virtuali (fino al 30%) a causa del reindirizzamento I/O, tuttavia le prestazioni variano a seconda del tipo di carico di lavoro dell'applicazione.	Le prestazioni sono agli stessi livelli dei computer virtuali normali.
Gestione/configurazione	Gestita dalla console UDP, è in grado di avviare o arrestare il computer virtuale istantaneo su richiesta quando è necessario l'accesso da parte dell'utente.	Se aggiunta come attività a un piano, tutti i dati sottoposti a backup vengono convertiti automaticamente in un formato di computer virtuale. L'attività VSB viene applicata a tutti i nodi protetti con il piano.
Salvataggio dei dati e migrazione del computer virtuale nell'ambiente di produzione	Il disco virtuale del computer virtuale istantaneo fa riferimento a blocchi di dati nel punto di ripristino da cui è stato avviato il computer virtuale. Pertanto, quando il computer virtuale istantaneo accede ai blocchi di dati dal rispettivo disco virtuale, i dati vengono in realtà richiesti dal server RPS (questo processo è palese per l'utente). Il reindirizzamento I/O comporta un ulteriore calo delle prestazioni.	Il disco o i dischi virtuali del computer virtuale VSB contengono già la maggior parte dei dati recenti dal punto di ripristino corrispondente. Poiché il reindirizzamento I/O non si verifica (come per il computer virtuale istantaneo), le prestazioni del computer virtuale VSB sono analoghe a quelle dei computer virtuali normali in quanto non vi sono dipendenze dal server RPS o dal punto di ripristino (a dif-

	Se si prevede di utilizzare il computer virtuale istantaneo in produzione, si consiglia di renderlo persistente e di attivare il disco virtuale del computer virtuale con i dati effettivi. Per riattivare il computer virtuale istantaneo, copiare o replicare il computer virtuale. A seconda del tipo di hypervisor utilizzato nell'ambiente di produzione, per conservare i dati del computer virtuale istantaneo è possibile utilizzare la funzione VMware Storage vMotion o la replica/migrazione di archiviazione del computer virtuale Hyper-V per copiare il computer virtuale istantaneo nel punto in cui i dati diventano permanenti.	ferenza dello scenario del computer virtuale istantaneo).

Protezione utente

La presente sezione descrive i seguenti argomenti:

- Ruoli per i servizi Arcserve UDP
- Privilegi dell'utente per le funzioni di Arcserve UDP

Ruoli per i servizi Arcserve UDP

Nella tabella seguente sono descritti i ruoli per i servizi Arcserve UDP:

Servizio	Descrizione	Esecuzione su ruolo
Controllo del registro eventi di Arcserve	Fornisce il servizio di gestione delle licenze SDK per accettare le chiavi di licenza.	Console/Server RPS/Agente
Servizio di estensione di Windows Explorer dell'agente Arcserve UDP	Fornire il servizio di backend per la visualizzazione di UDP in Windows Explorer.	Server RPS/Agente
Servizio dell'agente Arcserve UDP	Fornisce l'interfaccia utente Web e il servizio Web per l'agente Arcserve UDP, compreso l'invio del processo di backup/ripristino.	Server RPS/Agente
Servizio dell'identità Arcserve UDP	Fornire il servizio di autenticazione e autorizzazione per la Console Arcserve Unified Data Protection.	Console
Servizio di condivisione della porta di gestione di Arcserve UDP	Fornire il servizio di condivisione della porta che consente la condivisione di una porta da parte della Console, dal gateway e dal server dell'identità.	Console
Servizio di gestione di Arcserve UDP	Fornisce il servizio Web per la Console di gestione centrale Arcserve Unified Data Protection.	Console
Servizio gateway di gestione remota di Arcserve	Offre la possibilità di gestire le richieste bidirezionali tra il gateway e la Console via Intranet o Internet.	Gateway
Servizio dell'archivio dati del server RPS di Arcserve UDP	Fornisce il servizio Web per la gestione dell'archivio dati UDP compresi la creazione, la modifica, l'eliminazione l'avvio e l'interruzione.	Server RPS
Servizio di condivisione della porta del server RPS di Arcserve UDP	Espone soltanto una porta per il server RPS per la gestione della comunicazione con l'interfaccia Web dell'agente, il servizio Web del server RPS e il processo di replica.	Server RPS
Servizio di aggiornamento di Arcserve UDP	Rileva l'aggiornamento di Arcserve UDP e lo scarica se disponibile.	Console/Server RPS/Agente

Privilegi dell'utente per le funzioni di Arcserve UDP

Nella tabella seguente vengono descritti i privilegi dell'utente per le funzioni di Arcserve UDP:

Funzioni	Utente	Privilegio	Commenti
Installazione	**Gruppo di amministratori locali**	**Gruppo di amministratori locali**	
Console e gateway	**Gruppo di amministratori locali**	**Gruppo di amministratori locali**	
Recovery Point Server	**Gruppo di amministratori locali**	**Gruppo di amministratori locali**	
Backup client Windows	**Gruppo di amministratori locali**	**Gruppo di amministratori locali** Criteri di sicurezza: • Funzionamento come componente del sistema operativo • Accesso locale • Accesso in qualità di servizio • Accesso in qualità di processo batch	**Molte operazioni correlate al backup, come la snapshot VSS, richiedono privilegi amministrativi.**
Condivisione di rete per l'archivio dati non di deduplicazione	Se l'UAC del server RPS è abilitato, l'account di dominio o l'amministratore integrato.		
Troncamento del registro SQL	Gruppo di amministratori locali	L'amministratore locale in possesso del ruolo di database predefinito SQL sysadmin o db_owner.	Ai fini del troncamento del registro sono necessari il database di backup delle query, il backlog e le query compattate (database compattato).
Troncamento del	Gruppo di amministratori	Gruppo di ammi-	È necessario

registro Exchange	di dominio	nistratori di dominio	disporre dell'accesso ai database di Exchange
Protezione di Active Directory	Gruppo di amministratori di dominio	Gruppo di amministratori di dominio	
Ripristino client Windows			
Condivisione di rete per l'archivio dati non di deduplicazione	Se l'UAC del server RPS è abilitato, l'account di dominio o l'amministratore integrato.		
SQL	Gruppo di amministratori locali	L'amministratore locale in possesso del ruolo di database predefinito SQL sysadmin o db_owner.	
Exchange	Gruppo di amministratori di dominio	Gruppo di amministratori di dominio	È necessario disporre dell'accesso ai database di Exchange
Active Directory	Gruppo di amministratori di dominio	Gruppo di amministratori di dominio	
Utilità Exchange Granular Restore	Ripristino sulla casella di posta: l'account utilizzato per il ripristino deve rappresentare i privilegi della casella di posta di destinazione. Per le altre opzioni di ripristino, l'account non necessita di requisiti speciali.	Ripristino sulla casella di posta: l'account utilizzato per il ripristino deve rappresentare i privilegi della casella di posta di destinazione. Per le altre opzioni di ripristino, l'account non richiede requisiti specifici.	
Backup senza agente basato su host			
Aggiunta del nodo del computer virtuale da vCenter/ESXi	• vCenter: amministratore integrato • ESXi: root		Per vCenter, se viene utilizzato un amministratore non integrato, fare riferimento a questo collegamento.
Aggiunta di un nodo di computer	Amministrazione di cluster o utenti	Amministrazione di cluster o utenti	

virtuale da Nutanix AHV			
Aggiunta del nodo del computer virtuale da Hyper-V	• Hyper-v standalone: amministratore locale integrato, amministratore di dominio integrato oppure account di dominio membro del gruppo degli amministratori locali. • Cluster Hyper-V: account di dominio integrato o account di dominio membro del gruppo degli amministratori locali.		Se si utilizza un altro account amministrativo, disabilitare l'accesso remoto UAC. Fare riferimento al collegamento.
Metodo di disattivazione della snapshot VMware nel piano	Amministratore locale integrato o amministratore di dominio integrato **Nota:** Le credenziali richieste vengono impostate dal nodo di aggiornamento		Se si utilizza un altro account amministrativo, disabilitare il controllo UAC. Fare riferimento al collegamento.
Ripristino a livello di database dell'applicazione per il computer virtuale Hyper-V/Nutanix	Amministratore locale integrato, amministratore di dominio integrato, oppure account di dominio membro del gruppo di amministratori locali **Note:** • Le credenziali richieste vengono impostate dal nodo di aggiornamento • Se il sistema operativo guest del computer virtuale è la versione client		Se si utilizza un altro account amministrativo, disabilitare l'accesso remoto UAC. Fare riferimento al collegamento.

	di Windows (ad esempio Windows 10), è necessario configurare manualmente il firewall per consentire la Strumentazione gestione Windows (WMI).		
PFC	• Computer virtuale VMware: l'amministratore locale integrato o l'amministratore di dominio integrato • Computer virtuale Hyper-V: amministratore locale integrato, amministratore di dominio integrato, oppure l'account di dominio membro del gruppo degli amministratori locali • Computer virtuale Nutanix: amministratore locale integrato, amministratore di dominio integrato oppure account di dominio membro del gruppo di amministratori locali **Note:** • Le credenziali richieste vengono impostate dal nodo di aggiornamento		Se si utilizza un account amministrativo: • Per i computer virtuali VMware, disabilitare il controllo UAC. Fare clic sul seguente collegamento. • Per i computer virtuali Hyper-V, disabilitare l'accesso remoto UAC. Fare clic sul seguente collegamento.

	• Per il computer virtuale Hyper-V/Nutanix, se il sistema operativo guest del computer virtuale è la versione client di Windows (ad esempio Windows 10), è necessario configurare manualmente il firewall per consentire la Strumentazione gestione Windows (WMI).		
Comando di pre-/post-esecuzione	• Computer virtuale VMware: l'amministratore locale integrato o l'amministratore di dominio integrato • Computer virtuale Hyper-V: amministratore locale integrato, amministratore di dominio integrato, oppure l'account di dominio membro del gruppo degli amministratori locali • Computer virtuale Nutanix: amministratore locale integrato, amministratore di dominio integrato oppure account di dominio membro del gruppo di amministratori locali		Per utilizzare le credenziali impostate dal nodo di aggiornamento e dalla scheda Avanzate di un piano, fare clic sul seguente collegamento.

	Note: • Le credenziali richieste qui vengono impostate dal nodo di aggiornamento e dalla scheda Avanzate di un piano. • Per il computer virtuale Hyper-V, se il sistema operativo guest del computer virtuale è la versione client di Windows (ad esempio Windows 10), è necessario configurare manualmente il firewall per consentire la Strumentazione gestione Windows (WMI). • Per il computer virtuale Hyper-V/Nutanix, se il sistema operativo guest del computer virtuale è la versione client di Windows (ad esempio Windows 10), configurare manualmente il firewall per consentire la Strumentazione gestione Windows (WMI).		
Troncamento del registro SQL	Uguale al comando di pre-/post script		Uguale al comando di pre/post script

Troncamento del registro Exchange	Uguale al comando di pre-/post script		Uguale al comando di pre/post script
Ripristino a livello di file nella posizione originale	Amministratore locale integrato, amministratore di dominio integrato, oppure account di dominio membro del gruppo di amministratori locali **Note:** • Le credenziali richieste vengono impostate dal nodo di aggiornamento • Per il computer virtuale Hyper-V/Nutanix, se il sistema operativo guest del computer virtuale è la versione client di Windows (ad esempio Windows 10), è necessario configurare manualmente il firewall per consentire la Strumentazione gestione Windows (WMI).		Se si utilizza un altro account amministrativo, disabilitare l'accesso remoto UAC come indicato nel seguente collegamento.
Virtual StandBy			
Per Hyper-V	• Amministratore locale integrato • Amministratore di dominio integrato • Account di dominio membro del gruppo degli amministratori locali • Account locale membro del gruppo degli amministratori locali	Gruppo di amministratori locali	Se si utilizza l'account amministratore locale, disabilitare l'accesso remoto UAC. Fare clic sul seguente collegamento.

Per Nutanix	Amministratore del cluster	Amministratore del cluster	
Per VMware	• vCenter: amministratore integrato • ESXi: root		Per vCenter, se viene utilizzato un amministratore non integrato, fare riferimento a questo collegamento.
Computer virtuale istantaneo/Assured Recovery			
Per Hyper-V	• Amministratore locale integrato • Amministratore di dominio integrato • Account di dominio membro del gruppo degli amministratori locali • Account locale membro del gruppo degli amministratori locali		Se si utilizza l'account amministratore locale, disabilitare l'accesso remoto UAC. Fare clic sul seguente collegamento.
Per VMware	• vCenter: amministratore integrato • ESXi: root	Gruppo di amministratori locali	Per vCenter, se viene utilizzato un amministratore non integrato, fare riferimento a questo collegamento.
Attività di copia e archivio file	**Gruppo di amministratori locali**	**Gruppo di amministratori locali**	
Copia del punto di ripristino su cloud	**Gruppo di amministratori locali**	**Gruppo di amministratori locali**	
Protezione in percorso UNC/NFS	**Qualsiasi utente può eseguire l'accesso ed essere rappresentato**	**Autorizzazione in lettura per il percorso UNC/NFS**	
Virtual StandBy su AWS EC2	**Utenti Amazon IAM che dispongono delle autorizzazioni necessarie per l'interazione con l'API AWS**		Per AWS EC2, consultare il seguente collegamento.
Virtual StandBy su Microsoft Azure	**Applicazione**	**Ruolo di collaboratore della sottoscrizione**	

		selezionata	
Linux			
Installa	root	Lettura, scrittura, esecuzione	
Registrazione console	Amministrazione console		
Backup basato sull'agente			
-Condivisione di rete	amministratore di archiviazione	Lettura, scrittura	
--Connessione nodi	root/non-root/sudo	Lettura, scrittura, esecuzione	
Ripristino a livello di file			
-Condivisione di rete	amministratore di archiviazione	Lettura, scrittura	
--Connessione nodi	root/non-root/sudo	Lettura, scrittura, esecuzione	L'utente principale può eseguire il ripristino in qualsiasi punto; gli altri utenti possono eseguire il ripristino solo nelle directory di loro appartenenza
Ripristino bare metal		Informazioni di accesso all'hardware	
Ripristino bare metal di migrazione			
Computer virtuale istantaneo per Hyper-V			
Computer virtuale istantaneo per VMware			
Computer virtuale istantaneo per Nutanix AHV	Amministratore del cluster	Amministratore del cluster	
Computer virtuale istantaneo su Amazon EC2	**Utente IAM**	**Accesso completo di EC2**	
Computer virtuale istantaneo su	**Applicazione**	**Ruolo di collaboratore della sot-**	

Microsoft Azure		toscrizione selezionata	
Protezione Exchange Online	Qualsiasi account Exchange Online	Privilegi di rappresentazione applicazione sugli account protetti	
Protezione di SharePoint Online	Amministratore raccolta siti SharePoint Online	Amministratore raccolta siti SharePoint Online	
OneDrive	Amministratori di Azure Active Directory	Amministratori di Azure Active Directory	

Chapter 3: Installazione di Arcserve UDP

La presente sezione descrive i seguenti argomenti:

Installazione di Arcserve UDP

Arcserve UDP - Completa: dopo l'installazione, è possibile accedere alla console Arcserve UDP (Console) ed eseguire le funzioni di gestione dati. La console consente di gestire e monitorare nodi, Recovery Point Server e attività di backup, ripristino e replica.

Arcserve UDP - Agente: esegue solo l'installazione dell'agente Arcserve UDP. Installare l'agente nei nodi che si desidera proteggere. Eseguire questa fase solamente se si desidera installare manualmente l'agente in un nodo. Generalmente, l'agente viene distribuito automaticamente nei nodi a partire dalla console durante la creazione di un piano.

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Definizione del tipo di installazione
3. Installazione di Arcserve Unified Data Protection mediante la procedura guidata di installazione
4. Installazione di Arcserve Unified Data Protection mediante la riga di comando
5. Installazione di Arcserve Unified Data Protection mediante il programma di installazione unificato
6. Verifica dell'installazione
7. (Facoltativo) Porte di comunicazione utilizzate
8. (Facoltativo) Impatto del processo di installazione sui sistemi operativi

Verifica delle considerazioni e dei prerequisiti

Verificare i prerequisiti e le considerazioni di installazione seguenti prima di installare Arcserve UDP:

Prerequisiti

- Leggere le Note di rilascio di Arcserve UDP 8.0. Le Note di rilascio contengono una descrizione dei requisiti di sistema, dei sistemi operativi supportati e un elenco di problemi noti riscontrati nella release presente.
- Verificare che i sistemi soddisfino i requisiti software e hardware necessari a installare i componenti di Arcserve Unified Data Protection.
- Verificare che l'account Windows disponga dei privilegi di amministratore o equivalenti per l'installazione del software sui sistemi in cui si desidera installare i componenti di Arcserve Unified Data Protection.
- Verificare di disporre dei nomi utente e delle password dei sistemi su cui si sta eseguendo l'installazione dei componenti di Arcserve Unified Data Protection.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Considerazioni

Prima dell'installazione, si consiglia di determinare la modalità di installazione di Arcserve Unified Data Protection:

- Il sistema in cui si desidera installare la console.
- I nodi da proteggere.
- Il numero di Recovery Point Server che fungeranno da destinazione di backup.
- Il numero di server di replica che replicheranno i Recovery Point Server.

Definizione del tipo di installazione

È possibile installare Arcserve UDP utilizzando uno dei metodi seguenti:

- **Installazione standard mediante la procedura guidata di installazione:**questo metodo consente di installare Arcserve Unified Data Protection utilizzando la procedura guidata di installazione. In questo metodo, in ogni fase viene richiesta la selezione delle opzioni desiderate.
- **Installazione invisibile all'utente mediante la riga di comando:** questo metodo consente di eseguire un'installazione automatica mediante la riga di comando di Windows.
- **Installazione mediante il programma di installazione unificato:** questo metodo consente di installare Arcserve UDP, Arcserve Backup e Arcserve RHA tramite un singolo programma di installazione. È possibile scegliere di installare tutti e tre i prodotti contemporaneamente, oppure installare ciascun prodotto separatamente. È possibile scaricare il programma di installazione dal sito Web di Arcserve.

Installazione di Arcserve Unified Data Protection mediante la procedura guidata di installazione

Arcserve Unified Data Protection consente di gestire e monitorare a livello centrale i nodi, i Recovery Point Server, i computer virtuali in server ESX, vCenter o Microsoft Hyper-V, i server di replica e i rapporti Arcserve Unified Data Protection.

Installare Arcserve Unified Data Protection su un server in cui è possibile gestire nodi protetti e altri componenti di Arcserve Unified Data Protection.

Effettuare le operazioni seguenti:

1. Accedere al pacchetto di installazione di Arcserve UDP dal sito Web di Arcserve o dal CD del prodotto.

   Nota: Nel caso in cui venga rilevato uno dei sistemi operativi supportati non in lingua inglese, sarà necessario selezionare la lingua di installazione del prodotto.

2. Fare doppio clic sul pacchetto di installazione.

   Viene visualizzata la finestra di dialogo **Contratto di licenza**.

3. Leggere e accettare i termini del contratto di licenza, quindi fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo **Tipo di installazione**.

4. Selezionare uno dei tipi di installazione.

   Installazione standard

   Consente di installare l'Agente o tutti i componenti di Arcserve Unified Data Protection.

   Arcserve Unified Data Protection - Agente

   Installa soltanto l'agente Arcserve UDP.

   Per ulteriori informazioni, consultare la sezione *Installazione dell'Agente Arcserve Unified Data Protection per Windows mediante l'installazione guidata* della *Guida per l'utente dell'Agente Arcserve UDP per Windows*.

   Arcserve Unified Data Protection- Completo

   Installa la Console, il Recovery Point Server e l'Agente Arcserve Unified Data Protection.

   Installazione avanzata

   Consente di installare uno o più tra i seguenti componenti di Arcserve Unified Data Protection:

- Agente Arcserve UDP
- Recovery Point Server di Arcserve UDP
- Console Arcserve UDP

5. Specificare se si desidera installare il driver di rilevamento modifiche dell'Agente Arcserve Unified Data Protection per Windows.

   Questa opzione è selezionata per impostazione predefinita.

   - Se il driver non è installato, l'Agente Arcserve Unified Data Protection per Windows esegue sempre un backup completo.
   - Con il driver installato sarà comunque necessario disporre di una licenza dell'Agente Arcserve Unified Data Protection per Windows valida per eseguire un backup locale.
   - Il driver non è richiesto se l'agente viene utilizzato come computer di monitoraggio di Virtual Standby oppure come server proxy di Host-Based VM Backup.

     Nota: Una volta completata l'installazione, sarà possibile installare il driver in qualsiasi momento mediante l'esecuzione dell'utilità InstallDriver.bat dal seguente percorso:

     <Arcserve UDP install folder>\Engine\BIN\DRIVER

6. Fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo **Cartella di destinazione**.

7. Specificare la cartella in cui si desidera installare Arcserve Unified Data Protection e fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo **Configurazione** .

8. Nella finestra di dialogo **Configurazione**, specificare le informazioni seguenti:

   a. Selezionare il protocollo.

      Nota: per una comunicazione protetta, selezionare il protocollo HTTPS.

   b. Immettere il numero di porta dell'agente, se applicabile. In genere, il numero della porta è 8014.

   c. Immettere il numero di porta della console, se applicabile. In genere, il numero della porta è 8015.

   d. Digitare il nome e la password dell'amministratore di Windows.

   e. Specificare se si desidera visualizzare il computer di monitoraggio dell'agente Arcserve UDP per tutti gli utenti o solamente per l'utente corrente.

9. Fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo **Impostazioni database**.

10. Nella finestra di dialogo **Impostazioni database**, fare clic sull'elenco a discesa **Database** per scegliere un tipo di database. È possibile specificare uno dei seguenti database:

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

      Importante! Quando si hanno più di 500 nodi da gestire dalla Console, assicurarsi di selezionare Microsoft SQLServer e non SQLExpress.

    Dopo aver selezionato un database, nella finestra di dialogo **Impostazioni database** vengono visualizzate le opzioni relative al database specificato. Fornire i dettagli relativi alle impostazioni del database per uno dei database selezionati.

    Microsoft SQL Server 2014 Express (incluso):

    Nella finestra di dialogo **Impostazioni database**, compilare i seguenti campi:

    a. Specificare la posizione in cui installare Microsoft SQL Server 2014 Express. È possibile accettare il percorso predefinito o specificare un percorso alternativo.

    b. Specificare la posizione in cui si desidera installare i file di dati per il database predefinito di Arcserve Unified Data Protection. È possibile accettare il percorso predefinito o specificare un percorso alternativo.

       Nota: Microsoft SQL Server 2014 Express non supporta le comunicazioni remote. Pertanto, è necessario installare il database predefinito e il file di dati sul computer in cui si sta installando l'applicazione.

    Database Microsoft SQL Server

    Nella finestra di dialogo **Impostazioni database**, compilare i seguenti campi:

    a. **Tipo di SQL server**: specificare il tipo di comunicazione che l'applicazione dovrà utilizzare per comunicare con il database di SQL Server.

       Locale: specificare Locale quando l'applicazione e SQL Server sono installati sullo stesso computer.

       Remoto: specificare Remoto quando l'applicazione e SQL Server sono installati su computer differenti.

    b. **Nome SQL Server**: se il tipo di SQL Server specificato è Remoto, specificare il nome dell'SQL Server remoto. Se l'SQL Server è Locale, selezionare il server dall'elenco a discesa.

c. **Protezione**: specificare il tipo di credenziali da utilizzare per l'autenticazione di SQL Server.

   Usa protezione Windows: esegue l'autenticazione mediante le credenziali Windows. È possibile accedere utilizzando le credenziali della console Arcserve UDP.

   Usa protezione SQL Server: esegue l'autenticazione mediante le credenziali SQL Server. Immettere l'ID di accesso e la password per l'account SQL Server.

11. Fare clic su **Avanti**. Viene visualizzata la finestra di dialogo **Eccezioni del firewall**.

    Nella finestra di dialogo **Eccezioni del firewall** sono elencati i servizi e i programmi da registrare come eccezioni nel firewall di Windows per Arcserve UDP.

    Nota: Le eccezioni del firewall sono obbligatorie per la configurazione e la gestione di Arcserve UDP da computer remoti.

12. Fare clic su **Avanti**. Viene visualizzata la finestra di dialogo **Messaggio**.

13. Fare clic su **Avanti**. Viene visualizzata la finestra di dialogo **Riepilogo**.

14. Fare clic su **Installa** per avviare la procedura di installazione.

    Viene visualizzata la finestra di dialogo **Avanzamento installazione** in cui è indicato lo stato dell'installazione. Quando l'installazione è completa, viene visualizzata la finestra di dialogo **Rapporto installazione**.

    (Facoltativo) Se si desidera selezionare uno degli ultimi aggiornamenti del prodotto, seguire i passaggi seguenti:

    a. Selezionare **Verifica aggiornamenti** e fare clic su **Fine**.

       Verrà visualizzata la finestra di dialogo **Verifica aggiornamenti**.

    b. Selezionare il server in cui si desidera scaricare gli aggiornamenti e fare clic su **Scarica e installa aggiornamenti**.

       Viene visualizzata la finestra di dialogo **Processo di aggiornamento** che indica lo stato del download.

       Al completamento dell'aggiornamento viene visualizzato un messaggio di avviso.

    (Facoltativo) Per installare l'agente di Arcserve UDP per Linux, seguire le istruzioni contenute nella sezione **Installazione dell'agente Arcserve Unified Data Protection per Linux**.

15. Fare clic su **Fine**.

    Arcserve UDP è installato sul computer.

Installazione di Arcserve Unified Data Protection mediante la riga di comando

È possibile installare Arcserve Unified Data Protection in modalità invisibile all'utente. Se si utilizza l'installazione invisibile all'utente, non sarà necessaria alcuna operazione da parte dell'utente. Di seguito è descritta la procedura per l'installazione dell'applicazione in modalità invisibile all'utente mediante la riga di comando di Windows:

Effettuare le operazioni seguenti:

1. Aprire la riga di comando di Windows nel computer in cui si desidera iniziare il processo di installazione invisibile all'utente.
2. Scaricare il pacchetto di installazione autoestraente sul computer.

   Avviare il processo di installazione invisibile all'utente utilizzando la seguente sintassi della riga di comando:

   Arcserve_Unified_Data_Protection.exe -s -a -q -Products:<ProductList> -Path:<INSTALLDIR> -User:<UserName> -Password:<Password> -Https:<HTTPS> -ConsolePort:<Port Number> -AgentPort:<Port Number> -Driver:<DRIVER> -MonitorFlag:<MONITORFLAG> -StopUA:<STOPUA> -SummaryPath:<SUMMARYPATH> -AutoReboot:<AUTOREBOOT>

   Esempio:

   Arcserve_Unified_Data_Protection.exe -s -a -q -Products:Agent -User:administrator -Password:test
3. Configurare l'installazione invisibile all'utente mediante la sintassi seguente e i seguenti argomenti:

   Importante. Se i parametri includono i seguenti caratteri speciali, racchiudere i parametri tra virgolette:

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

   Esempio: Se la password è abc^*123, l'input corrisponderà a Password:"abc^*123".

   -s

   Esegue il pacchetto di file eseguibile in modalità invisibile all'utente.

   -a

   Specifica le opzioni supplementari della riga di comando.

   -q

   Installa l'applicazione in modalità invisibile all'utente.

-Products:<Elenco prodotti>

(Facoltativo) Specifica i componenti da installare in modalità invisibile all'utente. Se non si specifica alcun valore per questo argomento, durante la procedura di installazione invisibile all'utente vengono installati tutti i componenti. È possibile specificare i seguenti componenti:

Agente: installa il componente Agente di protezione dei dati.

RPS: installa il componente Recovery Point Server.

Console: installa il componente della console.

Tutto: installa tutti i componenti di Arcserve Unified Data Protection.

Esempio:

Per installare l'agente di protezione dati:

-Products:Agent

Per installare il Recovery Point Server:

-Products:Agent,RPS

Per installare l'agente di protezione dati, il Recovery Point Server e la console di protezione dati:

-Products:Agent,RPS,Console

Per installare tutti i componenti nel build:

-Products:All

-User:<UserName>

Specifica il nome utente che si desidera utilizzare per installare ed eseguire l'applicazione.

Nota: Il nome utente è l'amministratore o un account con privilegi amministrativi.

-Password:<Password>

Specifica la password per il nome utente.

-Https:<HTTPS>

(Facoltativo) Specifica il protocollo di comunicazione. Le opzioni sono 0 e 1. Utilizzare 0 per HTTP e 1 per HTTPS.
Impostazione predefinita: 0
Esempio:

-https:1

-Percorso:<INSTALLDIR>

(Facoltativo) Specifica il percorso di installazione di destinazione dell'agente di protezione dei dati.

Esempio:

-Path:C:\Programmi\Arcserve\Unified Data Protection

Nota: Se il valore di INSTALLDIR contiene uno spazio, racchiudere il percorso tra virgolette. Inoltre, il percorso non può terminare con una barra rovesciata.

-ConsolePort:<Port Number>

(Facoltativo) Specifica il numero di porta di comunicazione per la Console.

Impostazione predefinita: 8015

Esempio:

-ConsolePort:8015

Nota: Utilizzare questa opzione per installare la console.

-AgentPort:<Port Number>

(Facoltativo) Specifica il numero di porta di comunicazione per accedere all'agente Arcserve Unified Data Protection.

Impostazione predefinita: 8014

Esempio:

-AgentPort:8014

Nota: Utilizzare questa opzione per installare l'agente Arcserve Unified Data Protection.

-Driver:<DRIVER>

(Facoltativo) Specifica se installare il driver di rilevamento modifiche dell'agente Arcserve Unified Data Protection. Le opzioni sono 0 e 1.

0: non installa il driver
1: installa il driver

Valore predefinito: 1

Esempio:

-driver:1

-MonitorFlag:<MONITORFLAG>

(Facoltativo) Specifica la visualizzazione del computer di monitoraggio dell'agente Arcserve Unified Data Protection da parte degli utenti. Le opzioni sono 0 e 1.

0: mostra il computer di monitoraggio dell'agente a tutti gli utenti.
1: mostra il computer di monitoraggio dell'agente solo all'utente corrente.

Impostazione predefinita: 0.

Esempio:

-MonitorFlag:0

-StopUA:< STOPUA >

(Facoltativo) Specifica l'interruzione del servizio dell'agente universale Arcserve.

0: non interrompe il servizio dell'agente universale Arcserve se è in esecuzione durante il processo di installazione.
1: interrompe il servizio dell'agente universale Arcserve se è in esecuzione durante il processo di installazione.
Impostazione predefinita: 0

Esempio:

-StopUA:1

Nota: Utilizzare questa opzione durante l'esecuzione dell'aggiornamento a una nuova versione. Accertarsi di impostare il valore su 1 o di interrompere il servizio prima di avviare il processo di aggiornamento. Quest'operazione garantisce un corretto processo di installazione.

-SummaryPath:<SUMMARYPATH>

(Facoltativo) Specifica il percorso di destinazione per la generazione del file di riepilogo dell'installazione.

Esempio:

-SummaryPath:C:\Result

Nota: Se il valore di SUMMARYPATH contiene uno spazio, racchiudere il percorso tra virgolette. Inoltre, il percorso non può terminare con una barra rovesciata.

-AutoReboot:<AUTOREBOOT>

(Facoltativo) Consente al programma di installazione di riavviare il computer dopo l'installazione se necessario per l'installazione. Le opzioni sono 0 e 1.

0: il computer non viene riavviato.

1: il computer viene riavviato se richiesto dall'installazione.

Impostazione predefinita: 0

Esempio:

-AutoReboot:1

Nota: Se l'installazione non richiede un riavvio, il programma di installazione non riavvierà il computer anche se questo parametro è impostato su 1.

L'installazione invisibile all'utente è stata completata correttamente.

Installazione di Arcserve UDP mediante il programma di installazione unificato

Arcserve UDP consente di installare tutti i relativi componenti mediante un unico programma di installazione unificato. In base alle proprie esigenze, il programma di installazione suggerisce la licenza migliore per soddisfare le esigenze, quindi scarica e installa i componenti.

Effettuare le operazioni seguenti:

1. Scaricare il file ASDownloader dal sito Web di Arcserve.

   Nota: Nel caso in cui venga rilevato uno dei sistemi operativi supportati non in lingua inglese, sarà necessario selezionare la lingua di installazione del prodotto.

2. Fare doppio clic sul pacchetto di installazione.

   Viene visualizzata la finestra di dialogo **Contratto di licenza**.

3. Leggere e accettare i termini del contratto di licenza, quindi fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo **introduzione**.

4. Fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo **Choose Components to Download (Seleziona componenti da scaricare)**.

5. Selezionare una o più opzioni seguenti in base ai propri requisiti e fare clic su **Avanti**.

   Arcserve Unified Data Protection

   Esegue l'installazione di Arcserve UDP. Arcserve UDP consente di proteggere i computer virtuali e fisici Linux e Windows. È possibile gestire tutte le esigenze di protezione dei dati da un'unica console. Per gestire i dati, è possibile utilizzare la deduplicazione globale all'origine, la replica, la replica remota e altre funzioni.

   Arcserve Backup

   Esegue l'installazione di Arcserve Backup. Quando utilizzato insieme ad Arcserve, consente di gestire il backup su nastro dalla console di Arcserve UDP e sfruttare tutte le funzionalità di Arcserve UDP.

   Viene visualizzata la finestra di dialogo **Download prodotti**.

6. Fare clic su **Scarica**.

   Il prodotto inizia il download in un formato zip. È possibile verificare lo stato del download sulla barra di avanzamento. È anche possibile sospendere e riprendere il

download. La durata dell'operazione può richiedere alcuni minuti a seconda della larghezza di banda e del numero di componenti da scaricare.

Il pulsante Avanti rimane inattivo fino al completamento del download.

7. Una volta completato il download, fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo relativa al **metodo di installazione**.

8. Selezionare uno dei tipi di installazione.

   Installazione rapida

   Esegue l'installazione dei componenti utilizzando la configurazione predefinita. Fare clic su **Visualizza componenti e configurazione predefinita** per visualizzare i componenti installati.

   Installazione avanzata

   Consente di installare ciascun componente separatamente.

9. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Configurazione account**.

10. Specificare il nome utente e la password, quindi fare clic su **Installa**.

    Viene avviata la procedura di installazione. È possibile vedere l'avanzamento nella finestra di dialogo. Al completamento dell'installazione, chiudere la procedura guidata.

    Arcserve UDP è installato sul computer.

Verifica dell'installazione

Effettuare le operazioni seguenti:

1. Verificare che l'icona Arcserve UDP venga visualizzata nella barra delle applicazioni.
2. Verificare che i servizi dell'agente e del server siano attivi e in esecuzione dalla gestione dei servizi Windows.

   Arcserve Unified Data Protection è stato installato correttamente ed è possibile eseguire il backup del computer Windows.

Porte di comunicazione utilizzate da Arcserve UDP

Le informazioni fornite in questa sezione riguardano le porte utilizzate per i seguenti componenti:

- Componenti installati su Microsoft Windows
- Componenti installati su Linux
- Componenti installati sull'hypervisor

Le porte elencate sono richieste per il backup e per altri processi se si dispone di un ambiente LAN.

*La condivisione delle porte è supportata per i processi di replica. È possibile inviare alla porta 8014 (porta predefinita per il server UDP) tutti i dati relativi alle diverse porte. Le impostazioni possono essere modificate durante l'installazione. Quando un processo di replica viene eseguito tra due Recovery Point Server in WAN, è necessario aprire soltanto la porta 8014.

Allo stesso modo, per le repliche remote, l'amministratore remoto deve aprire o inviare soltanto la porta 8014 (per la replica dei dati) e la porta 8015 (porta predefinita della console UDP, che è possibile modificare durante l'installazione) per i Recovery Point Server locali al fine di ottenere l'assegnazione di un piano di replica.

Componenti installati su Microsoft Windows

Questa sezione contiene informazioni sulle porte utilizzate nella Console UDP e nel Recovery Point Server UDP (RPS):

- Console UDP
- Recovery Point Server (RPS) UDP
- Agente Windows UDP

Console UDP

Nella tabella seguente sono elencate le porte utilizzate dalla Console Arcserve UDP:

Numero porta	Tipo di porta	Avviato da	Processo in ascolto	Porta interna/esterna	Descrizione
1433	TCP	Java remoto	sqlsvr.exe	Esterna	Porta di comunicazione predefinita tra la console UDP e i database Microsoft SQL Server se risiedono su computer differenti. **Nota:** è possibile modificare la porta di comunicazione predefinita mediante l'installazione di SQL Server.
6052	TCP	Arcserve Backup Global Dashboard	Arcserve.CommunicationFoundation.WindowsService.exe	Esterna	Servizio di comunicazione che consente alla console Arcserve UDP e al server primario Arcserve Backup Glo-

					bal Dashboard di sincronizzare i dati. **Nota:** Questa porta è necessaria solo se si desidera sincronizzare i dati di Arcserve Backup Global Dashboard con la console UDP.
6054	TCP	Server primario Arcserve Backup	Arcserve.CommunicationFoundation.WindowsService.exe	Esterna	Servizio di comunicazione che consente alla console e al server primario Arcserve Backup di sincronizzare i dati. **Nota:** Questa porta è necessaria solo se si desidera sincronizzare i dati di Arcserve Backup Global Dashboard con la console UDP.

8012	TCP	Console UDP	java.exe	Interna	Porta predefinita utilizzata internamente dal servizio di identità della console UDP. **Nota:** la porta può non essere personalizzata e può essere ignorata per l'impostazione del firewall. Se la porta 8012 è occupata da altri programmi, il programma di installazione UDP assegnerà in modo dinamico un'altra porta disponibile.
8015	TCP	Console UDP Gateway UDP	httpd.exe	Esterna	Porta di comunicazione HTTP/HTTPS predefinita per accedere alla

					console e al gateway UDP. **Nota:** è possibile modificare la porta di comunicazione predefinita con l'installazione dei componenti UDP.
8029	TCP	Console UDP	tomcat9.exe	Interna	Porta predefinita utilizzata internamente dal servizio di gestione della console UDP. **Nota:** la porta può non essere personalizzata e può essere ignorata per l'impostazione del firewall. Se la porta 8029 è occupata da altri programmi, il programma di installazione UDP asse-

					gnerà in modo dinamico un'altra porta disponibile.
8030	TCP	Console UDP	tomcat9.exe	Interna	Porta predefinita utilizzata internamente dal servizio di gestione della console UDP. **Nota:** la porta può non essere personalizzata e può essere ignorata per l'impostazione del firewall. Se la porta 8030 è occupata da altri programmi, il programma di installazione UDP assegnerà in modo dinamico un'altra porta disponibile.
18007	TCP	TOMCA-	tomcat9.exe	Interna	Utilizzata

		T			internamente dal servizio di gestione Tomcat. **Nota:** è possibile modificare questa porta solo modificando i file di configurazione TOMCAT. È possibile ignorare la porta per l'impostazione del firewall.

Recovery Point Server (RPS) UDP

Nella tabella seguente sono elencate le porte utilizzate dal Recovery Point Server (RPS) Arcserve UDP:

Numero porta	Tipo di porta	Avviato da	Processo in ascolto	Porta interna/esterna	Descrizione
8014	TCP	UDP	httpd.exe	Esterna	Porta di comunicazione HTTP/HTTPS predefinita per accedere all'agente e al server RPS UDP **Note:** ▪ Questa è la porta condivisa predefinita ed è l'unica porta da aprire quando si utilizza il server RPS UDP come destinazione di replica. Non aprire la porta 5000-5060 utilizzata dagli archivi dati se è abilitata la deduplicazione globale. ▪ È possibile modificare la porta di comunicazione predefinita al momento dell'installazione dei componenti UDP.
8016	TCP	UDP	tomcat9.exe	Interna	Utilizzata internamente dai servizi Web RPS UDP per la comunicazione con il servizio di condivisione porta RPS UDP sullo stesso server. **Nota:** la porta può non essere personalizzata e può essere ignorata per l'impostazione del firewall.
5000-5060	TCP	UDP	GDDServer.exe	Interna	Questo intervallo di porte è riservato al servizio dell'archivio dati di deduplicazione RPS UDP. Un archivio dati di deduplicazione UDP RPS utilizzerà 4 porte libere e un archivio dati non di deduplicazione utilizzerà una porta libera. Entrambi inizieranno da 5000. Si tratta di un'operazione necessaria se l'archivio dati è abilitato per il backup o il ripristino. Se si utilizza il server RPS solo come destinazione di replica, non è necessario aprire le porte nella con-

					figurazione del firewall. **Nota:** modificare quanto segue per personalizzare l'intervallo di porte nel Registro di sistema: ■ HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore ▪ Nome chiave: PortRangeForGDD ▪ Tipo: Reg_SZ ▪ Valore predefinito: 5000-5060 Solo l'archivio dati creato inseguito alla modifica del Registro di sistema utilizzerà l'intervallo di porte appena modificato.
18005	TCP	TOMCAT	tomcat9.exe	Interna	Utilizzata per l'arresto di Tomcat dal server RPS o dall'agente UDP. **Nota:** È possibile modificare questa porta solo modificando i file di configurazione TOMCAT. È possibile ignorare la porta per l'impostazione del firewall.
7788	TCP	UDP	Sync_util_d.exe	Interna	Porta di comunicazione HTTP/HTTPS predefinita per accettare la replica nelle richieste.
445	TCP			Esterna	Utilizzata dal servizio SMB del sistema operativo Windows. La porta viene utilizzata quando il server RPS ospita l'archivio dati su un disco locale. L'archivio dati espone la cartella condivisa come destinazione di backup affinché l'agente UDP esegua il backup dei dati.

Agente Windows UDP

Nella tabella seguente sono elencate le porte utilizzate dall'agente Arcserve UDP per Windows:

Numero porta	Tipo di porta	Avviato da	Processo in ascolto	Porta interna/esterna	Descrizione
8014	TCP	Agente Windows UDP	tomcat9.exe	Esterna	Porta di comunicazione HTTP/HTTPS predefinita per accedere all'agente e al server RPS UDP. **Nota:** è possibile modificare la porta di comunicazione predefinita con l'installazione dei componenti UDP.
18005	TCP	TOMCAT	tomcat9.exe	Interna	Utilizzata per l'arresto di Tomcat dal server RPS o dall'agente UDP. **Nota:** È possibile modificare questa porta solo modificando i file di configurazione TOMCAT. È possibile ignorare la porta per l'impostazione del firewall.
4090	TCP	Agente Windows UDP	HATransServer.exe	Esterna	Utilizzata per trasferire dati per l'attività Virtual Standby in modalità proxy. **Nota:** questa porta è necessaria solo se si specifica l'agente UDP per Windows come monitoraggio di Virtual Standby.
135	TCP			Esterna	Porta di comunicazione per il servizio RPC sul sistema operativo Windows. **Nota:** questa porta è

					necessaria ogni volta che la console UDP esegue la distribuzione in remoto dell'agente Windows UDP sul computer dell'agente. Se l'agente Windows UDP viene installato tramite l'esecuzione del programma di installazione locale, questa porta non è necessaria.
445	TCP			Esterna	Porta di comunicazione per il servizio SMB per l'attivazione della cartella condivisa sul sistema operativo Windows. **Nota:** questa porta è necessaria ogni volta che la console UDP esegue la distribuzione in remoto dell'agente Windows UDP sul computer dell'agente. Se l'agente Windows UDP viene installato tramite l'esecuzione del programma di installazione locale, questa porta non è necessaria.

Componenti installati su Linux

Questa sezione fornisce informazioni sulle porte utilizzate nel Server di backup Linux e nei Nodi Linux protetti dal server di backup Linux in remoto.

Server di backup di Linux

Nella tabella seguente sono elencate le porte utilizzate dal server di backup Linux:

Numero porta	Tipo di porta	Avviato da	Processo in ascolto	Porta interna/esterna	Descrizione
67	UDP	UDP Linux	bootpd	Esterna	In entrata, utilizzata per il server di avvio PXE. Richiesta soltanto se l'utente desidera utilizzare la funzionalità di avvio PXE. **Nota:** il numero di porta non può essere personalizzato.
69	UDP	UDP Linux	tftpd	Esterna	In entrata, utilizzata per il server di avvio PXE. Richiesta soltanto se l'utente desidera utilizzare la funzionalità di avvio PXE. **Nota:** il numero di porta non può essere personalizzato.
8014	TCP	UDP Linux	java	Esterna	In entrata e in uscita. Porta di comunicazione HTTP/HTTPS predefinita per accedere all'agente UDP per Linux. **Nota:** è possibile modificare la porta di comunicazione predefinita con l'installazione dei componenti UDP.
8021	TCP	UDP Linux	cresvc	Esterna	In entrata, utilizzata per il servizio di backup.
18005	TCP	UDP Linux	java	Interna	Utilizzata da Tomcat. Ignorare questa porta per le impostazioni di firewall. **Nota:** È possibile modificare questa porta solo modificando i file di configurazione TOMCAT.

50000 o 50000+	TCP	UDP Linux	ssh	Esterna	Dipendenza di terze parti UDP Linux. Richiesta soltanto durante il ripristino bare metal di migrazione Linux dal cloud in locale. Viene selezionata e utilizzata una porta disponibile dalla porta 50000. Per impostazione predefinita, viene aperta la porta selezionata nel sistema Linux UDP.
22	TCP	Servizio SSH	sshd	Esterna	Dipendenza di terze parti UDP Linux. Valore predefinito per il servizio SSH. È comunque possibile modificare la porta. Si tratta della porta richiesta per le comunicazioni in entrata e in uscita.
8016	TCP	UDP Linux	d2ddss	Esterna	In entrata, utilizzata per il servizio dati del computer virtuale istantaneo o del ripristino bare metal istantaneo. Richiesta soltanto se l'utente desidera utilizzare la funzionalità del computer virtuale istantaneo o del ripristino bare metal immediato.
111	TCP	Portmapper	rpcbind	Esterna	Dipendenza di terze parti UDP Linux. Predefinita per il portmapper. Richiesta soltanto quando si esegue un computer virtuale istantaneo di Linux da un punto di ripristino di backup senza agente per il server ESX vSphere.
2049	TCP	Server NFS	nfsd	Esterna	Dipendenza di terze parti UDP Linux. Predefinita per il server NFS. Richiesta soltanto quando si esegue un computer virtuale istantaneo di Linux da un punto

					di ripristino di backup senza agente per il server ESX vSphere.
Porta dinamica	TCP	Servizio di montaggio NFS	rpc.mountd	Esterna	Dipendenza di terze parti UDP Linux. Consultare la pagina principale relativa a rpc.mountd per informazioni su come aggiungerla come porta fissa. Richiesta soltanto quando si esegue un computer virtuale istantaneo di Linux da un punto di ripristino di backup senza agente per il server ESX vSphere.

Nodi di Linux protetti dal server di backup di Linux in remoto

La tabella seguente elenca le porte utilizzate dai nodi Linux protetti dal server di backup Linux in remoto:

Numero porta	Tipo di porta	Avviato da	Processo in ascolto	Porta interna/esterna	Descrizione
22	TCP	Servizio SSH		Esterna	Dipendenza di terze parti UDP Linux. Valore predefinito per il servizio SSH. È comunque possibile modificare la porta. Si tratta della porta richiesta per le comunicazioni in entrata e in uscita.

Componenti installati sull'hypervisor

La presente sezione fornisce informazioni sulle porte utilizzate per l'host Hyper-V.

Host Hyper-V

Nella tabella seguente sono elencate le porte utilizzate dall'host Hyper-V:

Numero porta	Tipo di porta	Avviato da	Processo in ascolto	Interna/esterna	Descrizione
135	TCP			Esterna	Utilizzata dal servizio WMI del sistema operativo Windows. UDP utilizza WMI per interagire con l'host Hyper-V in alcuni casi.
445	TCP			Esterna	Utilizzata dal servizio SMB del sistema operativo Windows. UDP utilizza SMB per interagire con l'host Hyper-V in alcuni casi.
27000	TCP	Servizio UDP CBT	cbt_ rep.exe	Esterna	Utilizzata dal servizio CBT di backup basato su host UDP. Non è necessario registrare questa porta nell'eccezione del firewall perché UDP registra automaticamente la porta durante il backup. È necessario verificare che nessun'altra applicazione sia configurata con la stessa porta.
5895 o 5986	TCP	Servizio WinRM		Esterna	5895 per WinRM nel protocollo HTTP, 5896 per WinRM nel protocollo HTTPS È necessaria solo una delle due. Richiesta soltanto durante l'esecuzione del computer virtuale istantaneo Linux in Hyper-V.
1024 ~ 65535	TCP			Esterna	▪ Utilizzato durante l'importazione di computer virtuali dall'host Hyper-V e/o dal cluster per il piano di backup. ▪ Per impostazione predefinita, il processo di ripristino del computer virtuale sceglie casualmente una porta dispo-

					nibile nell'intervallo compreso tra 1024 e 65535. È possibile specificare manualmente l'intervallo in base ai valori del registro di sistema impostati nell'host Hyper-V. Per ulteriori informazioni, fare clic sul seguente collegamento.

Impatto del processo di installazione sui sistemi operativi

I processi di installazione seguenti aggiornano diversi sistemi operativi di Windows:

- Installazione di file binari non firmati
- Installazione di file binari con informazioni non corrette sulla versione dei file
- Installazione di file binari senza il sistema operativo nel Manifesto

Installazione di file binari non firmati

Nome file binario	Origine	Nome file binario	Origine
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-turbo.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

Installazione di file binari con informazioni non corrette sulla versione dei file

Nome file binario	Origine	Nome file binario	Origine
AxShockwaveFlashObjects.dll	Adobe	libisccfg.dll	bind
ShockwaveFlashObjects.dll	Adobe	liblwres.dll	bind
openssl.exe	Apache	libxml2.dll	bind
UpdateData.exe	Gestione licenze 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		

Installazione di file binari senza il sistema operativo nel Manifesto

Nome file binario	Origine
openssl.exe	Apache
win_nsupdate.exe	bind
plink.exe	putty
sqlite3.exe	sqlite
vddkReporter.exe	VMware

Configurazione Antivirus

Il software antivirus può interferire con la corretta esecuzione dell'agente Arcserve UDP (Windows) bloccando temporaneamente l'accesso ai file o mettendo in quarantena o eliminando i file classificati erroneamente come sospetti o pericolosi. È possibile configurare il software antivirus in modo da escludere determinati file o cartelle, per evitare di perdere tempo analizzando dati che non richiedono protezione.

È necessario configurare correttamente il software antivirus per escludere la destinazione di backup. La configurazione corretta consente di evitare interferenze con le operazioni di backup e ripristino, o con qualsiasi altro processo, come la generazione e l'unione del catalogo.

Percorsi da escludere durante l'analisi antivirus:

Analisi antivirus per	Percorsi da escludere
Server RPS	Cartella archivio dati Percorso di destinazione dei dati Percorso di destinazione dell'indice Percorso di destinazione hash
Agente di Windows non dalla console	Destinazione di backup

Installazione degli aggiornamenti di Arcserve UDP

Il processo di acquisizione e installazione degli aggiornamenti di Arcserve UDP è composto da due fasi: selezione e download dell'aggiornamento e installazione dell'aggiornamento.

Nota: Tutti gli aggiornamenti rilasciati per Arcserve UDP sono cumulativi. Come risultato, ogni aggiornamento conterrà tutti gli aggiornamenti delle versioni precedenti. In tal modo, il computer sarà sempre completamente aggiornato. La finestra di dialogo **Informazioni** mostra il livello di aggiornamento installato su un computer. Se lo si desidera, è possibile utilizzare queste informazioni per generare un altro server con lo stesso livello di configurazione/patch.

Per installare gli aggiornamenti di Arcserve UDP, procedere come segue:

1. Revisione delle considerazioni per l'installazione degli aggiornamenti
2. Impostazione delle preferenze di aggiornamento
3. Verifica e installazione degli aggiornamenti
4. (Facoltativo) Installazione degli aggiornamenti di Arcserve UDP in modalità invisibile all'utente
5. Verifica dell'installazione degli aggiornamenti

Revisione delle considerazioni per l'installazione degli aggiornamenti

Prima di installare gli aggiornamenti di Arcserve UDP, tenere presenti le seguenti considerazioni:

- Durante l'installazione di un aggiornamento di Arcserve UDP o dell'Agente Arcserve Unified Data Protection per Windows, è importante mantenere le prestazioni ottimali tra la console, il Recovery Point Server (RPS) e gli agenti. Di conseguenza, se l'installazione dell'aggiornamento viene eseguita in un ambiente che include sia una Console che un agente, sarà necessario installare l'aggiornamento sulla Console, quindi sul server RPS e infine sull'agente. (Per l'agente installato sulla Console o sul server RPS, l'aggiornamento verrà installato in modo automatico e simultaneo sull'agente).
- Se necessario, scaricare gli aggiornamenti disponibili da Arcserve direttamente su un computer client oppure prima su un server di gestione temporanea, quindi su un computer client.
- Se necessario, utilizzare il nodo workstation come server di gestione temporanea per scaricare gli aggiornamenti di Arcserve UDP.
- Verificare che le impostazioni relative alle preferenze degli aggiornamenti siano configurate correttamente.
  - È possibile installare gli aggiornamenti attraverso l'interfaccia utente oppure in modalità invisibile all'utente tramite la riga di comando.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

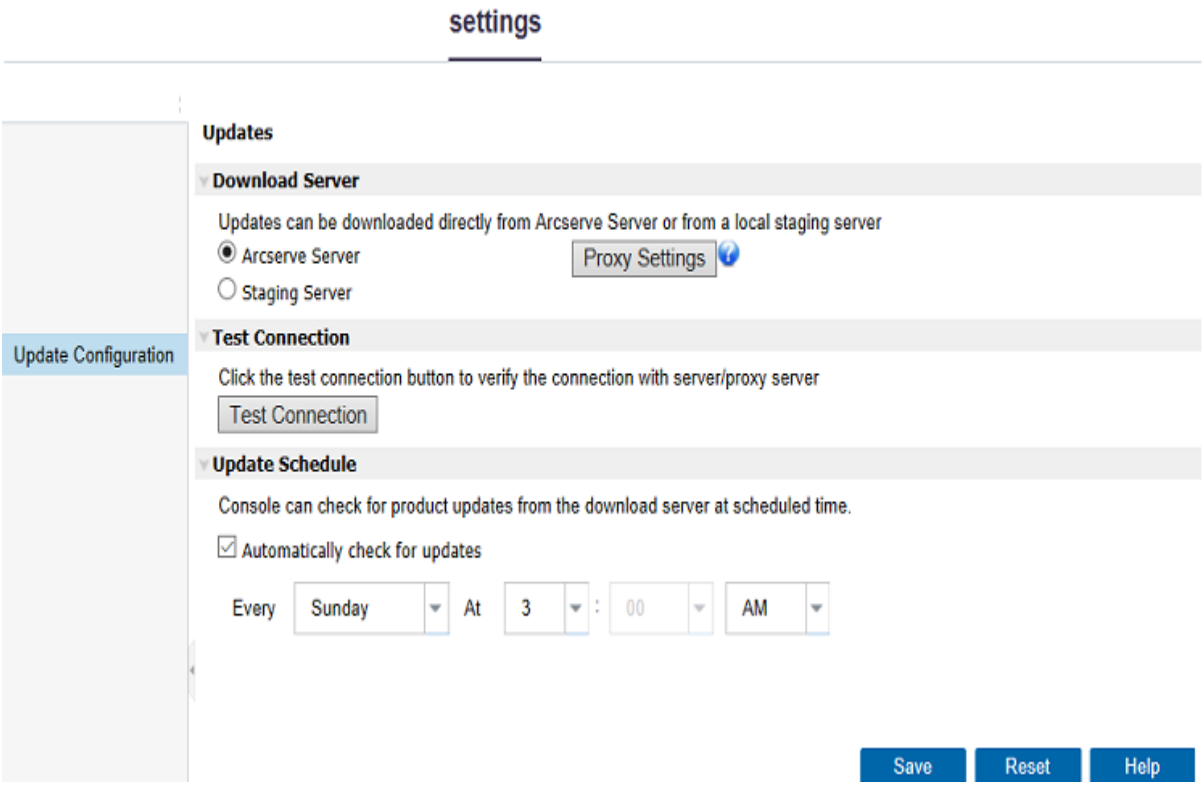
Indicazione delle preferenze di aggiornamento

Con Arcserve UDP è possibile specificare le preferenze di aggiornamento.

Effettuare le operazioni seguenti:

1. Dalla console Arcserve UDP, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Configurazione aggiornamento**.

   Nel riquadro destro viene visualizzata la pagina **Aggiornamenti**.



3. Specificare le impostazioni delle preferenze di **aggiornamento** desiderate.

   Server di download

   Indica il server di origine a cui il server Arcserve UDP si connette e dal quale scarica gli aggiornamenti disponibili.

   - **Server Arcserve**

     Specifica che gli aggiornamenti vengono scaricati dal server Arcserve direttamente sul server locale dell'utente.

     Si tratta dell'impostazione predefinita.

   - **Server di gestione temporanea**

Specifica che gli aggiornamenti vengono scaricati dal server di gestione temporanea.

Nota: Se necessario, è possibile creare un server di gestione temporanea. Per ulteriori informazioni, consultare la sezione Creazione di un server di gestione temporanea.

Specificando più server di gestione temporanea, il primo server elencato verrà designato come server di gestione temporanea primario. Arcserve UDP cercherà inizialmente di connettersi al server di gestione temporanea primario. Se il primo server elencato non è disponibile, il server successivo in elenco diventa il server di gestione temporanea primario. La stessa sequenza verrà mantenuta fino a quando l'ultimo server elencato diventerà il server di gestione temporanea primario. L'elenco dei server di gestione temporanea è limitato a un massimo di 5 server.

- Utilizzare i pulsanti **Sposta su** e **Sposta giù** per modificare la sequenza dei server di gestione temporanea.
- Utilizzare il pulsante **Elimina** per rimuovere un server dall'elenco.
- Utilizzare il pulsante **Aggiungi server** per aggiungere un nuovo server all'elenco. Facendo clic sul pulsante **Aggiungi server**, verrà visualizzata la finestra di dialogo **Server di gestione temporanea**, da cui sarà possibile specificare il nome del server di gestione temporanea aggiunto.

Quando si seleziona il server di gestione temporanea come server di download:

- Se sono presenti aggiornamenti per il server di gestione temporanea specificato, la Console Arcserve UDP può scaricare l'aggiornamento da questo server di gestione temporanea.
- Se non sono presenti aggiornamenti per il server di gestione temporanea specificato, la Console Arcserve UDP non sarà in grado di scaricare tali aggiornamenti dal server di gestione temporanea. Il registro visualizza il seguente messaggio:

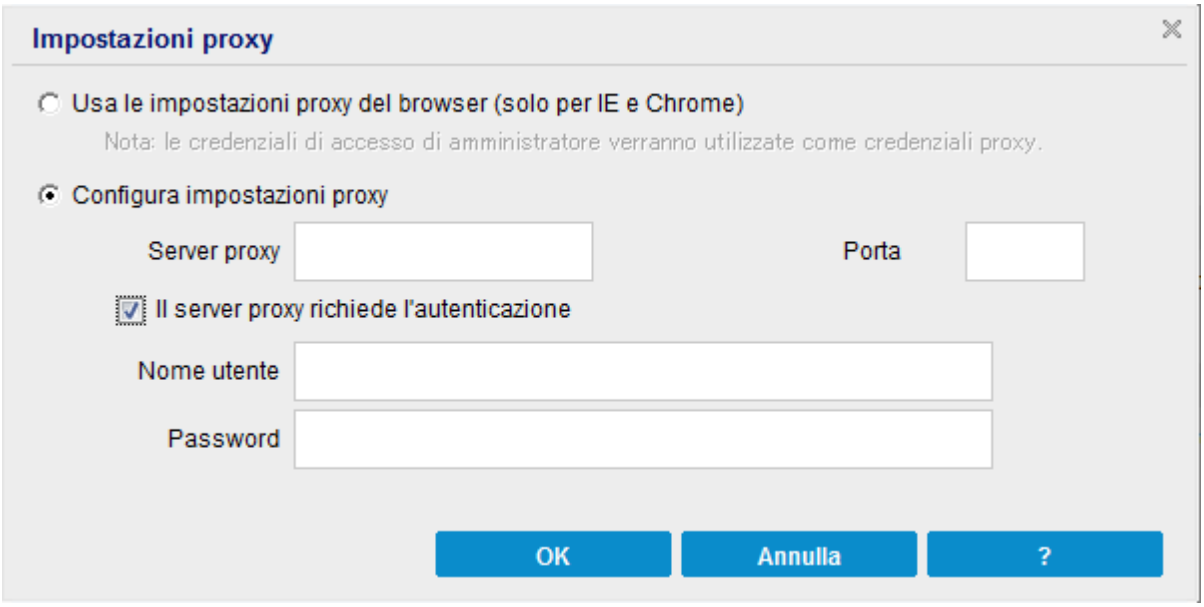
  Non è disponibile alcun aggiornamento

- **Impostazioni proxy**

  Nota: L'opzione **Server proxy** è disponibile solo se si seleziona il server Arcserve come server di download.

  Selezionare Impostazioni proxy.

  Selezionando questa opzione, verrà visualizzata la finestra di dialogo **Impostazioni proxy.**



Utilizza le impostazioni proxy del browser

Questa opzione è applicabile soltanto per Windows Internet Explorer (IE) e Google Chrome.

Se selezionata, Arcserve UDP rileva e utilizza automaticamente le stesse impostazioni proxy applicate al browser per stabilire la connessione al server Arcserve e acquisire le informazioni sull'aggiornamento di Arcserve UDP.

Configurazione delle impostazioni proxy

Se selezionata, questa opzione abilita la connessione del server proxy specificato al server Arcserve per le informazioni sull'aggiornamento di Arcserve UDP. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet.

Inoltre, sarà possibile specificare se il server proxy richiede l'autenticazione. Se selezionata, infatti, l'opzione indica che sono necessarie informazioni di autenticazione (ID utente e password) per l'utilizzo del server proxy.

Nota: il nome utente del dominio deve essere completo e presentare il formato <nome dominio>\<nome utente>.

Verifica connessione

Consente di verificare le seguenti connessioni e visualizza un messaggio di stato al completamento:

- Se è stato selezionato Server Arcserve come server di download, verifica la connessione tra il computer e il server Arcserve attraverso il server proxy specificato.
- Se è stato selezionato il server di gestione temporanea come server di download, verrà verificata la connessione fra il computer e il server di gestione temporanea specificato. Il pulsante Verifica connessione viene utilizzato per verificare la disponibilità di ciascun server di gestione temporanea in elenco. Lo stato del server viene visualizzato nel campo **Stato connessione**. Se nessuno dei server di gestione temporanea configurati è disponibile, nella parte superiore della console Arcserve UDP viene visualizzato il seguente messaggio: Server di aggiornamento non disponibile.

  Nota: La connessione di prova viene eseguita automaticamente all'apertura della pagina **Configurazione aggiornamento** nella scheda **Impostazioni** della console Arcserve UDP. Durante questa verifica automatica, verrà controllato lo stato della connessione più recente del server di download configurato in precedenza (server Arcserve o server di gestione temporanea, a seconda della selezione effettuata). Se sono stati configurati più server di gestione temporanea, la verifica automatica verrà eseguita su tutti i server di gestione temporanea per acquisire lo stato di connessione più recente.

Pianificazione aggiornamenti

Indica quando verificare la presenza di nuovi aggiornamenti di Arcserve UDP e scaricarli.

4. Fare clic su **Salva**.

Le impostazioni di preferenza per gli aggiornamenti vengono salvate.

Creazione di un server di gestione temporanea

Il server di gestione temporanea è un nodo sul quale viene installato l'agente o la console di Arcserve UDP. Il nodo deve completare il download degli aggiornamenti dal server di download di Arcserve in modo da poter funzionare come server di gestione temporanea in grado di fornire gli aggiornamenti.

Aggiunta di server di gestione temporanea:

È possibile aggiungere un server di gestione temporanea su qualsiasi nodo in grado di soddisfare i seguenti due requisiti:

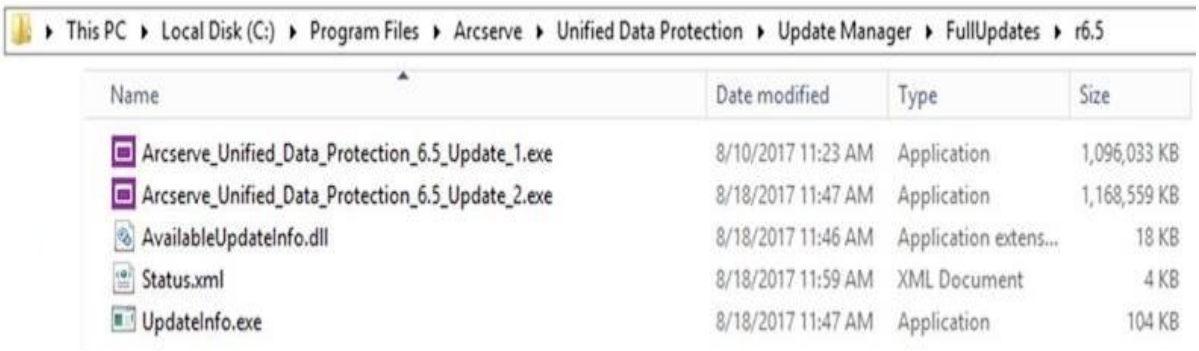
- Il nodo disponga dell'agente Arcserve UDP o della Console Arcserve UDP.
  - Arcserve UDPLa console di è in grado di scaricare gli aggiornamenti soltanto dal relativo server di gestione temporanea.
  - Arcserve UDPL'agente è in grado di scaricare gli aggiornamenti dal server di gestione temporaneo della console o dell'agente.
- Il nodo ha scaricato correttamente gli aggiornamenti dal server di download di Arcserve almeno una volta.

Nota: non è necessario eseguire l'altra configurazione se il server di gestione temporanea di destinazione soddisfa i prerequisiti.

Configurazione dell'aggiornamento dal server di gestione temporanea

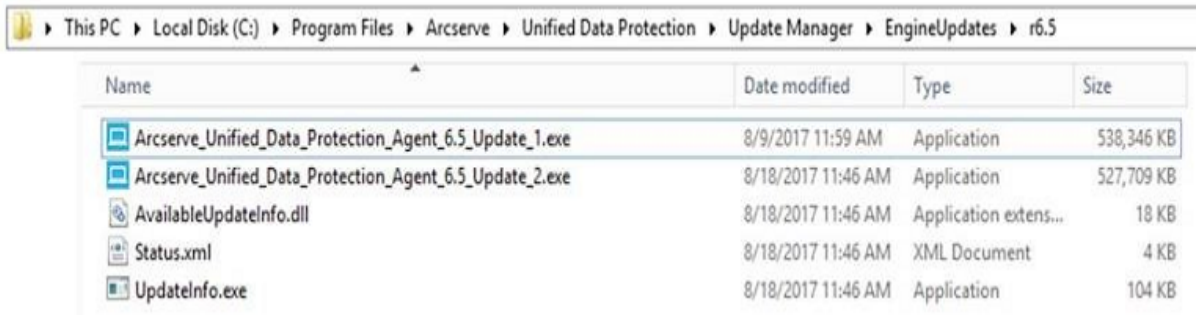
- Se viene selezionato il server di gestione temporanea della Console Arcserve UDP installata su tale nodo, tenere presenti le seguenti note:
  - Porta predefinita: 8015
  - La Console Arcserve UDP è in grado di acquisire gli aggiornamenti dal server di gestione temporanea
  - L'agente Arcserve UDP è in grado di acquisire gli aggiornamenti dal server di gestione temporanea

  Nota: dalla directory <UDP Installed path\Update Manager\FullUpdates> sul server di gestione temporanea di destinazione, verificare la disponibilità della versione di aggiornamento più recente. Di seguito viene riportato un esempio.



- Se viene selezionato il server di gestione temporanea per l'agente Arcserve UDP installato sul nodo in questione, considerare le seguenti note:
  - Porta predefinita: 8014
  - La Console Arcserve UDP non è in grado di acquisire gli aggiornamenti dal server di gestione temporanea
  - L'agente Arcserve UDP è in grado di acquisire gli aggiornamenti dal server di gestione temporanea

  Nota: dalla directory <UDP Installed path\Update Manager\EngineUpdates> sul server di gestione temporanea di destinazione, verificare la disponibilità della versione di aggiornamento più recente. Di seguito viene riportato un esempio.



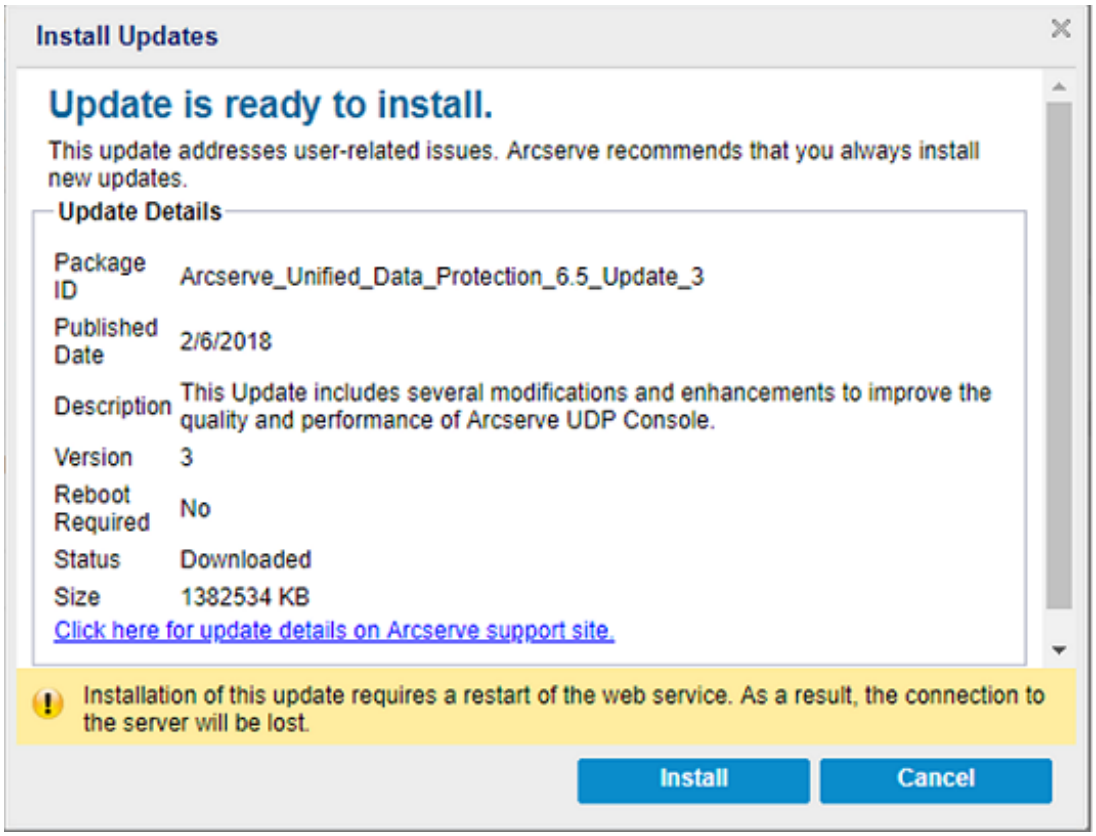
Verifica e installazione degli aggiornamenti

Dalla Console UDP, è possibile determinare se sono disponibili nuovi aggiornamenti.

Effettuare le operazioni seguenti:

1. Fare clic su **Verifica aggiornamenti** dal menu a discesa **?**. Se è disponibile un nuovo aggiornamento, viene visualizzato un messaggio nella barra superiore. Inoltre, viene visualizzata la finestra di dialogo **Update Installation** (Installazione aggiornamento).
2. Se si abilita la pianificazione degli aggiornamenti, quando è disponibile un nuovo aggiornamento, tale aggiornamento viene scaricato automaticamente sul server UDP. Nella barra superiore viene visualizzato un collegamento **Nuovi aggiornamenti disponibili** che fornisce un'indicazione visiva della presenza di un nuovo aggiornamento pronto per l'installazione.
3. Fare clic sul **collegamento Nuovi aggiornamenti disponibili** nella barra superiore.

   Viene visualizzata la finestra di dialogo **Installa aggiornamenti** contenente le informazioni relative all'aggiornamento disponibile. La finestra di dialogo include informazioni quali descrizione, stato del download, dimensioni, requisiti per il riavvio e un collegamento al server Arcserve per ottenere ulteriori informazioni sull'aggiornamento.



4. Fare clic su **Installa**.

   L'installazione degli aggiornamenti di Arcserve UDP viene avviata.

Aggiornamento degli agenti sui nodi remoti mediante Gateway

I nodi e il server remoti in un sito interagiscono con la console mediante un gateway. Arcserve UDP consente di rilevare e distribuire l'ultima versione dell'agente sui nodi. Per eseguire l'aggiornamento o l'installazione dell'agente Arcserve UDP per un nodo in un sito, utilizzare l'opzione Installa/Aggiorna agente.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro **Navigazione**, selezionare un sito dall'elenco a discesa.
3. Viene visualizzata la pagina **Nodi: Tutti i nodi**.
4. Selezionare uno o più nodi.
5. Dal riquadro centrale, fare clic sull'elenco a discesa **Azioni**, quindi fare clic su **Installa/Aggiorna agente**.

   I dettagli dell'installazione o dell'aggiornamento vengono visualizzati sul riquadro centrale.
6. Verificare i dettagli e fare clic su **OK**.

   Il nodo viene aggiornato all'ultima versione dell'agente di Arcserve UDP.

Aggiornamento del server RPS sul server remoto mediante gateway

I nodi e il server remoti in un sito interagiscono con la console mediante un gateway. Arcserve UDP consente di rilevare e distribuire l'ultima versione del componente RPS sui Recovery Point Server. In seguito alla distribuzione del componente RPS, il server è pronto per archiviare le sessioni di backup e fungere da Recovery Point Server. Per eseguire l'aggiornamento o l'installazione del componente RPS di Arcserve UDP su un Recovery Point Server in un sito, utilizzare l'opzione Installa/Aggiorna Recovery Point Server.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro **Navigazione**, selezionare un sito dall'elenco a discesa.
3. Fare clic su **Recovery Point Server**.

   Viene visualizzata la pagina **Destinazione:** Viene visualizzata la pagina **Recovery Point Server**.
4. Eseguire una delle seguenti operazioni:
   - Fare clic con il pulsante destro del mouse su un Recovery Point Server.
   - Selezionare un Recovery Point Server e dal riquadro centrale fare clic sul menu a discesa **Azioni**.

   Viene visualizzato un elenco di opzioni.
5. Fare clic su **Installazione o aggiornamento del Recovery Point Server**.

   Viene visualizzata la pagina **Installazione e aggiornamento**.
6. Modificare le impostazioni di distribuzione, quindi fare clic su **OK** per distribuire il Recovery Point Server sul nodo selezionato.

   La distribuzione del Recovery Point Server viene avviata. È possibile visualizzare l'avanzamento della distribuzione nel riquadro destro.

(Facoltativo) Installazione degli aggiornamenti di Arcserve UDP in modalità invisibile all'utente

L'installazione degli aggiornamenti in modalità invisibile all'utente consente di eseguire delle installazioni automatiche degli aggiornamenti senza richiedere alcun tipo di input da parte dell'utente.

Effettuare le operazioni seguenti:

1. Avviare l'installazione degli aggiornamenti di Arcserve UDP in modalità invisibile all'utente.

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

2. Configurare l'installazione invisibile all'utente mediante la sintassi seguente e i seguenti argomenti:

   UpdateExeFile

   Consente di eseguire il file eseguibile auto-estraente.

   s

   Consente di eseguire il file eseguibile auto-estraente tramite la modalità invisibile all'utente.

   v

   Specifica gli argomenti aggiuntivi per l'installazione dell'aggiornamento.

   Argomenti aggiuntivi

   /s

   Consente di eseguire l'installazione degli aggiornamenti in modalità invisibile all'utente.

   /AutoReboot

   Definisce l'esecuzione di un riavvio automatico dopo l'installazione dell'aggiornamento. Se per completare l'aggiornamento è necessario riavviare il sistema, il computer si riavvierà automaticamente senza nessuna notifica.

   Esempi:

   - Per installare un aggiornamento mediante la modalità invisibile all'utente senza eseguire il riavvio automatico al completamento, utilizzare il comando seguente:

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

- Per installare un aggiornamento mediante la modalità invisibile all'utente e non eseguire il riavvio automatico al completamento, utilizzare il seguente comando:

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

Verifica dell'installazione degli aggiornamenti

Dalla Console Arcserve UDP, selezionare la **Guida in linea**, quindi fare clic su **Informazioni** e verificare che in questa finestra di dialogo di Arcserve UDP sia visualizzata la versione più recente aggiornata.

Disinstallazione dell'Arcserve UDP

Per disinstallare Arcserve Unified Data Protection, è possibile utilizzare i metodi seguenti:

- **Disinstallazione standard**: utilizzare questo metodo per eseguire la disinstallazione mediante il pannello di controllo di Windows.
- **Disinstallazione invisibile all'utente**: questo metodo consente di eseguire disinstallazioni automatiche mediante la riga di comando di Windows.

Disinstallazione standard

È possibile disinstallare i seguenti componenti:

- Console Arcserve Unified Data Protection
- Recovery Point Server Arcserve Unified Data Protection
- Agente Arcserve Unified Data Protection

Effettuare le operazioni seguenti:

1. Aprire il Pannello di controllo di Windows.
2. Fare clic sull'opzione di disinstallazione del programma.

   Verrà visualizzata la finestra di dialogo di disinstallazione o modifica del programma.
3. Selezionare Arcserve Unified Data Protection e fare clic su Disinstalla.

   Viene visualizzata la finestra di dialogo Applicazione di disinstallazione di Arcserve Unified Data Protection.
4. Selezionare i componenti da disinstallare e da fare clic Avanti.

   Viene visualizzata la finestra di dialogo **Messaggi**.
5. Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo **Rimuovi componenti**.
6. Fare clic su **Rimuovi**.

   I componenti selezionati vengono disinstallati dal computer.

Disinstallazione invisibile all'utente

Utilizzando la disinstallazione invisibile all'utente, non sarà necessario alcun intervento da parte dell'utente.

Effettuare le operazioni seguenti:

1. Accedere al computer da cui si desidera disinstallare i componenti di Arcserve UDP.

   Nota: Accedere al computer utilizzando un account amministrativo.

2. Aprire la riga di comando di Windows ed eseguire il seguente comando che corrisponde al sistema operativo specificato:

   - **Sistema operativo x86:**

     Per disinstallare tutti i componenti

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

     Per disinstallare i componenti selezionati

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

   - **Sistema operativo x64:**

     Per disinstallare tutti i componenti

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

     Per disinstallare i componenti selezionati

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

   I valori seguenti definiscono i codici restituiti:

   0 = Disinstallazione completata correttamente.

   3010 = Disinstallazione completata correttamente. È richiesto il riavvio.

   Altro = Errore di disinstallazione.

   Uso:

   La tabella sottostante definisce il codice di prodotto che è necessario specificare per il componente di Arcserve Unified Data Protection da disinstallare.

   Esempio:

   La seguente sintassi consente di disinstallare il Recovery Point Server Arcserve Unified Data Protection in modalità invisibile all'utente.

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

Componente	<Codice prodotto>
Agente Arcserve Unified Data Protection (piattaforme x86)	{CAAD8AEA-A455-4A9F-9B48-C3838976646A}
Agente Arcserve Unified Data Protection (piattaforme x64)	{CAAD1E08-FC33-462F-B5F8-DE9B765F2C1E}
Arcserve Unified Data Protection Recovery Point Server	{CAAD8172-1858-4DC7-AE81-C887FA6AFB19}
Console Arcserve Unified Data Protection	{CAAD3E40-C804-4FF0-B1C0-26D534D438C0}
Gateway Arcserve Unified Data Protection	{FB95E75D-494F-4146-9B35-F867434B264A}

Dopo l'esecuzione del comando, i componenti di Arcserve UDP vengono disinstallati.

Rimozione dei componenti ignorati dal programma di disinstallazione

Importante:

1. Le licenze Arcserve sono condivise da tutti i prodotti Arcserve. Verificare che sul computer non siano installati altri prodotti Arcserve. In caso contrario, la licenza per tutti i prodotti Arcserve installati sul computer potrebbe andare persa.
2. Se i componenti vengono rimossi, qualsiasi programma installato dopo l'Agente Arcserve Unified Data Protection per Windows e dipendente da tali componenti potrebbe non funzionare correttamente.

   Se si desidera rimuovere manualmente questi componenti, procedere come segue:

   Rimozione manuale del componente Arcserve Licensing

1. Accedere alla directory *C:\Programmi (x86)\Arcserve\SharedComponents\CA_LIC*.
2. Individuare il file zip denominato *lic98_uninstaller.zip* ed estrarlo in un'altra posizione (ad esempio C:\temp).
3. Accedere alla posizione di estrazione dei file e individuare i due file di script denominati *rmlic.exe* e *rmlicense.bat.*.
4. Fare clic su *rmlicense.bat* per eseguire lo script di disinstallazione dei componenti.
5. Eliminare manualmente le seguenti cartelle:
   - C:\Programmi (x86)\Arcserve
   - C:\Programmi\Arcserve
   - La cartella di estrazione del file zip.
6. Rimuovere la chiave di registro per il componente Arcserve Licensing.
   - Per la piattaforma x64: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Arcserve\License
   - Per la piattaforma x86: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\License

   Rimozione manuale di Microsoft Visual C++ e Microsoft SQL Server Express

1. Accedere all'applicazione standard Installazione applicazioni situata nel Pannello di controllo di Windows (Pannello di controllo, Programmi e funzionalità, Rimuovi programmi).
2. Selezionare *Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501* e fare clic su Disinstalla.

3. Selezionare *Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501* e fare clic su Disinstalla.
4. Selezionare Microsoft SQL Server 2014 (a 64 bit) e fare clic su Disinstalla.
5. Per rimuovere solamente il database Arcserve UDP, selezionare ARCSERVE_APP e fare clic su Disinstalla.

Chapter 4: Aggiornamento ad Arcserve UDP versione 8.0

La presente sezione descrive i seguenti argomenti:

Nota: per le procedure consigliate sulle modalità di protezione del server Arcserve UDP, consultare la sezione Protezione del server Arcserve UDP.

Versioni supportate per l'aggiornamento

Arcserve UDP 8.1 fornisce l'aggiornamento e la compatibilità con le versioni precedenti in base alle regole seguenti:

- Arcserve UDP 8.1 supporta l'aggiornamento da Arcserve UDP versione 8.0, 7.0 Aggiornamento 2, 7.0 Aggiornamento 1, 7.0 versione finale e Arcserve UDP versione 6.5 Aggiornamento 4.

  Note: prima di eseguire l'aggiornamento ad Arcserve UDP 8.1 da altre versioni precedenti, considerare quanto segue:

  - Per Arcserve UDP 6.5 con Aggiornamento 3, Aggiornamento 2, Aggiornamento 1 o versione finale, eseguire prima l'aggiornamento a UDP 6.5 Aggiornamento 4.
  - Per Arcserve UDP versione 6.0 Aggiornamento 3 per Windows, eseguire prima l'aggiornamento a Arcserve UDP versione 7.0.
  - Per Arcserve UDP versione 6.0 Aggiornamento 2, Aggiornamento 1 o versione finale per Windows, eseguire prima l'aggiornamento a Arcserve UDP versione 6.5 Aggiornamento 4.
  - Per Arcserve UDP versione 6.0 Aggiornamento 1 o versione finale per Linux, eseguire prima l'aggiornamento a Arcserve UDP versione 6.5 Aggiornamento 4.
  - Per Arcserve UDP 5.0 Aggiornamento 4, eseguire prima l'aggiornamento a UDP 6.5 Aggiornamento 4.
  - Per Arcserve UDP 5.0 con Aggiornamento 3, Aggiornamento 2, Aggiornamento 1 o versione finale, eseguire prima l'aggiornamento a UDP 6.0 Aggiornamento 3, quindi l'aggiornamento a UDP 7.0.

- Arcserve UDP 8.1 non supporta l'aggiornamento da Arcserve D2D r16.5, Arcserve Central Protection Management r16.5, Arcserve Data Protection Console r16.5, Arcserve Central Reporting r16.5 e Arcserve Central Virtual Standby r16.5.

  Per ulteriori informazioni, consultare la sezione Procedura per aggiornare la licenza di Arcserve UDP.

Sequenza di aggiornamento sull'appliance Arcserve

Arcserve UDP versione 8.0 supporta l'aggiornamento sull'appliance.
L'aggiornamento potrebbe avvenire in base alle sequenze riportate di seguito:

- Aggiornamento di Arcserve UDP
  - Aggiornamento dell'appliance Arcserve eseguita come console e server RPS Arcserve UDP
  - Aggiornamento dell'appliance Arcserve eseguita solo come server RPS Arcserve UDP
  - Procedura di aggiornamento per gli ambienti in cui vengono utilizzati due o più appliance Arcserve
- Aggiornamento dell'agente Arcserve per Linux sull'appliance Arcserve UDP
- Aggiornamento di Arcserve Backup sull'appliance Arcserve

Aggiornamento dell'appliance Arcserve eseguita come console e server RPS Arcserve UDP

Aggiornare l'appliance Arcserve, quindi completare la sequenza di aggiornamento descritta per eseguire l'aggiornamento dell'ambiente.

Aggiornamento dell'appliance Arcserve eseguita solo come server RPS Arcserve UDP

Eseguire l'aggiornamento dell'ambiente produttivo completo. Per ulteriori informazioni, consultare la sezione Sequenza di aggiornamento.

Procedura di aggiornamento per gli ambienti in cui vengono utilizzati due o più appliance Arcserve

Eseguire l'aggiornamento dell'intero ambiente intero di produzione. Per ulteriori informazioni, consultare la sezione Sequenza di aggiornamento.

Aggiornamento dell'agente Arcserve per Linux sull'appliance Arcserve UDP

1. Aggiornare la console Arcserve UDP, che permette di gestire l'ambiente del server di backup Linux.
2. Aggiornare il server di backup Linux sull'appliance Arcserve. Per ulteriori informazioni, fare riferimento alla *Guida in linea dell'agente Arcserve Unified Data Protection per Linux*.

Aggiornamento di Arcserve Backup sull'appliance Arcserve

Fare riferimento alla *Guida all'implementazione di Arcserve Backup* per completare l'aggiornamento sull'appliance Arcserve.

Criterio per il supporto della compatibilità con le versioni precedenti

Si consiglia di aggiornare tutti i componenti a Arcserve UDP versione 8.1 nell'ambiente completo in modo da garantire il corretto funzionamento delle nuove funzionalità di Arcserve UDP versione 8.1. I piani di backup esistenti non risulteranno interessati se l'aggiornamento non viene completato per tutti i componenti contemporaneamente.

La compatibilità con le versioni precedenti supporta Arcserve UDP versione 8.0, 7.0, 7.0 Aggiornamento 1, 7.0 Aggiornamento 2 e Arcserve UDP 6.5 Aggiornamento 4.

La presente sezione descrive i seguenti argomenti:

Criterio per il supporto della compatibilità con le versioni precedenti per Arcserve UDP versione 8.0

Supporto della compatibilità con le versioni precedenti tra diverse console UDP mediante l'attività Replica su server RPS gestito in remoto

Se si desidera eseguire l'attività *Replica su server RPS gestito in remoto*, aggiornare la console e il server RPS di destinazione prima di aggiornare la console, il server RPS o l'agente di origine.

- La replica è supportata se la versione del server RPS di origine è UDP 8.1, mentre quella del server RPS di destinazione è ancora la 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2.
- La replica è supportata se la versione del server RPS di origine è UDP 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2, mentre quella del server RPS di destinazione è UDP 8.1.
- Comportamenti di replica:
  - Se si esegue l'aggiornamento a UDP 8.1 su entrambi i siti, è possibile eseguire la replica da Cloud Hybrid a on-premise senza un indirizzo IP pubblico (nuovo comportamento UDP).
  - Se si esegue l'aggiornamento a UDP 8.1 solo su uno dei siti e l'altro sito utilizza una versione supportata di UDP, è possibile eseguire la replica da Cloud Hybrid a on-premise utilizzando l'IP pubblico.

Supporto della compatibilità con le versioni precedenti per il server RPS o l'agente Windows (o proxy di backup senza agente)

- La console di Arcserve UDP 8.1 supporta i Recovery Point Server (RPS) e gli agenti (o i proxy di backup senza agente) di UDP 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2 per il backup se il piano non viene modificato in seguito all'aggiornamento.
- La console di Arcserve UDP 8.1 e il Recovery Point Server (RPS) supportano gli agenti (o i proxy di backup senza agente) di UDP 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2 per il backup se il piano non viene modificato in seguito all'aggiornamento.
- La console di Arcserve UDP 8.1 supporta la distribuzione del piano esistente senza alcuna modifica quando il server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione in UDP 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2. L'agente non viene aggiornato automaticamente.
- La console di Arcserve UDP 8.1 supporta azioni come la sospensione o la ripresa del piano esistente senza alcuna modifica quando il server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione in UDP 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2. L'agente non viene aggiornato automaticamente.
- La console di Arcserve UDP 8.1 supporta la creazione di nuovi piani o la modifica dei piani esistenti per configurare le funzionalità legacy già supportate nella release precedente quando i server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione in UDP 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2. L'agente non viene aggiornato automaticamente.
- La console di Arcserve UDP 8.1 supporta la creazione di nuovi piani o la modifica dei piani esistenti per includere le nuove funzionalità di UDP 8.1 quando il server RPS, il proxy o l'agente associati sono già aggiornati alla versione prevista.

  Ad esempio:

  - La definizione di una rete di backup è supportata se la console, il server RPS, il proxy e l'agente vengono aggiornati a UDP 7.0, 7.0 Aggiornamento 1, 7.0 Aggiornamento 2, 8.0 e 8.1.
- La console di Arcserve UDP 8.1 supporta il nodo di aggiornamento quando il server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione in UDP 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2. Il piano verrà distribuito. L'agente non viene aggiornato automaticamente.
- La console di Arcserve UDP 8.1 supporta l'aggiunta di un server RPS versione 8.0. Tuttavia, il server RPS non viene aggiornato automaticamente ad Arcserve UDP versione 8.1 al momento dell'aggiunta.

- La console di Arcserve UDP 8.1 supporta l'aggiunta di una versione precedente dell'agente (o del proxy di backup senza agente) senza l'aggiornamento automatico dell'agente.
- La console di Arcserve UDP8.1 supporta l'aggiunta di nodi al piano esistente.
  - L'aggiunta di un nodo pulito al piano esistente è supportata quando il server RPS associato viene aggiornato alla versione 8.1. In caso contrario, il piano viene salvato ma la sua distribuzione non riesce.
  - L'aggiunta di un nodo con versione precedente al piano esistente è supportata se la versione è simile a quella del server RPS in esecuzione. L'agente non viene aggiornato automaticamente.
  - L'aggiunta di un nodo Arcserve UDP 8.1 al piano esistente è supportata quando il server RPS associato esegue l'aggiornamento alla versione UDP 8.1.
- Il gateway viene aggiornato automaticamente in modo che corrisponda alla versione della console di Arcserve UDP.
- Criterio di compatibilità con le versioni precedenti di replica:
  - La replica è supportata se la console viene aggiornata a Arcserve UDP 8.1 ma tutti i Recovery Point Server (RPS) associati sono ancora in esecuzione su UDP 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2.
    - La replica è supportata da un server RPS di origine Arcserve UDP 8.1 a un server RPS di destinazione di UDP 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2.
    - La replica è supportata dal server RPS di origine di Arcserve UDP UDP 8.0, 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2 al server RPS di destinazione UDP 8.1.
- Criterio di compatibilità con le versioni precedenti di Virtual Standby:
  - La versione del computer di monitoraggio o del proxy VSB deve essere analoga a quella dell'agente quando la destinazione di backup è una cartella condivisa.
  - La versione del computer di monitoraggio o del proxy VSB deve essere analoga a quella del server RPS quando la destinazione di backup è un server RPS.
- Criterio di compatibilità con le versioni precedenti del computer virtuale istantaneo:

  La versione del server di ripristino del computer virtuale istantaneo deve essere analoga a quella della console Arcserve UDP.

Criterio per il supporto della compatibilità con le versioni precedenti per Arcserve UDP versione 7.x

Supporto della compatibilità con le versioni precedenti tra diverse console UDP mediante l'attività Replica su server RPS gestito in remoto

Se si desidera eseguire l'attività *Replica su server RPS gestito in remoto*, aggiornare la console e il server RPS di destinazione prima di aggiornare la console, il server RPS o l'agente di origine.

- La replica è supportata se la versione del server RPS di origine è UDP 8.1, mentre quella del server RPS di destinazione è ancora UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2.
- La replica è supportata se la versione del server RPS di origine è UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2, mentre quella del server RPS di destinazione è UDP 8.1.
- Comportamenti di replica:
  - Se si esegue l'aggiornamento a UDP 8.1 su entrambi i siti, è possibile eseguire la replica da Cloud Hybrid a on-premise senza un indirizzo IP pubblico (nuovo comportamento UDP).
  - Se si esegue l'aggiornamento a UDP 8.1 solo su uno dei siti e l'altro sito utilizza una versione supportata di UDP, è possibile eseguire la replica da Cloud Hybrid a on-premise utilizzando l'IP pubblico.

Supporto della compatibilità con le versioni precedenti per il server RPS o l'agente Windows (o proxy di backup senza agente)

- La console di Arcserve UDP 8.1 supporta i Recovery Point Server (RPS) e gli agenti (o i proxy di backup senza agente) di UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2 per il backup se il piano non viene modificato in seguito all'aggiornamento.
- La console di Arcserve UDP 8.1 e il Recovery Point Server (RPS) supportano gli agenti (o i proxy di backup senza agente) di UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2 per il backup se il piano non viene modificato in seguito all'aggiornamento.
- La console di Arcserve UDP 8.1 supporta la distribuzione del piano esistente senza alcuna modifica quando il server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione in UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2. L'agente non viene aggiornato automaticamente.

- La console di Arcserve UDP 8.1 supporta azioni come la sospensione o la ripresa del piano esistente senza alcuna modifica quando il server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione in UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2. L'agente non viene aggiornato automaticamente.
- La console di Arcserve UDP 8.1 supporta la creazione di nuovi piani o la modifica dei piani esistenti per configurare le funzionalità legacy già supportate nella release precedente quando i server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione in UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2. L'agente non viene aggiornato automaticamente.
- La console di Arcserve UDP 8.1 supporta la creazione di nuovi piani o la modifica dei piani esistenti per includere le nuove funzionalità della versione UDP 8.1 quando il server RPS, il proxy o l'agente associati sono già aggiornati alla versione prevista.

  Ad esempio:

  - La definizione di una rete di backup è supportata se la console, il server RPS, il proxy e l'agente vengono aggiornati a UDP 7.0, 7.0 Aggiornamento 1, 7.0 Aggiornamento 2, 8.0 e 8.1.
- La console di Arcserve UDP 8.1 supporta il nodo di aggiornamento quando il server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione in UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2. Il piano verrà distribuito. L'agente non viene aggiornato automaticamente.
- La console di Arcserve UDP 8.1 supporta l'aggiunta di una versione UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2 del server RPS. Tuttavia, il server RPS non viene aggiornato automaticamente ad Arcserve UDP 8.1 al momento dell'aggiunta.
- La console di Arcserve UDP 8.1 supporta l'aggiunta di una versione precedente dell'agente (o del proxy di backup senza agente) senza l'aggiornamento automatico dell'agente.
- La console di Arcserve UDP8.1 supporta l'aggiunta di nodi al piano esistente.
  - L'aggiunta di un nodo pulito al piano esistente è supportata quando il server RPS associato viene aggiornato alla versione UDP 8.1. In caso contrario, il piano viene salvato ma la sua distribuzione non riesce.
  - L'aggiunta di un nodo con versione precedente al piano esistente è supportata se la versione è simile a quella del server RPS in esecuzione. L'agente non viene aggiornato automaticamente.

        - L'aggiunta di un nodo Arcserve UDP 8.1 al piano esistente è supportata quando il server RPS associato esegue l'aggiornamento alla versione UDP 8.1.
- Il gateway viene aggiornato automaticamente in modo che corrisponda alla versione della console di Arcserve UDP.
- Criterio di compatibilità con le versioni precedenti di replica:
    - La replica è supportata se la console viene aggiornata a Arcserve UDP 8.1 ma tutti i Recovery Point Server (RPS) associati sono ancora in esecuzione su UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2.
        - La replica è supportata da un server RPS di origine Arcserve UDP 8.1 a un server RPS di destinazione di UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2.
        - La replica è supportata dal server RPS di origine Arcserve UDP UDP 7.0, 7.0 Aggiornamento 1 e 7.0 Aggiornamento 2 al server RPS di destinazione UDP 8.1.
- Criterio di compatibilità con le versioni precedenti di Virtual Standby:
    - La versione del computer di monitoraggio o del proxy VSB deve essere analoga a quella dell'agente quando la destinazione di backup è una cartella condivisa.
    - La versione del computer di monitoraggio o del proxy VSB deve essere analoga a quella del server RPS quando la destinazione di backup è un server RPS.
- Criterio di compatibilità con le versioni precedenti del computer virtuale istantaneo:

  La versione del server di ripristino del computer virtuale istantaneo deve essere analoga a quella della console Arcserve UDP.

Criterio per il supporto della compatibilità per Arcserve UDP versione 6.5 Aggiornamento 4

Supporto della compatibilità con le versioni precedenti tra diverse console UDP mediante l'attività Replica su server RPS gestito in remoto

Se si desidera eseguire l'attività *Replica su server RPS gestito in remoto*, aggiornare la console e il server RPS di destinazione prima di aggiornare la console, il server RPS o l'agente di origine.

- La replica è supportata se la versione del server RPS di origine è UDP 8.1, mentre quella del server RPS di destinazione è ancora la 6.5 Aggiornamento 4.
- La replica è supportata se la versione del server RPS di origine è la 6.5 Aggiornamento 4 e quella del server RPS di destinazione è UDP 8.1 e viene applicata la patch P00001738. Se la versione del server RPS di origine è la 6.5 aggiornamento 1, 2 o 3, eseguire prima l'aggiornamento 4, quindi applicare la patch P00001738.

Supporto della compatibilità con le versioni precedenti per il server RPS o l'agente Windows (o proxy di backup senza agente)

- La console di Arcserve UDP 8.1 supporta i Recovery Point Server (RPS) e gli agenti (o i proxy di backup senza agente) della versione 6.5 Aggiornamento 4 per il backup se il piano non viene modificato in seguito all'aggiornamento.
- La console di Arcserve UDP 8.1 e il server RPS corrispondente supportano gli agenti (o i proxy di backup senza agente) della versione 6.5 Aggiornamento 4 per il backup se il piano non viene modificato in seguito all'aggiornamento.
- La console di Arcserve UDP 8.1 supporta la distribuzione del piano esistente senza alcuna modifica quando il server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione nella versione 6.5 Aggiornamento 4. L'agente non viene aggiornato automaticamente.
- La console di Arcserve UDP 8.1 supporta azioni come la sospensione o la ripresa del piano esistente senza alcuna modifica quando il server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione nella versione 6.5 Aggiornamento 4. L'agente non viene aggiornato automaticamente.
- La console di Arcserve UDP 8.1 supporta la creazione di nuovi piani o la modifica dei piani esistenti per configurare le funzionalità legacy già supportate nella release precedente quando i server RPS e gli agenti (o i proxy di backup

senza agente) sono ancora in esecuzione nella versione 6.5 Aggiornamento 4. L'agente non viene aggiornato automaticamente.

- La console di Arcserve UDP 8.1 supporta la creazione di nuovi piani o la modifica dei piani esistenti per includere le nuove funzionalità della versione UDP 8.1 quando il server RPS, il proxy o l'agente associati sono già aggiornati alla versione prevista.

  Ad esempio:

  - La definizione di una rete di backup è supportata se la console, il server RPS, il proxy e l'agente vengono aggiornati alla versione 7.0 Aggiornamento 1, Aggiornamento 2 o a UDP 8.1.
- La console di Arcserve UDP 8.1 supporta il nodo di aggiornamento quando il server RPS e gli agenti (o i proxy di backup senza agente) sono ancora in esecuzione nella versione 6.5 Aggiornamento 4. Il piano verrà distribuito. L'agente non viene aggiornato automaticamente.
- La console di Arcserve UDP 8.1 supporta l'aggiunta di un server RPS versione 6.5 Aggiornamento 4. Tuttavia, il server RPS non viene aggiornato automaticamente ad Arcserve UDP 8.1 al momento dell'aggiunta.
- La console di Arcserve UDP 8.1 supporta l'aggiunta di una versione precedente dell'agente (o del proxy di backup senza agente) senza l'aggiornamento automatico dell'agente.
- La console di Arcserve UDP8.1 supporta l'aggiunta di nodi al piano esistente.
  - L'aggiunta di un nodo pulito al piano esistente è supportata quando il server RPS associato viene aggiornato alla versione UDP 8.1. In caso contrario, il piano viene salvato ma la sua distribuzione non riesce.
  - L'aggiunta di un nodo con versione precedente al piano esistente è supportata se la versione è simile a quella del server RPS in esecuzione. L'agente non viene aggiornato automaticamente.
  - L'aggiunta di un nodo Arcserve UDP 8.1 al piano esistente è supportata quando il server RPS associato esegue l'aggiornamento alla versione UDP 8.1.
- Il gateway viene aggiornato automaticamente in modo che corrisponda alla versione della console di Arcserve UDP.
- Criterio di compatibilità con le versioni precedenti di replica:
  - La replica è supportata quando la console viene aggiornata a Arcserve UDP 8.1 ma tutti i server RPS associati vengono ancora eseguiti nella versione 6.5 Aggiornamento x.

- La replica è supportata da un server RPS di origine Arcserve UDP 6.5 Aggiornamento x a un server RPS di destinazione 6.5 Aggiornamento 4.
- La replica è supportata da un server RPS di origine Arcserve UDP 6.5 Aggiornamento 4 a un server RPS di destinazione 6.5 Aggiornamento x.

- La replica è supportata da un server Arcserve UDP 6.5 Aggiornamento x di origine a un server RPS di destinazione UDP 8.1.
- La replica è supportata da un server RPS di origine Arcserve UDP 8.1 Aggiornamento a un server RPS di destinazione 6.5 Aggiornamento 4.
- La replica non è supportata da un server RPS di origine Arcserve UDP 8.1 a un server RPS di destinazione 6.5 Aggiornamento 3, Aggiornamento 2, Aggiornamento 1 o versione finale.

- Criterio di compatibilità con le versioni precedenti di Virtual Standby:
  - La versione del computer di monitoraggio o del proxy VSB deve essere analoga a quella dell'agente quando la destinazione di backup è una cartella condivisa.
  - La versione del computer di monitoraggio o del proxy VSB deve essere analoga a quella del server RPS quando la destinazione di backup è un server RPS.
- Criterio di compatibilità con le versioni precedenti del computer virtuale istantaneo:

  La versione del server di ripristino del computer virtuale istantaneo deve essere analoga a quella della console Arcserve UDP.

Supporto della compatibilità con le versioni precedenti del server di backup Linux

Per i server di backup Linux 7.x e 6.5.x:

- La console di Arcserve UDP 8.1 supporta i server di backup Linux versione 6.5.x e 7.x se il Recovery Point Server (RPS) utilizza Arcserve UDP 8.1. Tutti i processi vengono eseguiti correttamente, ad eccezione della nuova funzionalità o del miglioramento nella versione UDP 8.1.
- La console di Arcserve UDP 8.1 supporta i Recovery Point Server (RPS) e i server di backup Linux delle versioni 6.5.x e 7.x. Tutti i processi devono essere eseguiti senza problemi, ad eccezione della nuova funzionalità o del miglioramento nella versione 8.1.
- Dopo aver aggiornato il server di backup Linux ad Arcserve UDP 8.1, tutte le nuove funzionalità di UDP 8.1 saranno supportate.

Sequenza di aggiornamento per console UDP, server RPS e agente

In base alla politica di assistenza di compatibilità retroattiva, pianificare l'aggiornamento in base alla seguente sequenza consente di procedere in maniera più veloce:

1. Aggiornare la console Arcserve UDP.
2. Aggiornare il server RPS Arcserve UDP (sito DR).
3. Aggiornare Arcserve UDP RPS (Datacenter).
4. Aggiornare il proxy senza agente Arcserve UDP e alcuni agenti (oppure tutti) nel Datacenter.
5. Aggiornare Arcserve UDP RPS (sito remoto).
6. Aggiornare il proxy senza agente Arcserve UDP e alcuni agenti (oppure tutti) nel sito remoto.

   Nota: ripetere i passaggi 5 e 6 per ogni posizione remota.

   Note:

   - Se è configurata l'attività di replica MSP, aggiornare prima il sito MSP sulla console o sul server RPS.
   - Il gateway viene aggiornato automaticamente in modo che corrisponda alla versione della console.
   - In base al criterio per il supporto della compatibilità con le versioni precedenti ai fini della replica, aggiornare sempre il server RPS di destinazione prima di quello di origine.

Aggiornamento ad Arcserve UDP 8.0 da una release precedente

Aggiornare la versione di un'installazione significa reinstallare le funzionalità o i componenti con una versione successiva. Il processo di aggiornamento consente di mantenere la maggior parte delle impostazioni correnti e di effettuare la migrazione al nuovo database Arcserve UDP delle informazioni archiviate nel database Arcserve UDP precedente.

Considerazioni per l'aggiornamento

- Verificare che i requisiti hardware di Arcserve UDP versione 8.0 siano soddisfatti. Per ulteriori informazioni, consultare la sezione *Informazioni sul sistema* nelle *Note di rilascio v8.0*.
- È necessario utilizzare piattaforme, hypervisor, sistemi operativi o versioni dell'applicazione supportati da Arcserve UDP versione 8.0. Per ulteriori informazioni, consultare la matrice di compatibilità.
- Evitare di sospendere un piano esistente prima di eseguire l'aggiornamento dalla versione 6.5.3 o dalle versioni supportate precedenti. Se il piano viene sospeso prima dell'aggiornamento, potrà essere ripreso solo dopo l'aggiornamento di tutti i server RPS correlati.
- Acquistare il codice Product Key per Arcserve UDP versione 8.0 e tenerlo a disposizione.
- Rimuovere la versione precedente dell'utilità standalone Arcserve Exchange Granular Restore (AEGR) per Arcserve UDP versione 5.0. Se viene rilevata, nella procedura di installazione guidata verrà richiesto di rimuoverla.
- In generale, i piani precedenti dovrebbero funzionare correttamente in ogni fase di aggiornamento descritta.

Per aggiornare la versione, procedere come segue:

1. Per il sito MSP, aggiornare la console Arcserve UDP precedente ad Arcserve UDP 8.0.

   Questa operazione è obbligatoria se nella release precedente è stata configurata l'opzione **Attività: Replica da server RPS gestito in remoto**.

   Note:

   - Se il nodo comprende solo la console, aggiornare la console. Non è necessario interrompere i processi in esecuzione per eseguire l'aggiornamento della Console.

- Se il nodo comprende la console e il server RPS, pianificare l'aggiornamento della console quando non vi sono processi in esecuzione prima dell'aggiornamento. Se necessario, interrompere l'archivio dati del server RPS per annullare i processi in esecuzione prima di aggiornare la console.
- Per ulteriori informazioni sull'aggiornamento della console, consultare la sezione Installazione di Arcserve Unified Data Protection mediante la procedura guidata di installazione o Installazione di Arcserve UDP mediante il programma di installazione unificato.

2. Per il sito MSP, aggiornare il server RPS Arcserve UDP precedente ad Arcserve UDP versione 8.0.

   Questa operazione è obbligatoria se nella release precedente è stata configurata l'opzione **Attività: Replica da server RPS gestito in remoto**.

   Note:

   - Pianificare l'aggiornamento del server RPS quando nessun processo è in esecuzione prima dell'aggiornamento. Se necessario, interrompere l'archivio dati del server RPS per annullare i processi in esecuzione prima di aggiornare il server RPS.
   - Per ulteriori informazioni sull'aggiornamento del server RPS, consultare la sezione Installazione/Aggiornamento del Recovery Point Server.

3. Per il sito Cliente, aggiornare la console Arcserve UDP precedente ad Arcserve UDP versione 8.0.

   Note:

   - Se il nodo comprende solo la console, aggiornare la console. Non è necessario interrompere i processi in esecuzione per eseguire l'aggiornamento della Console.
   - Se il nodo comprende la console e il server RPS e sono presenti processi in esecuzione sul server RPS, arrestare l'archivio dati del server RPS e annullare prima i processi in esecuzione. Aggiornare quindi la console.
   - Per ulteriori informazioni sull'aggiornamento della console, consultare la sezione Installazione di Arcserve Unified Data Protection mediante la procedura guidata di installazione o Installazione di Arcserve UDP mediante il programma di installazione unificato.

4. Per il sito Cliente, aggiornare il precedente server RPS Arcserve UDP di destinazione della replica ad Arcserve UDP 8.0.

   Note:

- Arcserve UDP 8.0 supporta la replica da un serve RPS di origine Arcserve UDP versione 6.5.x a un server RPS di destinazione Arcserve UDP 8.0. Quando il piano include più attività di replica, aggiornare innanzitutto l'ultimo server RPS di destinazione della replica.
- La replica dal serve RPS di origine Arcserve UDP 8.0 a una versione precedente del server RPS di destinazione è supportata solo se il server RPS di destinazione è Arcserve UDP versione 6.5 Aggiornamento 4.
- Per ulteriori informazioni sull'aggiornamento del server RPS, consultare la sezione Installazione/Aggiornamento del Recovery Point Server.

5. Per il sito Cliente, aggiornare il precedente server RPS di origine della replica ad Arcserve UDP 8.0.

   Nota: per ulteriori informazioni sull'aggiornamento del server RPS, consultare la sezione Installazione/Aggiornamento del Recovery Point Server.

6. Per il sito Cliente, aggiornare i precedenti proxy e agenti ad Arcserve UDP 8.0.

   Note:

   - Per ulteriori informazioni sull'aggiornamento dell'agente e del proxy senza agente di Windows, consultare la sezione Distribuzione dell'agente sui nodi.
   - Per ulteriori informazioni sull'aggiornamento del server di backup Linux, consultare la sezione Aggiornamento dell'agente Arcserve UDP (Linux).

7. Per il sito Cliente, aggiornare il precedente server di monitoraggio di Virtual Standby o di ripristino del computer virtuale istantaneo ad Arcserve UDP 8.0.

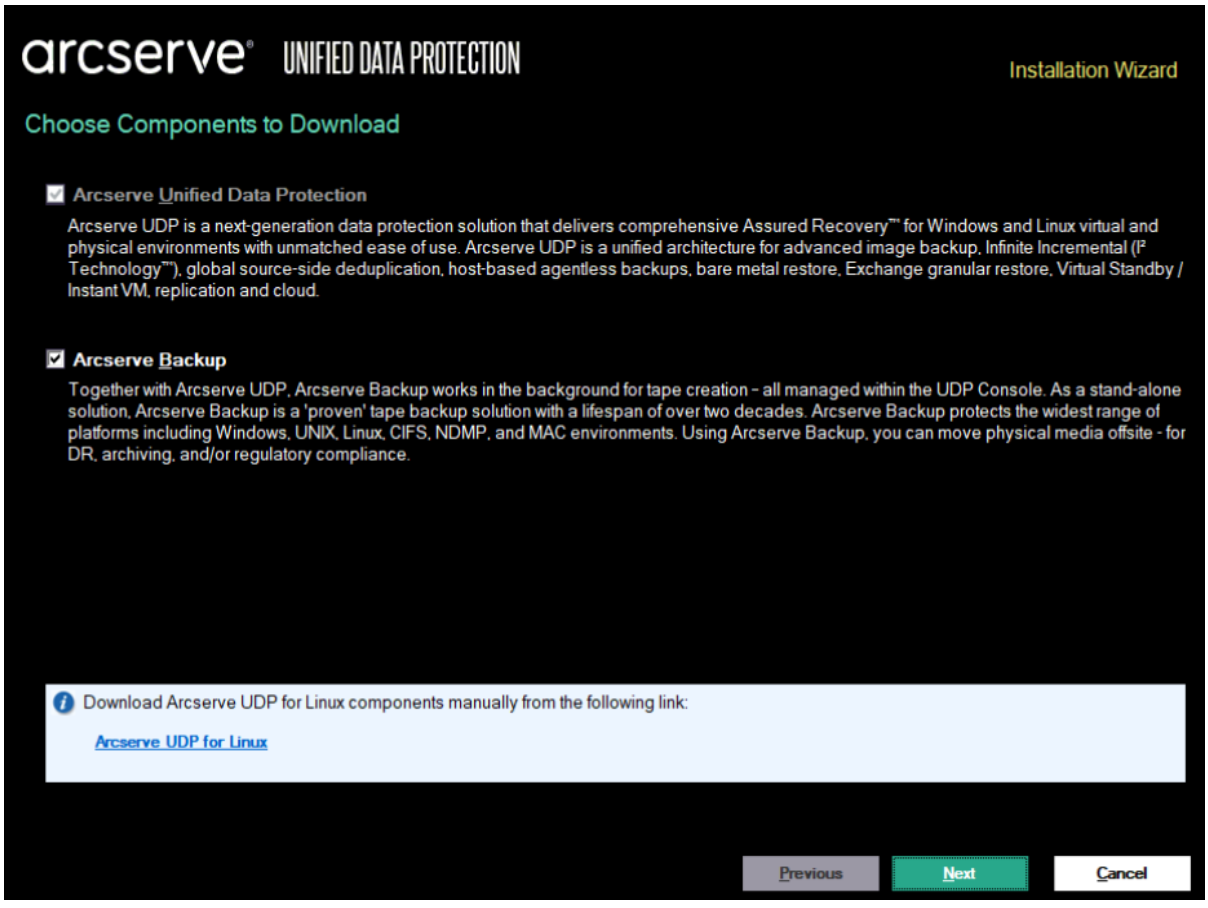
   Nota: per ulteriori informazioni sull'aggiornamento del computer di monitoraggio di Virtual Standby, consultare la sezione Installazione di Arcserve Unified Data Protection mediante la procedura guidata di installazione o Installazione di Arcserve UDP mediante il programma di installazione unificato.

Aggiornamento ad Arcserve UDP 8.0 mediante il programma di installazione unificato

È possibile eseguire l'aggiornamento ad Arcserve UDP versione 8.0 tramite il programma di installazione singolo. Prima di procedere, controllare le versioni supportate.

Effettuare le operazioni seguenti:

1. Scaricare il file ASDownloader.exe dal collegamento di download di Arcserve.
2. Eseguire ASDownloader.exe, accettare il contratto di licenza, quindi fare clic su **Avanti**.
3. Nella **schermata introduttiva** fare clic su **Avanti**.
4. Nella schermata **Choose Components to Download**, selezionare i componenti che si desidera scaricare.



Considerazioni per la selezione dei componenti:

- Per aggiornare la versione precedente di Arcserve UDP, selezionare l'opzione **Arcserve Unified Data Protection**.
- Per aggiornare la versione precedente di Arcserve Backup, selezionare l'opzione **Arcserve Backup**.

Nota: quando si sceglie l'opzione **Arcserve Backup**, alcuni componenti vengono selezionati automaticamente in base alla dipendenza. Se non si desidera installare i componenti sullo stesso computer, consultare la sezione Aggiornamento ad Arcserve UDP 8.0 da una release precedente e utilizzare la procedura guidata di installazione per aggiornare soltanto i componenti esistenti. Da qui è possibile anche scaricare l'installazione di Linux più recente per Arcserve UDP.

5. Dopo aver scaricato i componenti, selezionare il metodo di installazione per aggiornarli.

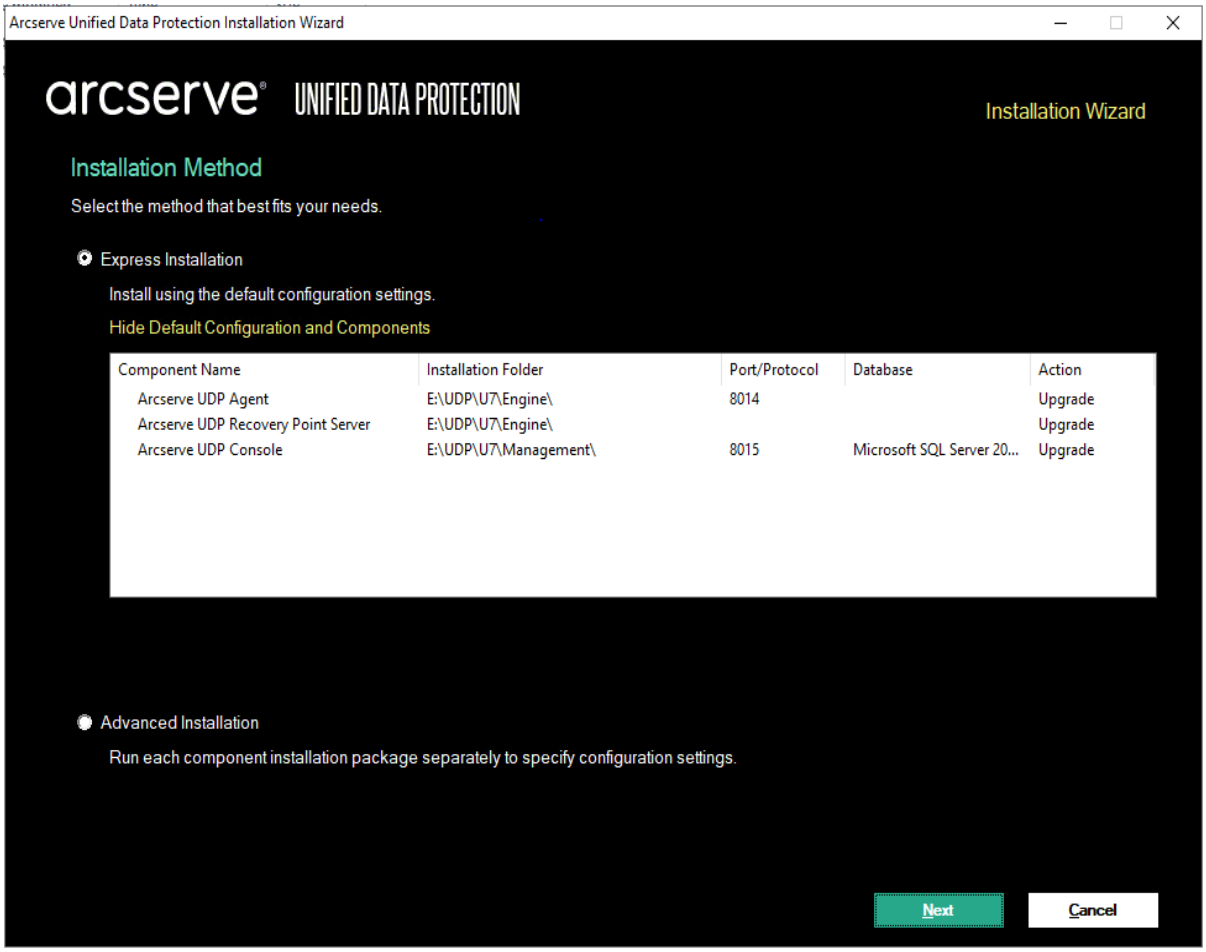
   Installazione rapida

   L'installazione rapida è consigliabile quando si intende installare tutti i componenti con la configurazione predefinita sullo stesso computer.

   Note:

   - verificare tutti i prerequisiti per l'aggiornamento. Ad esempio, .NET 4.5.1 è obbligatorio per Arcserve Backup. Seguire le istruzioni visualizzate nel programma di installazione per soddisfare tutti i prerequisiti.
   - Verificare il requisito della matrice di compatibilità.
   - Il metodo di installazione rapida installa i componenti con le configurazioni predefinite, ad esempio relative a percorso, protocollo, porta e database. Quando si esegue l'aggiornamento utilizzando il metodo di installazione

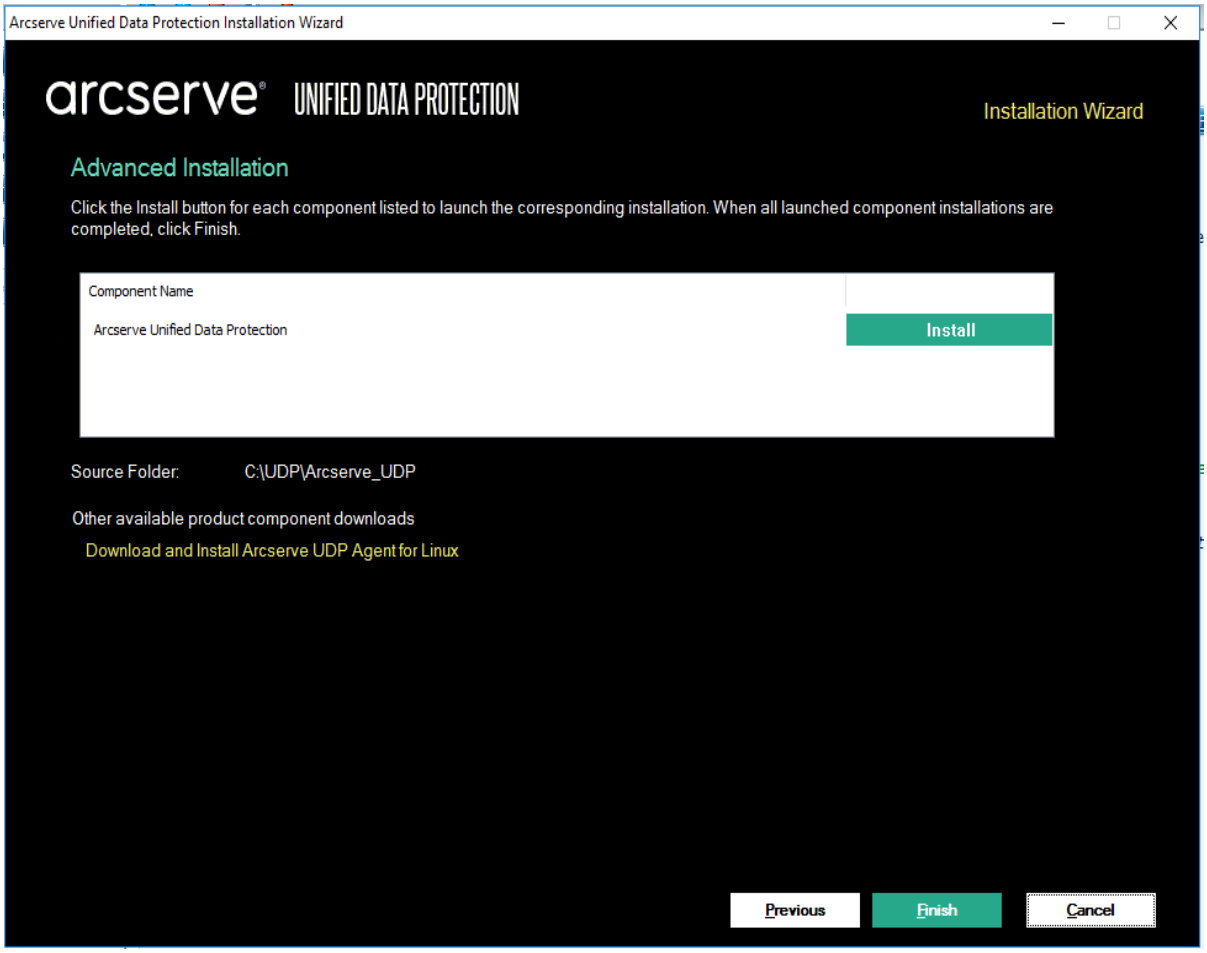
rapida, viene utilizzata la configurazione della versione precedente.



Installazione avanzata

Si consiglia l'Installazione avanzata per l'installazione o l'aggiornamento di ogni componente separatamente nello stesso computer. Fare clic su **Installa** per aggiornare o installare ciascun componente separatamente.

Nota: Per aggiornare l'Agente Arcserve Unified Data Protection per Linux mediante il programma di installazione unificato, scaricare le immagini facendo riferimento ai collegamenti condivisi alla fine del programma di installazione. Dopo aver copiato le immagini nel server di backup Linux, procedere come indicato nella sezione *Aggiornamento dell'agente Arcserve UDP (Linux)* nella Guida in linea dell'agente per Linux.



Arcserve UDP viene aggiornato utilizzando il programma di installazione unificata.

Nota: Per ulteriori informazioni, consultare la sezione Aggiornamento ad Arcserve UDP 8.0 da una release precedente.

Aggiornamento ad Arcserve UDP 8.0 o Arcserve Backup 18.0 per abilitare la copia su nastro

Questa sezione fornisce informazioni sull'aggiornamento ad Arcserve UDP o Arcserve Backup 18.0 dalle versioni precedenti di Arcserve UDP o Arcserve Backup per abilitare la copia su nastro. Arcserve UDP versione 8.0 integra Arcserve Backup 18.0 e fornisce la funzionalità di copia dei dati di backup in supporti nastro di destinazione. È possibile modificare un piano esistente o crearne uno con l'attività **Copia su nastro** della Console Arcserve UDP.

Considerazioni per l'aggiornamento

- Per garantire la corretta esecuzione del piano esistente con l'attività Copia su nastro, aggiornare Arcserve Backup alla versione 18.0 prima di aggiornare Arcserve UDP alla versione 8.0.
- Verificare i requisiti hardware di Arcserve UDP versione 8.0. Per ulteriori informazioni sui requisiti hardware, consultare la sezione *Informazioni sul sistema* nelle *Note di rilascio 8.0*.
- È necessario utilizzare piattaforme, hypervisor, sistemi operativi o versioni dell'applicazione supportati da Arcserve UDP versione 8.0. Per ulteriori informazioni, consultare la matrice di compatibilità.
- Prima di aggiornare UDP 6.5.3 o una versione supportata precedente, non sospendere un piano esistente. Se il piano viene sospeso prima dell'aggiornamento, può essere ripreso solo dopo aver aggiornato tutti i relativi server RPS.
- Acquistare il codice Product Key per Arcserve UDP versione 8.0 e tenerlo a disposizione.
- Rimuovere la versione precedente dell'utilità standalone Arcserve Exchange Granular Restore (AEGR) per Arcserve UDP versione 5.0. Se viene rilevata, nella procedura di installazione guidata verrà richiesto di rimuoverla.
- In generale, i piani precedenti dovrebbero funzionare correttamente in ogni fase di aggiornamento descritta.

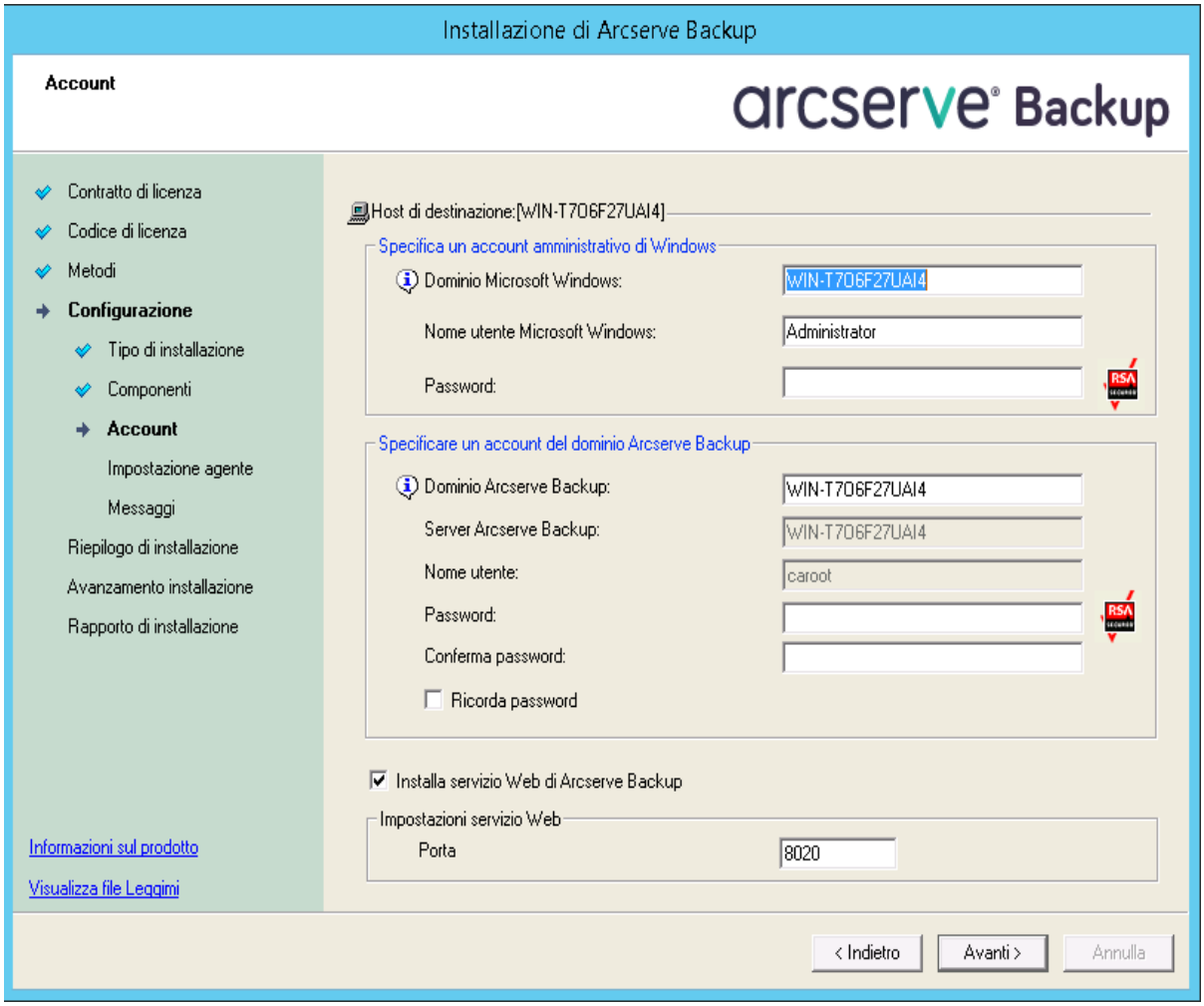
Considerazioni per la copia su nastro

- Installare il server Arcserve Backup 18.0 o aggiornarlo da qualsiasi percorso di aggiornamento supportato in precedenza. È necessario disporre di Arcserve Backup prima di configurare l'attività **Copia su nastro** in un piano di Arcserve UDP.

- Verificare se il requisito Arcserve Backup 18.0 viene rispettato. Per ulteriori informazioni, consultare la matrice di compatibilità.
- Acquistare il codice Product Key per Arcserve Backup 18.0 e tenerlo a disposizione.

Per eseguire l'aggiornamento e abilitare la funzionalità di copia su nastro, procedere come segue:

1. Eseguire l'aggiornamento ad Arcserve Backup 18.0 da una release precedente o installare Arcserve Backup 18.0 con l'opzione **Installa servizio Web Arcserve Backup** abilitata.



Nota: per ulteriori informazioni sull'installazione e sull'aggiornamento di Arcserve Backup, consultare la *Guida all'implementazione di Arcserve Backup 18.0*.

Dopo il completamento dell'aggiornamento, eseguire le operazioni seguenti:

- Verificare se il modulo processo è avviato in Gestione Arcserve Backup.
- Nella console dei servizi Windows, verificare che il **servizio Web di Arcserve Backup** sia in esecuzione.

2. Eseguire l'aggiornamento ad Arcserve UDP versione 8.0 da una release precedente.

   Nota: per ulteriori informazioni su come eseguire l'aggiornamento da una release precedente, consultare la sezione Aggiornamento ad Arcserve UDP 8.0 da una release precedente.

3. Configurare l'attività **Copia su nastro** nella console di Arcserve UDP per un piano nuovo o esistente.

   Nota: Per ulteriori informazioni sulla configurazione dell'attività di copia su nastro, consultare la sezione Creazione di un piano di copia su nastro.

   Il piano dovrebbe funzionare in ogni fase.

Migrazione della console Arcserve UDP da un server a un altro

Per ulteriori informazioni, fare clic sul seguente collegamento.

Aggiornamento del gateway alla stessa versione della console registrata

Il gateway Arcserve UDP deve presentare la stessa versione della relativa console registrata. Dopo aver aggiornato la console Arcserve UDP, all'avvio del servizio viene verificata la versione del gateway associato. Se non corrisponde a quella della console, Arcserve UDP attiva l'aggiornamento automatico per i server gateway.

Se il gateway non è disponibile per l'aggiornamento automatico, è possibile aggiornarlo manualmente in seguito.

Per aggiornare il gateway, attenersi alla procedura seguente:

1. Accedere alla console Arcserve UDP.
2. Fare clic sulla scheda **risorse**, accedere a **Infrastruttura**, quindi fare clic su **Siti**.
3. Selezionare il sito che si desidera aggiornare.
4. Dall'elenco a discesa **Azioni**, fare clic su **Aggiorna gateway**.

   Viene visualizzata una finestra di dialogo di conferma.
5. Fare clic su **Sì**.

   Il gateway viene aggiornato alla versione più recente di Arcserve UDP.

Migrazione della Console Arcserve UDP

È possibile eseguire la migrazione di una Console Arcserve UDP a un'altra Console Arcserve UDPmediante *ConsoleMigration.exe*. A partire da Arcserve UDP v6.5 Aggiornamento 2, è possibile eseguire la migrazione della Console Arcserve UDP tra due Console Arcserve UDP qualsiasi.

Utilizzare *ConsoleMigration.exe* per BackupDB e RecoverDB. Nella schermata che segue viene visualizzato l'utilizzo di *ConsoleMigration.exe*:



Per completare il processo di migrazione, attenersi alla seguente procedura:

1. Sulla Console Arcserve UDP precedente, eseguire il backup del database Arcserve UDP

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe
-BackupDB

Backed up DB and version files completed.

DB and version files were created at "C:\Program Files\Arcserve\Unified Data
Protection\Management\BIN\Appliance\DB_Migration".
```

La cartella *DB_Migration* è stata creata correttamente.

2. Sulla nuova Console Arcserve UDP, copiare la cartella *DB_Migration* nel seguente percorso:

   <UDP_Home> *Management**BIN**Appliance*\

3. Nella nuova Console Arcserve UDP, procedere come indicato nella schermata riportata di seguito per ripristinare il database della ConsoleArcserve UDP

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe
-RecoverDB

Are you sure you want to recover the backup DB file? (y/n): y

Stopping Arcserve UDP management service, please wait...

Recovering backup DB file...

Updating nodes, please wait...

Please update nodes manually from UDP console, if you still encounter disconnected nodes.

The disconnected nodes(if exist) will be saved at "C:\Program Files\Arcserve\Unified Data Protec
tion\Management\BIN\Appliance\DB_Migration\logs".

Console migration completed. Console use DB "localhost\ARCSERVE_APP".
```

Nota: Arcserve UDP nella console , se esiste un sito diverso dal sito locale, attenersi alla procedura menzionata nel file *NewRegistrationText.txt* per registrare il sito nuovamente.

La migrazione della Console Arcserve UDP è stata completata correttamente sulla nuova Console Arcserve UDP.

È possibile utilizzare questo strumento per eseguire la migrazione della Console Arcserve UDP connessa al database SQL remoto. Al termine della migrazione, la Console Arcserve UDP di cui è stata eseguita la migrazione viene configurata per la connessione allo stesso database SQL remoto.

Nota: in UDP v6.5 Aggiornamento 2 e Aggiornamento 3, se si utilizza lo strumento di migrazione della Console per eseguire la migrazione tra due Console Arcserve UDP, entrambe le versioni della Console di Arcserve UDP e del database SQL dovranno corrispondere sui due sistemi della Console Arcserve UDP. In caso

contrario, la migrazione della Console produce un errore e viene visualizzato il messaggio di errore corrispondente nella riga di comando e nei file di registro nel seguente percorso:

<UDP_Home> \Management\BIN\Appliance\logs

In Arcserve UDP v6.5 Aggiornamento 4, l'opzione ***-force*** è stata introdotta nel comando ***ConsoleMigration.exe*** per imporre la migrazione del file di database di backup sulla console di destinazione nel caso in cui si verifichino le seguenti condizioni:

1. Quando si desidera eseguire la migrazione della Console tra due console in cui la console di origine utilizza SQL Server Enterprise Edition e quella di destinazione utilizza SQL Server Express Edition. In questo caso, le dimensioni minime richieste per il database della Console UDP di origine corrispondono a 4000 MB.
2. Quando si desidera eseguire la migrazione della Console da una console che utilizza una versione avanzata del database SQL Server a una console che utilizza una versione precedente del database SQL Server. Ad esempio, la migrazione da una console con SQL Server 2016 alla console con SQL Server 2014.

Chapter 5: Esplorazione e configurazione di Arcserve UDP

La presente sezione descrive i seguenti argomenti:

Accesso alla console Arcserve UDP mediante l'autenticazione a più fattori

Arcserve UDP supporta l'autenticazione a più fattori (MFA) che fornisce un ulteriore livello di protezione per tutti gli utenti. L'MFA è un processo di accesso in cui all'utente viene richiesto di fornire un'ulteriore forma di identificazione. Questo metodo di autenticazione richiede più di un fattore per la verifica dell'identità dell'utente. In generale, il processo di accesso a MFA utilizza l'autenticazione a due fattori, la quale consente due fattori per l'identificazione dell'utente.

Arcserve UDP supporta l'autenticazione a due fattori. Consente l'autenticazione con nome utente e password come primo fattore. L'autenticazione del secondo fattore utilizza uno dei seguenti elementi:

- **TOTP (time-based one-time passcode)**: a differenza della tradizionale OTP inviata a un indirizzo di posta elettronica o SMS, un TOTP viene generato mediante un'app di autenticazione. Il TOTP è valido per un breve periodo di tempo e viene aggiornato ogni 30 secondi.
- **Posta elettronica OTP**: questa funzionalità esegue l'autenticazione con una OTP inviata all'indirizzo di posta elettronica registrato e la OTP è valida per 30 secondi. Viene abilitata solo dopo aver configurato l'indirizzo di posta elettronica.

La presente sezione descrive i seguenti argomenti:

Verifica dei prerequisiti

Tenere presente i seguenti prerequisiti:

- È necessario abilitare l'autenticazione a più fattori (MFA) per tutti gli utenti. Per ulteriori informazioni sull'attivazione dell'autenticazione a più fattori, consultare la sezione Configurazione dell'autenticazione a più fattori come utente amministratore.

  Nota: solo gli amministratori possono abilitare l'autenticazione a più fattori (MFA) per tutti gli utenti.

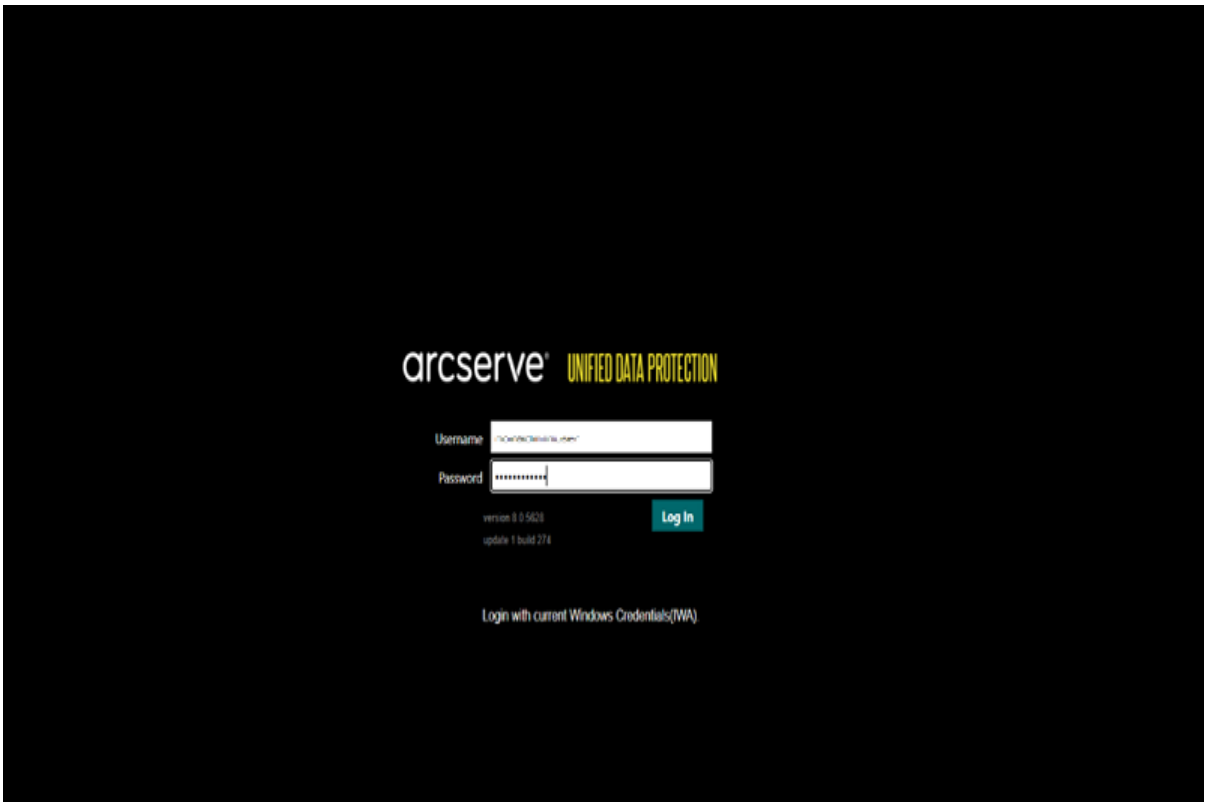
- Installare un'app di autenticazione mobile sul proprio dispositivo mobile. È possibile trovare le app di autenticazione come Google Authenticator o Microsoft Authentication nell'App Store del proprio dispositivo mobile.

Accesso alla console Arcserve UDP mediante MFA

In questa sezione vengono fornite informazioni su come accedere alla console Arcserve UDP mediante MFA.

Effettuare le operazioni seguenti:

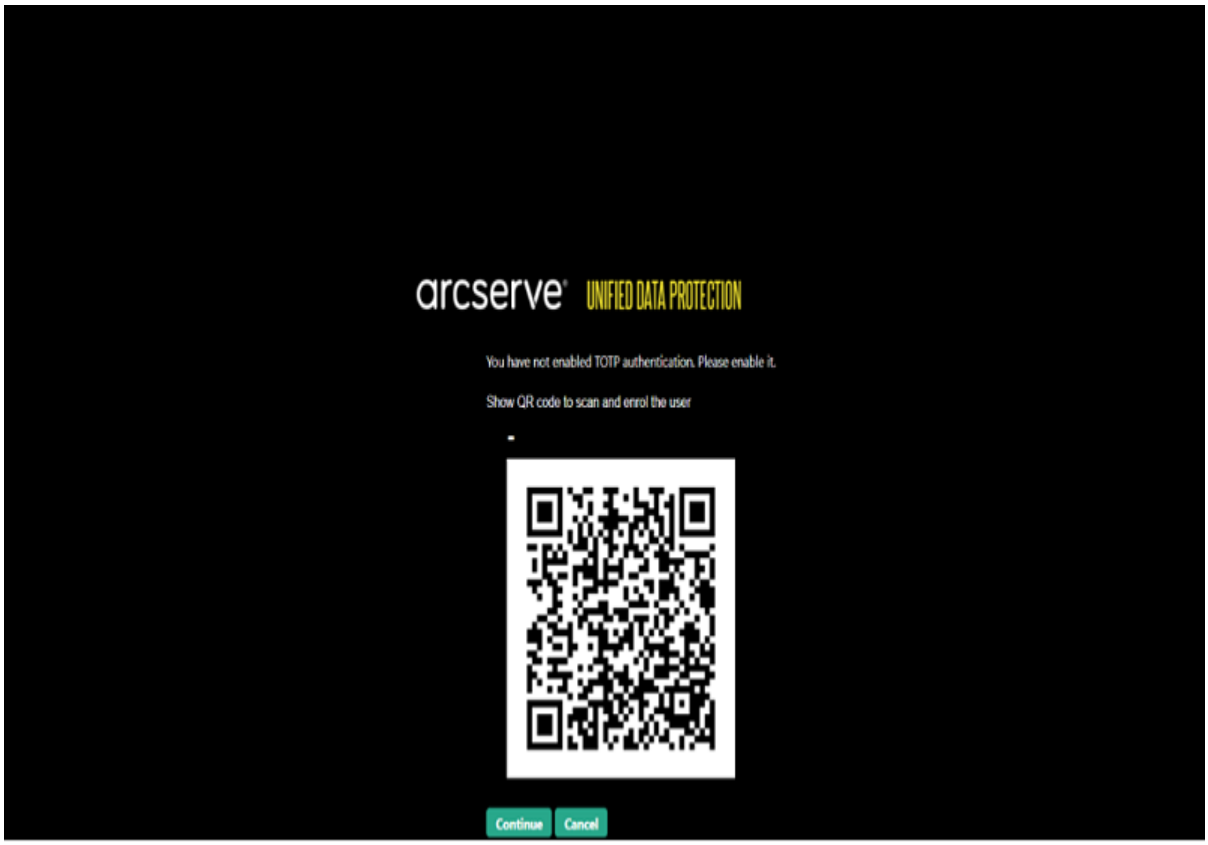
1. Accedere alla pagina di accesso alla console UDP.
2. Digitare il nome utente e la password, quindi fare clic sul pulsante **Accedi**.



Una volta completata correttamente la verifica dell'autenticazione del primo fattore, viene visualizzata la pagina di autenticazione del secondo fattore.

3. Se non è stata abilitata l'autenticazione TOTP, eseguire le seguenti operazioni:
   a. Fare clic sul collegamento **Mostra codice QR per eseguire la scansione e registrare l'utente**.

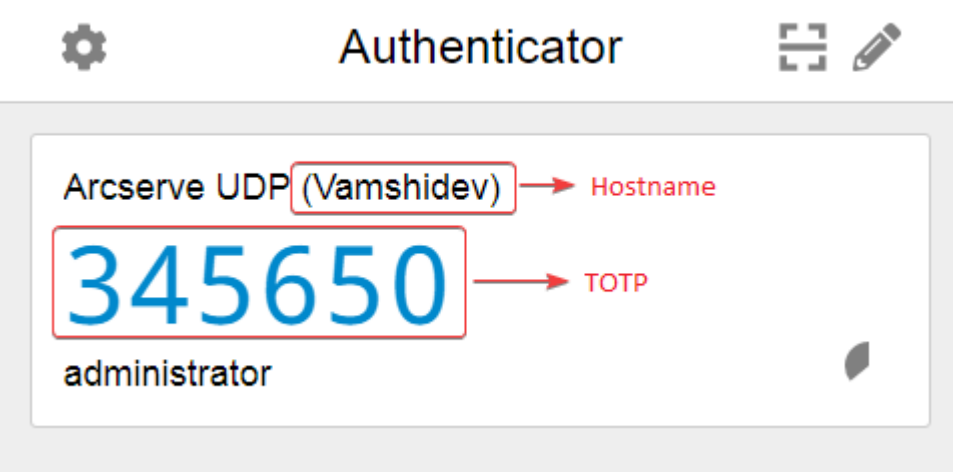
      Viene visualizzata l'immagine del codice QR.



b. Per generare il TOTP, eseguire la scansione dell'immagine del codice QR utilizzando un'app di autenticazione.

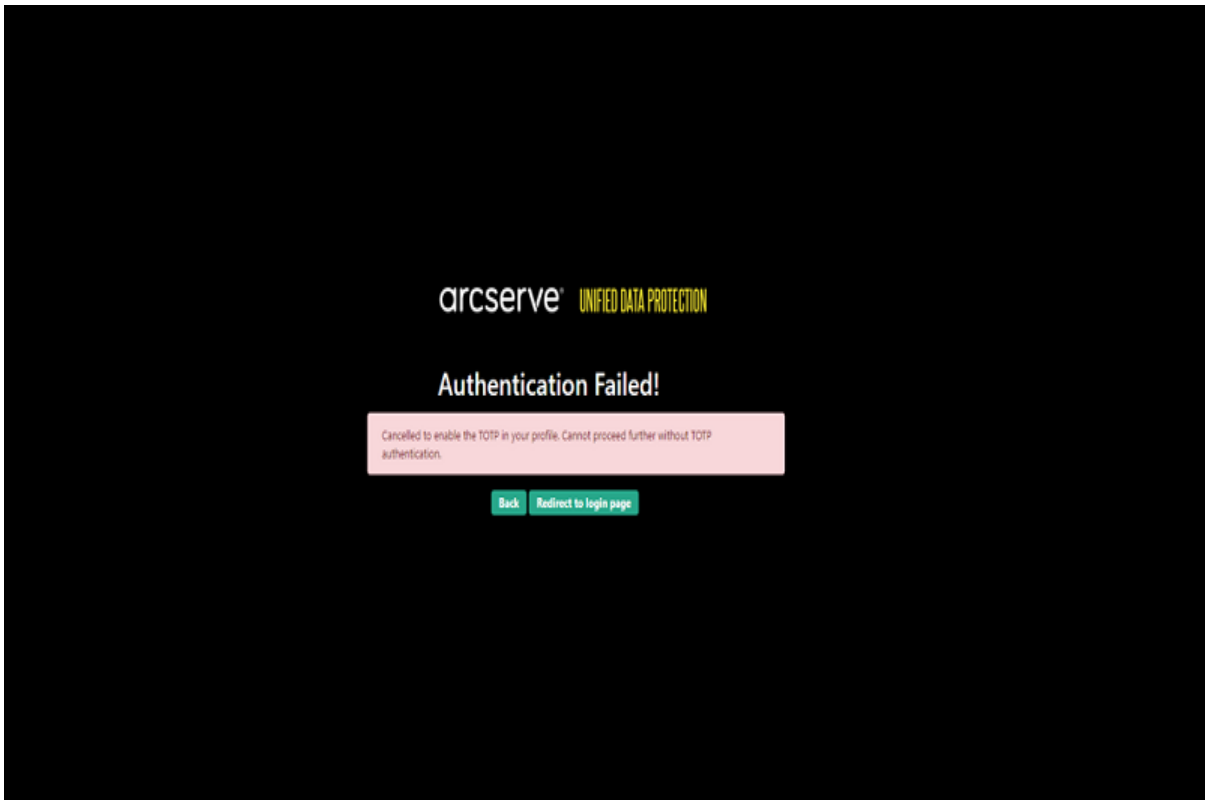
Note:

- È possibile utilizzare qualsiasi app di autenticazione mobile, ad esempio l'app Google Authenticator o l'app Microsoft Authenticator sul proprio dispositivo mobile. In alternativa, è possibile utilizzare anche l'estensione Authenticator per il browser Chrome.
- Quando si utilizza un'app di autenticazione per più account utente, il nome host dell'account utente distingue i TOTP. Nell'app di autenticazione è possibile visualizzare il nome host e il rispettivo TOTP.



c. Fare clic sul pulsante **Continua**.

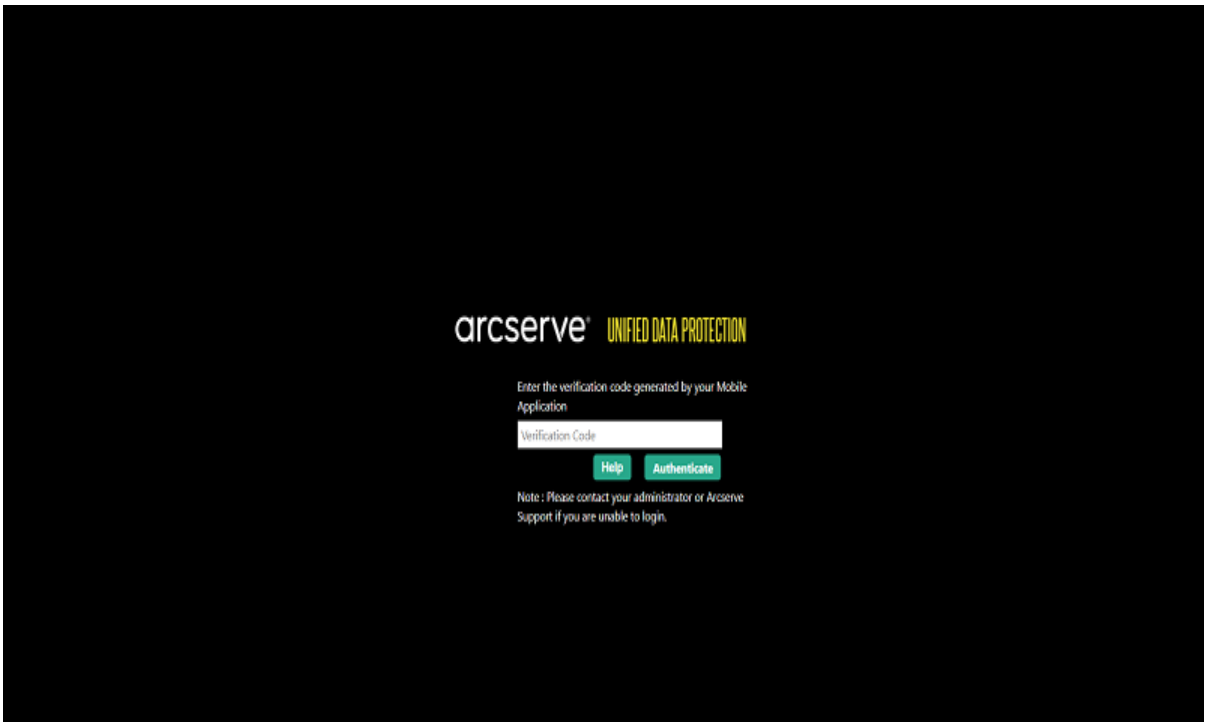
Se si fa clic sul pulsante **Annulla**, l'autenticazione non riesce.



Nota: se in precedenza è stato abilitato il fattore di autenticazione TOTP, non viene richiesto di eseguire il passaggio 3.

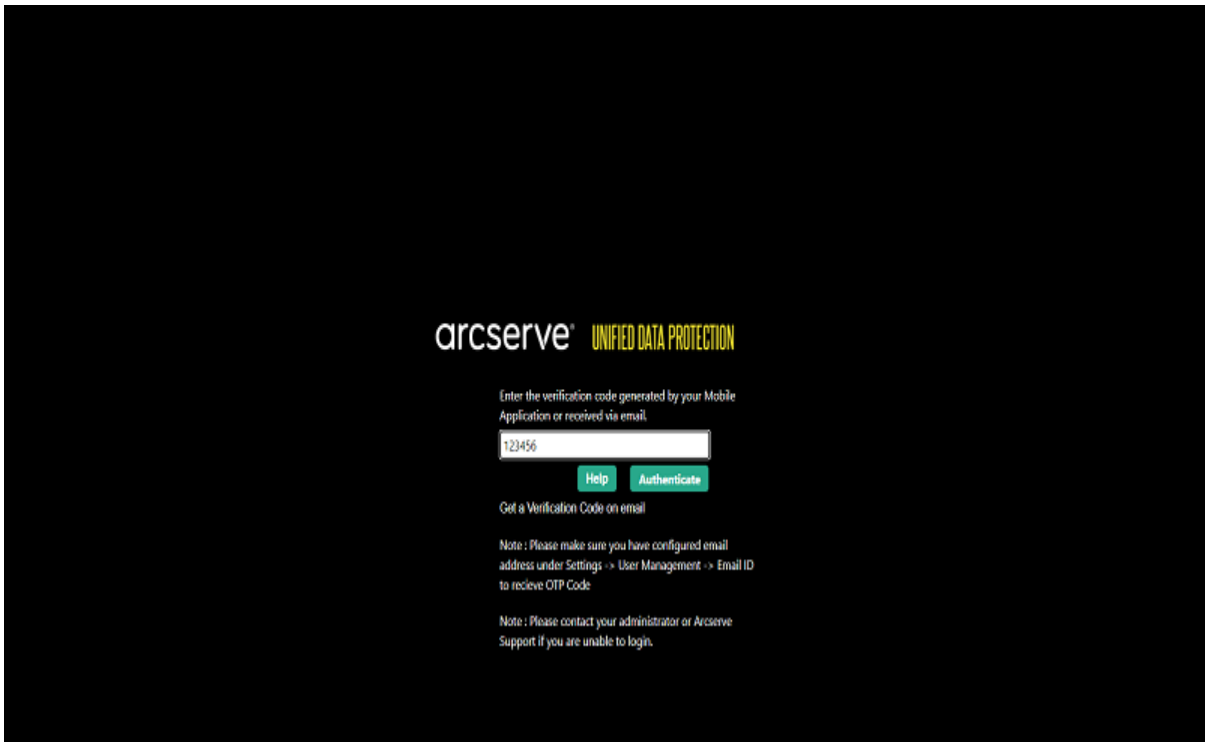
4. Nel campo Codice di verifica, digitare il TOTP.

Per TOTP, aprire l'app di autenticazione per dispositivi mobili sul proprio dispositivo mobile o l'estensione di autenticazione sul browser Chrome. Il numero è valido per 30 secondi e viene aggiornato ogni 30 secondi.



5. (Facoltativo) Se non si dispone di un TOTP, procedere come segue:
   a. Fare clic sul collegamento **Ottieni un codice di verifica tramite posta elettronica**.

      Il messaggio di posta elettronica OTP temporaneo viene inviato al proprio indirizzo di posta elettronica.



Note:

- L'opzione OTP di posta elettronica è accessibile solo quando un utente amministratore abilita la funzionalità OTP di posta elettronica e configura le impostazioni di posta elettronica. Per ulteriori informazioni, consultare la sezione Configurazione dell'autenticazione a più fattori come utente amministratore.
- Assicurarsi di configurare l'indirizzo di posta elettronica in *Impostazioni* > *Gestione utente* per ricevere l'OTP di posta elettronica.

b. Nel campo del codice di verifica, immettere l'OTP di posta elettronica.

6. Fare clic sul pulsante **Esegui autenticazione**.

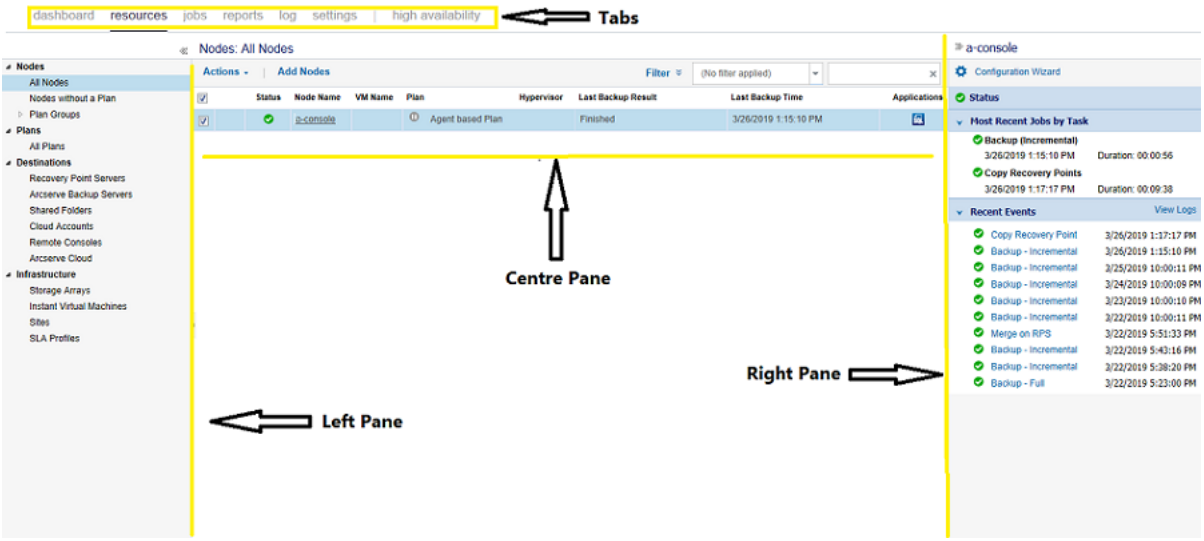
   L'accesso alla console UDP è stato eseguito correttamente.

Arcserve Unified Data Protection Interfaccia utente

Prima di utilizzare Arcserve Unified Data Protection, è opportuno acquisire familiarità con l'interfaccia utente. L'interfaccia di Arcserve Unified Data Protection consente di completare le seguenti attività:

- Gestione e monitoraggio dei processi
- Aggiunta e gestione dei nodi di origine
- Aggiunta e gestione dei Recovery Point Server di destinazione
- Gestione dei piani per la creazione di pianificazioni di backup
- Ottenimento di statistiche sulla protezione dei dati
- Visualizzazione di registri di errori e di avvisi
- Gestione e monitoraggio di Arcserve High Availability
- Configurazione delle impostazioni di protezione dei dati
- Ripristino dei dati di backup

Accesso ad Arcserve UDP



Schede

Consente di accedere alle varie funzioni di Arcserve Unified Data Protection.

Riquadri

Quando si accede a ogni scheda, la schermata visualizzata viene divisa nei riquadri seguenti. Ogni riquadro viene utilizzato per eseguire le relative azioni.

Riquadro sinistro

Consente di accedere a varie funzioni e operazioni. Il risultato di ciascun clic viene mostrato nel riquadro centrale.

Riquadro centrale

Consente di eseguire la maggior parte delle azioni, come ad esempio aggiunta, eliminazione e modifica. Questo riquadro mostra inoltre il risultato e lo stato di ogni attività quali processi, piani e rapporti. La maggior parte delle azioni vengono eseguite in questo riquadro. Le informazioni mostrate in questa pagina sono principalmente il risultato delle opzioni selezionate nel riquadro sinistro.

Riquadro destro

Mostra un riepilogo degli elementi selezionati nel riquadro centrale. Ad esempio, nella scheda Jobs (Processi), se un processo è stato selezionato dal riquadro centrale, nel riquadro destro vengono visualizzati un breve riepilogo del processo come monitoraggio del processo (se è presente un processo in esecuzione) e i dettagli del processo come nome del nodo di origine, attività, Recovery Point Server di destinazione e archivio dati di destinazione.

Schede

La soluzione Arcserve Unified Data Protection presenta le seguenti schede per svolgere le funzioni di protezione dei dati:

- Dashboard
- Risorse
- processi
- rapporti
- registro
- impostazioni
- High Availability

Dashboard

La scheda **Dashboard** consente di visualizzare una rappresentazione grafica dello stato dell'ultima attività e dell'archiviazione dei dati negli ultimi sette giorni. La scheda **Dashboard** consente di eseguire le operazioni seguenti:

- Visualizzare l'ora dell'ultimo aggiornamento. Facendo clic sull'icona *Aggiorna*, vengono visualizzati i dati più recenti nel dashboard.
- Facendo clic sul grafico a barre RTO, viene visualizzata la pagina Rapporti RTO.
- Visualizzare l'ultimo stato di attività dei nodi o dei piani in base ai filtri selezionati nel grafico **Stato ultima attività**.



Nella scheda Dashboard, è possibile visualizzare i grafici delle opzioni seguenti:

Ultimo stato attività

Stato ultima attività fa riferimento allo stato più recente dell'attività e fornisce più filtri per la visualizzazione dello stato. In base alla selezione dall'opzione di filtro, è possibile visualizzare l'ultimo stato dell'attività. Ad esempio, selezionare **Tutti i nodi** per visualizzare lo stato di attività più recente di tutti i nodi, oppure selezionare un piano per visualizzare lo stato di attività più recente dei nodi protetti dal piano. Filtrare ulteriormente per un tipo di attività specifica. Se si seleziona **Tutti i nodi**, è possibile visualizzare lo stato seguente:

- **Completato correttamente** indica che il backup dei nodi è stato eseguito correttamente.

- **Non riuscito** indica che l'ultimo backup non è riuscito.
- **Annullato** indica che l'ultimo backup è stato arrestato.
- **Missed** (Perso) indica che l'ultimo backup non è stato eseguito secondo la pianificazione.
- **Non connesso** indica che Arcserve UDP la console non è riuscita a stabilire la connessione con il nodo.
- **Incompleto** indica che il processo di ripristino non è stato completato.

Quando si fa clic su ogni fetta (lo stato) del grafico a torta, si apre la pagina **Risorse** e vengono visualizzati i nodi associati. Ad esempio, se si fa clic su **Operazione riuscita** dal grafico a torta, viene visualizzata la pagina **Risorse**. La pagina **Risorse** visualizza i nodi privi di piano. Inoltre, il filtro **Operazione riuscita** filtro è preselezionato nella pagina **Risorse**.

Dimensione dei dati effettivi, di ripristino e non elaborati: 7 giorni

Il grafico confronta i dati non elaborati, i dati di ripristino e l'archiviazione dati effettiva degli ultimi sette giorni.

Dimensione dei dati di ripristino

Si riferisce alla dimensione dei dati che è possibile ripristinare dai dati archiviati su tutti i sistemi di archiviazione di destinazione in quel giorno. Indipendentemente dal tipo di backup, che può essere completo o incrementale, ogni punto di ripristino viene utilizzato per ripristinare un'origine completa. Questa è la dimensione totale dell'intera origine di ripristino disponibile.

Se ad esempio la dimensione dei dati non elaborati è di 30 GB e, dopo la compressione e la deduplicazione, scende a 22 GB, la dimensione dei dati di ripristino è di 30 GB per il primo backup completo. Per una modifica incrementale di 4 GB, la dimensione dei dati di ripristino è 30 + 34 GB = 64 GB.

Dimensione di archiviazione dei dati effettivi

Si riferisce alla dimensione finale dei dati. Dopo la compressione dei dati non elaborati, la rimozione dei blocchi di dati duplicata dai dati non elaborati e l'aggiunta di alcuni metadati, i dati non elaborati diventano finali e vengono salvati nello spazio di archiviazione di destinazione.

Dimensione dei dati non elaborati

Si riferisce ai dati letti dall'origine e trasferiti nella destinazione.

Rapporto SLA per RTO e RPO

Arcserve UDPIl rapporto Service Level Agreement (SLA) in consente alle aziende di generare rapporti di conformità relativi all'obiettivo del punto di ripristino (Recovery Point Objective, RPO) e all'obiettivo del momento di ripristino (Recovery Time Objective, RTO).

Rapporto RTO

Il rapporto RTO di Arcserve UDP è un rapporto di conformità che visualizza il confronto tra i valori relativi al momento effettivo di ripristino e all'obiettivo del momento di ripristino per tutti i tipi di processo di recupero eseguiti, quali il ripristino di file system, il ripristino di computer virtuali, i computer virtuali istantanei e Assured Recovery. Il grafico a barre utilizza più colori per visualizzare lo stato dei processi. È possibile eseguire un'ulteriore analisi in dettaglio per verificare se lo stato a livello di nodo filtrato per RTO è soddisfatto, non soddisfatto, non verificato o non definito.

Rapporto RPO

Arcserve UDPIl rapporto RPO di mostra il numero totale di nodi con i punti di ripristino disponibili durante il periodo di tempo specificato nella visualizzazione della barra, categorizzato in base alla data dei punti di ripristino più recenti (15 minuti, ultima ora, 12 ore, ultimo giorno e così via), alla data dei punti di ripristino meno recenti (30 giorni e oltre) e alla distribuzione mensile (gennaio - dicembre). È possibile eseguire un'ulteriore analisi in dettaglio per visualizzare lo stato a livello di nodo per la categoria selezionata.

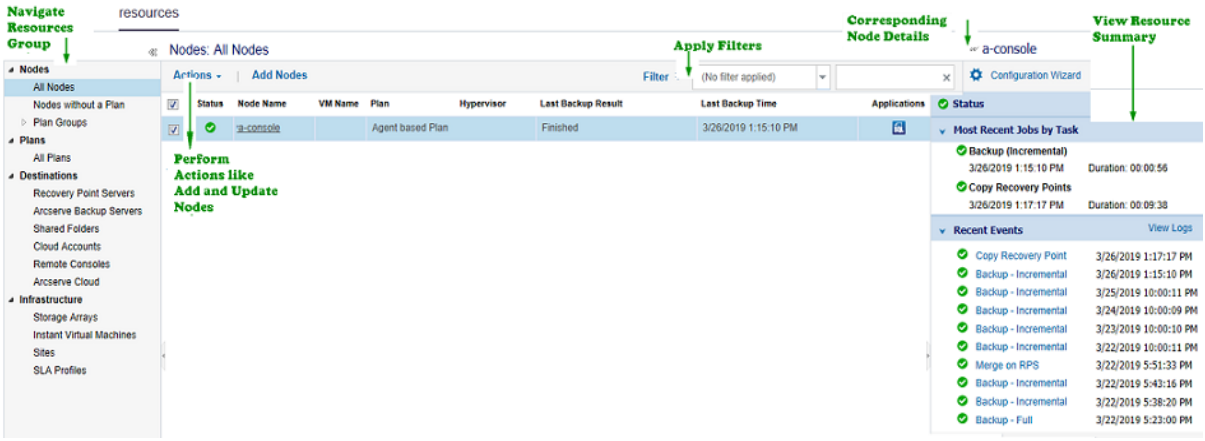
Nota: Dal dashboard, è possibile visualizzare direttamente il rapporto RPO di un mese specifico. Il rapporto viene compilato direttamente dal dashboard Arcserve UDP. Facendo clic nel grafico a barre RPO di un mese nel Dashboard viene visualizzata la schermata del rapporto RPO per il mese specifico nella schermata RPO.

Risorse

La scheda **Risorse** consente di gestire le risorse Arcserve Unified Data Protection: Nodi, Destinazioni, Virtual Standby e Piani. Utilizzare questa scheda per aggiungere risorse a Arcserve Unified Data Protection, quali i nodi da proteggere o i Recovery Point Server per il backup. Utilizzare questa scheda anche per creare piani e attività per il backup, Virtual Standby e la replica. La scheda Risorse consente di svolgere le operazioni seguenti:

- Gestione nodi
- Gestione della destinazione
- Gestione piano
- Gestione infrastruttura

Nota: soltanto la scheda **Risorse** della console effettua il riconoscimento dei siti. Le altre schede della console visualizzano i dati consolidati per tutti i siti. Per ulteriori informazioni sui siti, consultare la sezione Aggiunta e gestione di un sito.



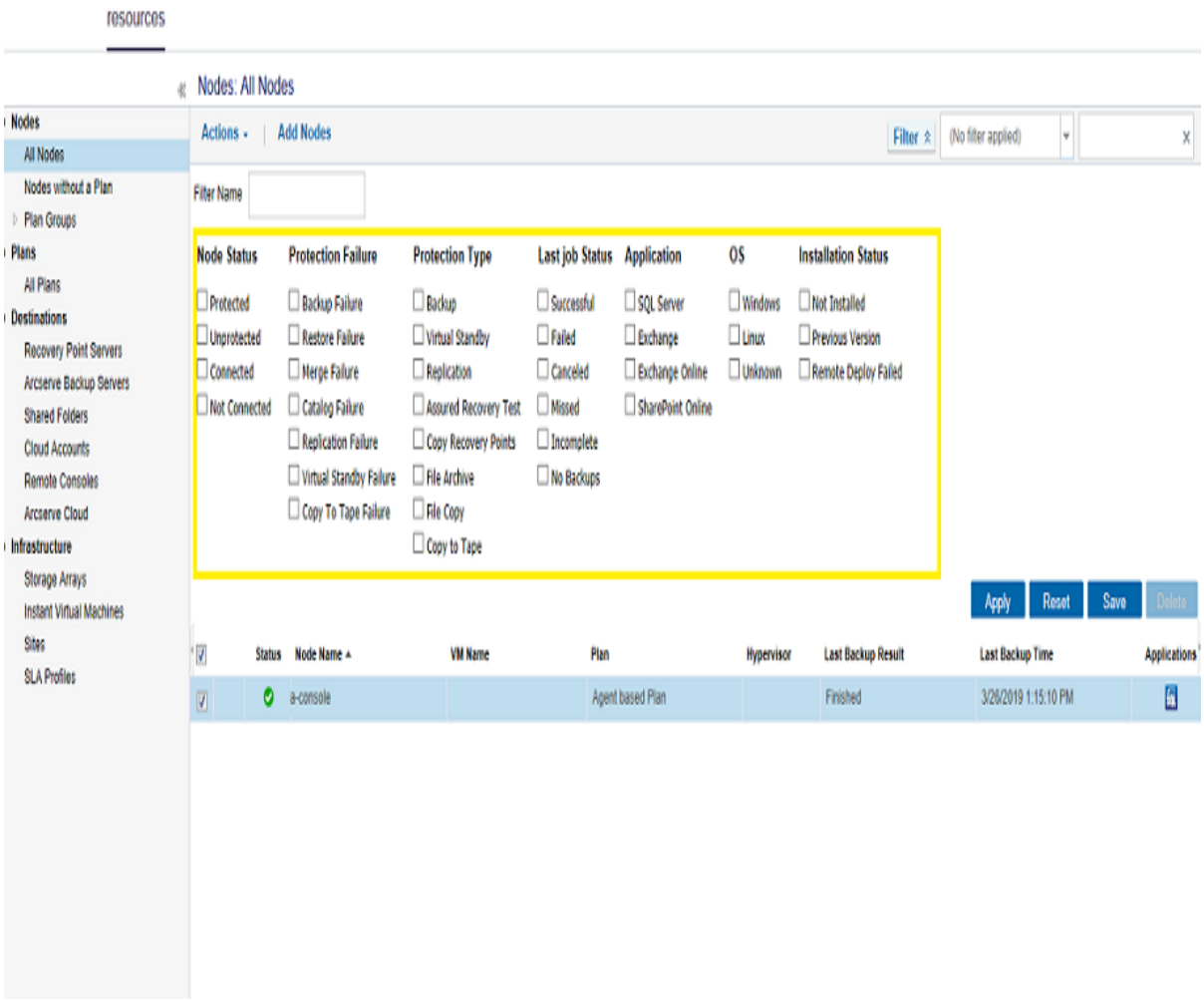
Gestione nodi

La vista Gestione nodi consente di gestire tutti i nodi e applicare filtri per affinare la ricerca del nodo. Quando si seleziona nodo specifico nel riquadro centrale, è possibile visualizzato lo stato e gli eventi recenti vicino al nodo nel riquadro destro. È possibile applicare vari filtri dal riquadro centrale. È possibile creare gruppi di nodi nel riquadro sinistro per raggruppare nodi specifici.

Quando si seleziona un nodo dal riquadro centrale, lo stato del nodo e gli eventi recenti vengono visualizzati nel riquadro destro.

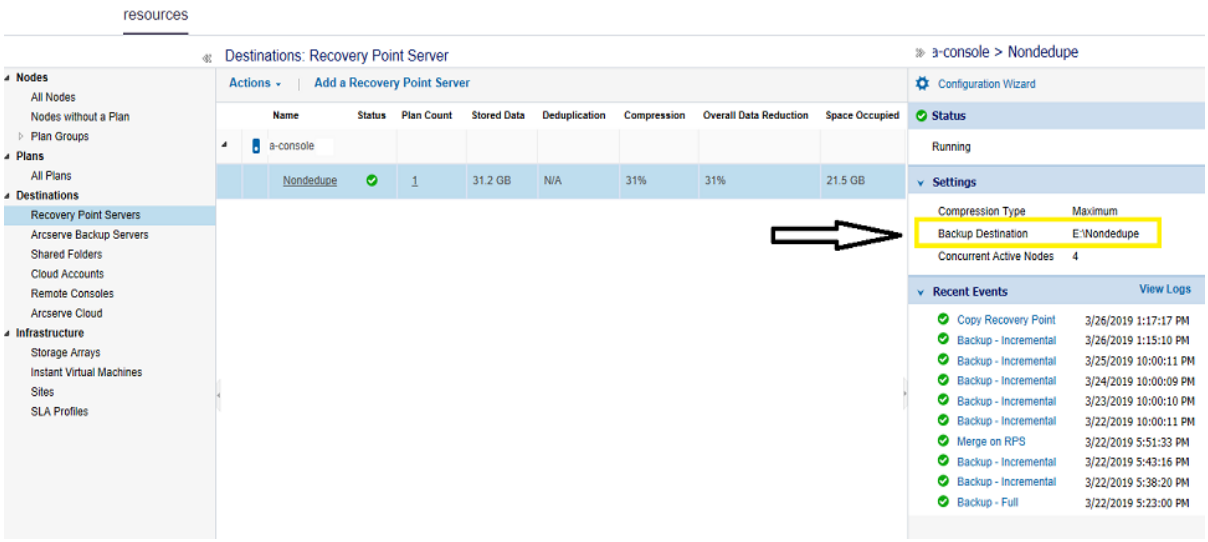
È possibile eseguire delle operazioni sui nodi facendo clic sul menu a discesa Azioni dal riquadro centrale. Le operazioni eseguibili attraverso Azioni nel riquadro centrale vengono applicate a tutti i nodi di origine. Tali operazioni che è possibile eseguire tramite Azioni nel riquadro destro vengono applicate solo al nodo selezionato nel riquadro centrale.

Dalla scheda Risorse, in Nodo fare clic su **Tutti i nodi** nel riquadro a sinistra. Quindi, dal riquadro centrale, selezionare un nodo e fare clic su **Filtro** per visualizzare le opzioni di gestione dei nodi. È possibile selezionare le caselle di controllo per le opzioni desiderate e fare clic su **Applica**.


resources
Nodes: All Nodes
Nodes
All Nodes
Nodes without a Plan
Plan Groups
Plans
All Plans
Destinations
Recovery Point Servers
Arcserve Backup Servers
Shared Folders
Cloud Accounts
Remote Consoles
Arcserve Cloud
Infrastructure
Storage Arrays
Instant Virtual Machines
Sites
SLA Profiles
Actions
Add Nodes
Filter
(No filter applied)
Filter Name
Node Status
Protected
Unprotected
Connected
Not Connected
Protection Failure
Backup Failure
Restore Failure
Merge Failure
Catalog Failure
Replication Failure
Virtual Standby Failure
Copy To Tape Failure
Protection Type
Backup
Virtual Standby
Replication
Assured Recovery Test
Copy Recovery Points
File Archive
File Copy
Copy to Tape
Last job Status
Successful
Failed
Canceled
Missed
Incomplete
No Backups
Application
SQL Server
Exchange
Exchange Online
SharePoint Online
OS
Windows
Linux
Unknown
Installation Status
Not Installed
Previous Version
Remote Deploy Failed
Apply
Reset
Save
Delete
Status
Node Name
VM Name
Plan
Hypervisor
Last Backup Result
Last Backup Time
Applications
a-console
Agent based Plan
Finished
3/26/2019 1:15:10 PM

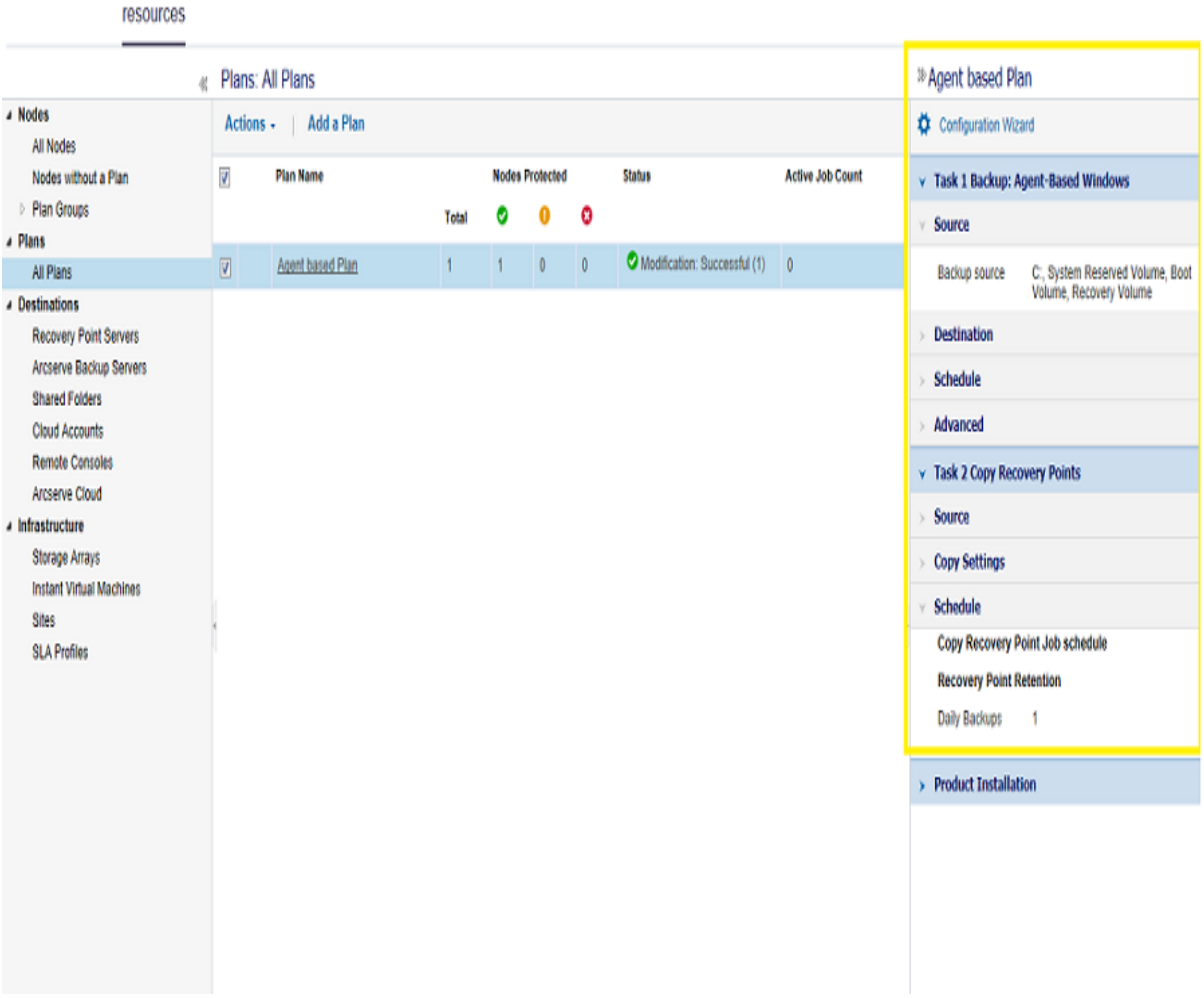
Gestione della destinazione

La vista Gestione della destinazione consente di gestire i Recovery Point Server di destinazione. Quando si seleziona un server dal riquadro centrale, i relativi eventi recenti vengono visualizzati nel riquadro destro. Quando si seleziona un archivio dati, lo stato e le relative impostazioni vengono visualizzate nel riquadro destro.



Gestione piano

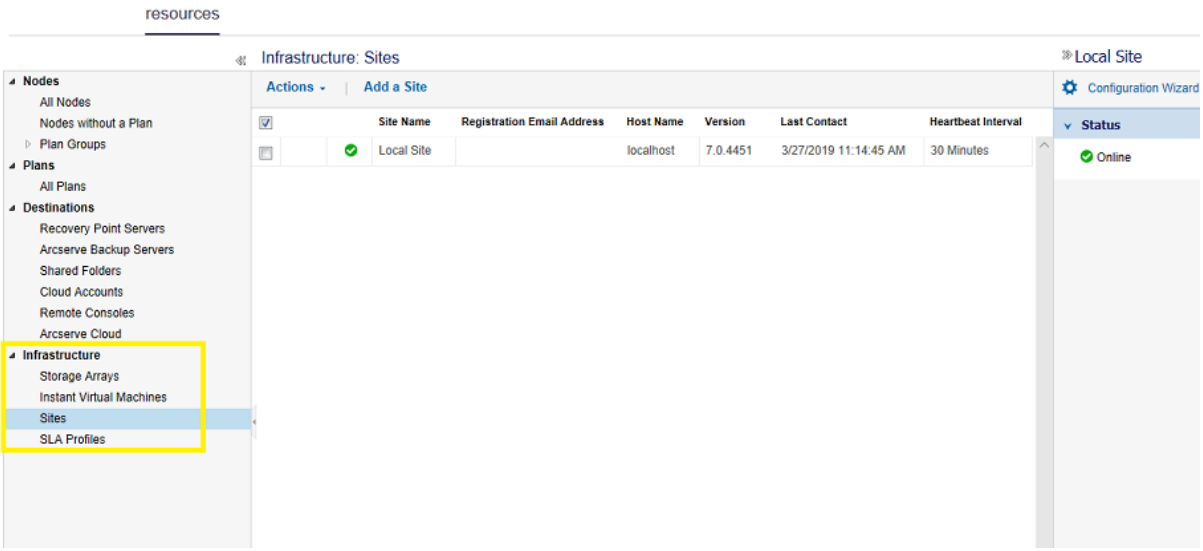
La vista Gestione piano consente di gestire tutti i piani. Da questa visualizzazione è possibile creare, modificare, eliminare, distribuire, interrompere e riprendere i piani. I dettagli del piano vengono visualizzati nel riquadro destro. È possibile fare clic sui campi necessari per visualizzare e gestire i dettagli.



Gestione infrastruttura

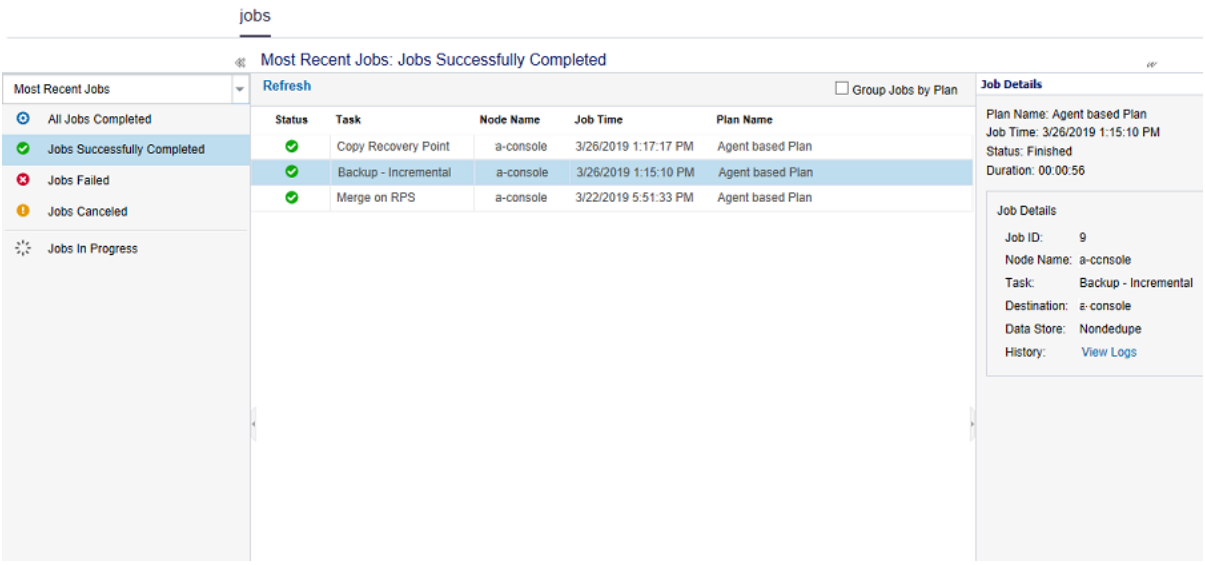
La visualizzazione della gestione dell'infrastruttura consente di gestire gli array di archiviazione, i computer virtuali istantanei e i siti remoti.

La schermata che segue evidenzia il riquadro di gestione dell'infrastruttura:



processi

La scheda **Jobs** (Processi) mostra lo stato dei processi per un periodo specifico. Applicare filtri per classificare i risultati o raggruppare i processi per piano.

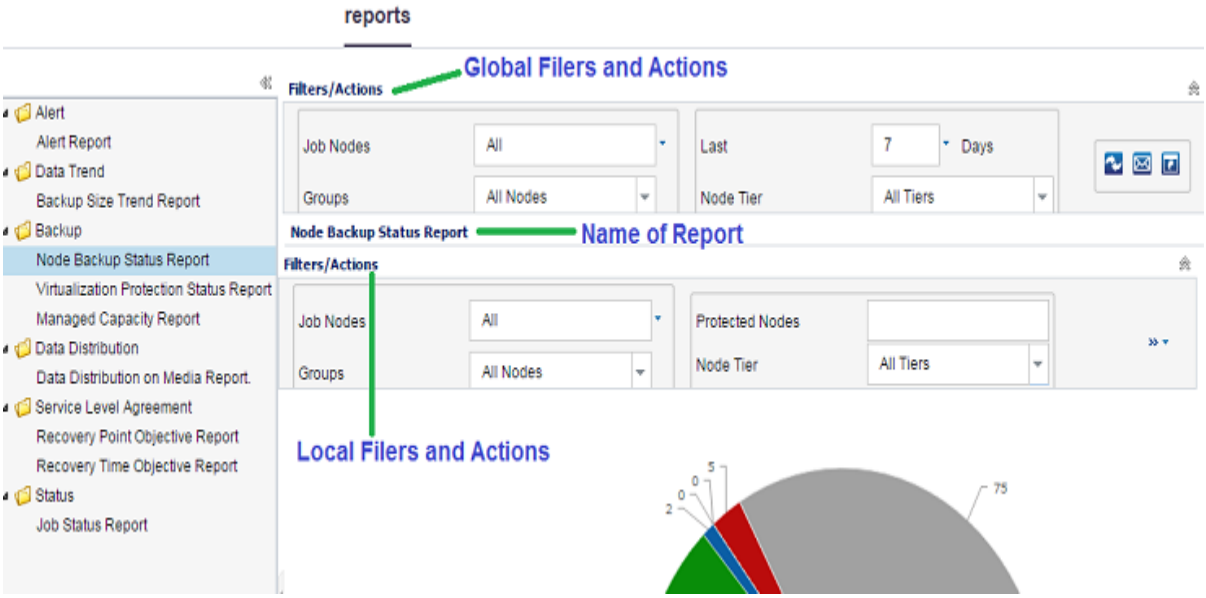


Quando un processo è in corso, il riquadro a destra indica il monitoraggio del processo che contiene l'avanzamento del processo stesso. Fare clic su **Dettagli processo** nel riquadro a destra per aprire il monitoraggio dei processi. È possibile visualizzare i monitoraggi dei processi soltanto se il processo è in corso.

Per annullare un processo, aprire il monitoraggio dei processi e fare clic su **Annulla.**

rapporti

La scheda **Rapporti** mostra un elenco dei rapporti che possono essere generati. Ai rapporti è possibile applicare filtri per ottenere rapporti specifici. I rapporti vengono generati nei formati CSV, PDF o HTML. Per ulteriori informazioni su questi rapporti, consultare la sezione Generazione dei rapporti di Arcserve UDP.



registro

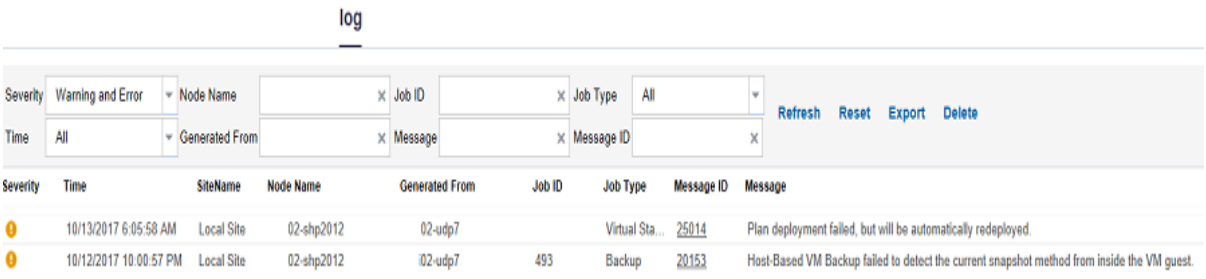
La scheda **Registro** mostra tutti i registri delle attività per i nodi protetti, i server di destinazione, gli archivi dati e i piani. È possibile visualizzare i registri e applicare vari filtri come ad esempio gravità, nodo specifico, registri generati dal computer, ID processo e contenuto del registro.

L'ID di messaggio contiene un collegamento ipertestuale per accedere alla documentazione dettagliata. Fare clic sul collegamento ipertestuale nella colonna MessageID per visualizzare la descrizione e la soluzione relativa al messaggio.

Nota: I registri attività generati da console, server/agente di backup Linux e processo di copia su nastro non contengono ID di messaggio.

È possibile cercare i registri attività mediante la combinazione dei filtri disponibili oppure utilizzando una delle seguenti opzioni:

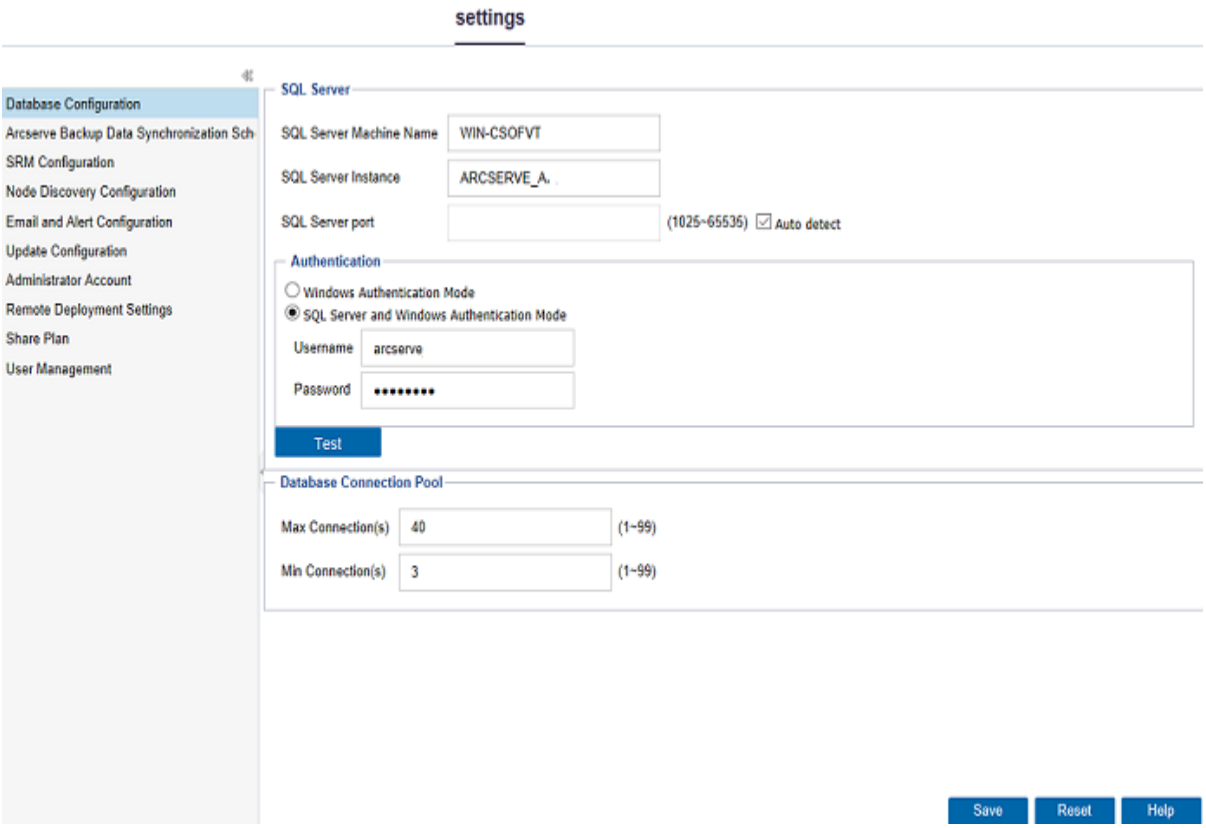
- Selezionare i tipi di gravità per visualizzare tutti i registri corrispondenti al tipo selezionato.
- Immettere altri dettagli (ad esempio il nome del nodo, l'ID del processo), quindi fare clic su **Cerca**.
- **Aggiorna:** mostra i registri più recenti disponibili in base ai filtri definiti.
- **Reimposta:** utilizza solo i filtri predefiniti e visualizza soltanto errori e avvisi per tutti i tipi di processo.
- **Esporta:** scarica il registro di processo corrente come file *.zip (activitylog_export_2017_10_12_15_02_27_586.zip) nella directory Download di Windows.
- **Elimina:** rimuove tutti i record di registro oppure i record di registro precedenti alla data specificata.



impostazioni

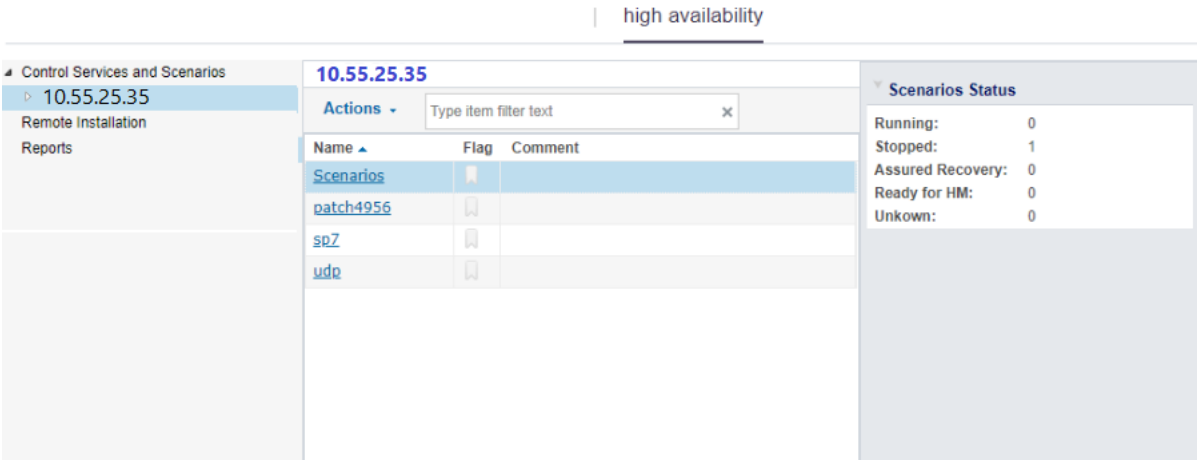
La scheda **Impostazioni** consente di configurare determinate preferenze, ad esempio il server di posta elettronica da utilizzare, la configurazione dell'ID utente e della password dell'amministratore e la definizione del percorso predefinito di distribuzione dei nodi.

Per ulteriori informazioni sulla scheda **Impostazioni**, consultare la sezione Configurazione di Arcserve UDP.



High Availability

La scheda **High Availability** consente di gestire e verificare le funzioni di Arcserve High Availability. Se necessario, immettere le credenziali nella finestra di dialogo **Aggiungi controllo servizio** e visualizzare i dettagli.

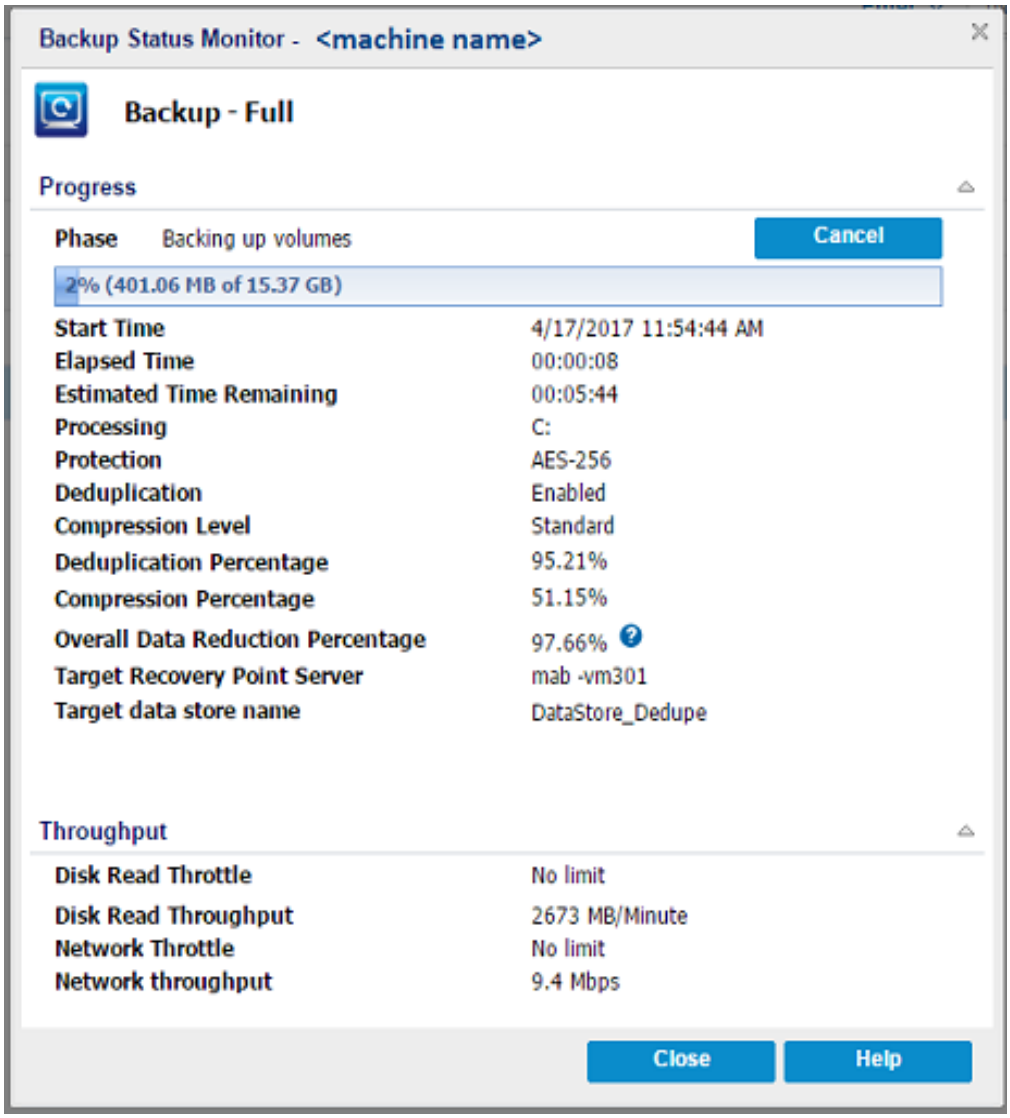


Finestra di dialogo Monitoraggio processi

La finestra di dialogo Monitoraggio processi consente di visualizzare lo stato di un processo. Quando il processo è in esecuzione, il riquadro si espande per visualizzare informazioni sull'evento in corso, ad esempio il tempo rimanente stimato per il completamento del processo, la percentuale e la dimensione del processo già completato, nonché la dimensione totale del processo una volta completato.

Quando viene eseguito un processo, espandere **Eventi recenti** dal riquadro destro, quindi fare clic sul pulsante **Dettagli** per aprire i monitoraggi dello stato e visualizzare ulteriori informazioni circa il processo corrente in esecuzione.

È possibile fare clic sul pulsante **Annulla** per interrompere il processo corrente.



Configurazione di Arcserve UDP

Mediante Arcserve Unified Data Protection è possibile specificare le seguenti impostazioni di configurazione di Arcserve Unified Data Protection.

- Protocollo di comunicazione del server
- Impostazioni del database
- Sincronizzazione dei dati di Arcserve Backup
- Configurazione SRM
- Configurazione rilevamento nodi
- Configurazione posta elettronica e avvisi
- Configurazione delle impostazioni proxy
- Configurazione aggiornamento
- Account di amministratore
- Impostazioni di distribuzione remota
- Condividi piano
- Gestione utenti
- Configurazione della durata del timeout per la console

Configurazione del protocollo di comunicazione del server

La soluzione HTTP utilizza il protocollo HTTP (Hypertext Transfer Protocol) per la comunicazione tra tutti i componenti. Arcserve Unified Data Protection Se si desidera utilizzare un livello di protezione superiore per la comunicazione delle password tra i componenti, è possibile modificare il protocollo HTTP e utilizzare il protocollo HTTPS (Hypertext Transfer Protocol Secure). Se non si desidera utilizzare tale livello di protezione aggiuntivo, è possibile modificare il protocollo utilizzato selezionando HTTP.

Nota: in caso di modifica del protocollo in HTTPS, verrà visualizzato un avviso nel browser Web. La visualizzazione dell'avviso è causata da un certificato di protezione autofirmato che richiede all'utente di ignorare l'avviso e continuare oppure di aggiungere il certificato al browser per evitarne la visualizzazione.

Effettuare le operazioni seguenti:

1. Accedere al computer di installazione della console Arcserve Unified Data Protection utilizzando un account amministrativo o un account con privilegi di amministratore.

   Nota: Se l'accesso non viene eseguito con un account amministrativo o un con privilegi di amministratore, è necessario configurare la riga di comando per l'esecuzione utilizzando l'opzione con privilegi Esegui come amministratore.
2. Aprire la riga di comando di Windows.
3. Eseguire una delle seguenti operazioni:
   - Per modificare il protocollo da HTTP a HTTPS:

     Avviare l'utilità changeToHttps.bat dalla seguente posizione predefinita.

     Nota: La posizione della cartella BIN può variare in base a percorso di installazione della console Arcserve Unified Data Protection.

     C:\Programmi\Arcserve\Unified Data Protection\Management\BIN

     Una volta apportate le modifiche al protocollo, verrà visualizzato il messaggio seguente:

     Il protocollo di comunicazione è stato convertito in HTTPS.
   - Per modificare il protocollo da HTTPS a HTTP:

     Avviare l'utilità changeToHttp.bat dalla seguente posizione predefinita

     Nota: La posizione della cartella BIN può variare in base a percorso di installazione della console Arcserve Unified Data Protection.

C:\Programmi\Arcserve\Unified Data Protection\Management\BIN

Una volta apportate le modifiche al protocollo, verrà visualizzato il messaggio seguente:

Il protocollo di comunicazione è stato convertito in HTTP.

4. Riavviare il browser e connettersi nuovamente alla Console Arcserve Unified Data Protection.

   Nota: Per aggiornare il protocollo di comunicazione utilizzato dal Recovery Point Server Arcserve Unified Data Protection e dall'agente Arcserve Unified Data Protection per comunicare con la console Arcserve Unified Data Protection, è necessario aggiornare il nodo direttamente dalla console.

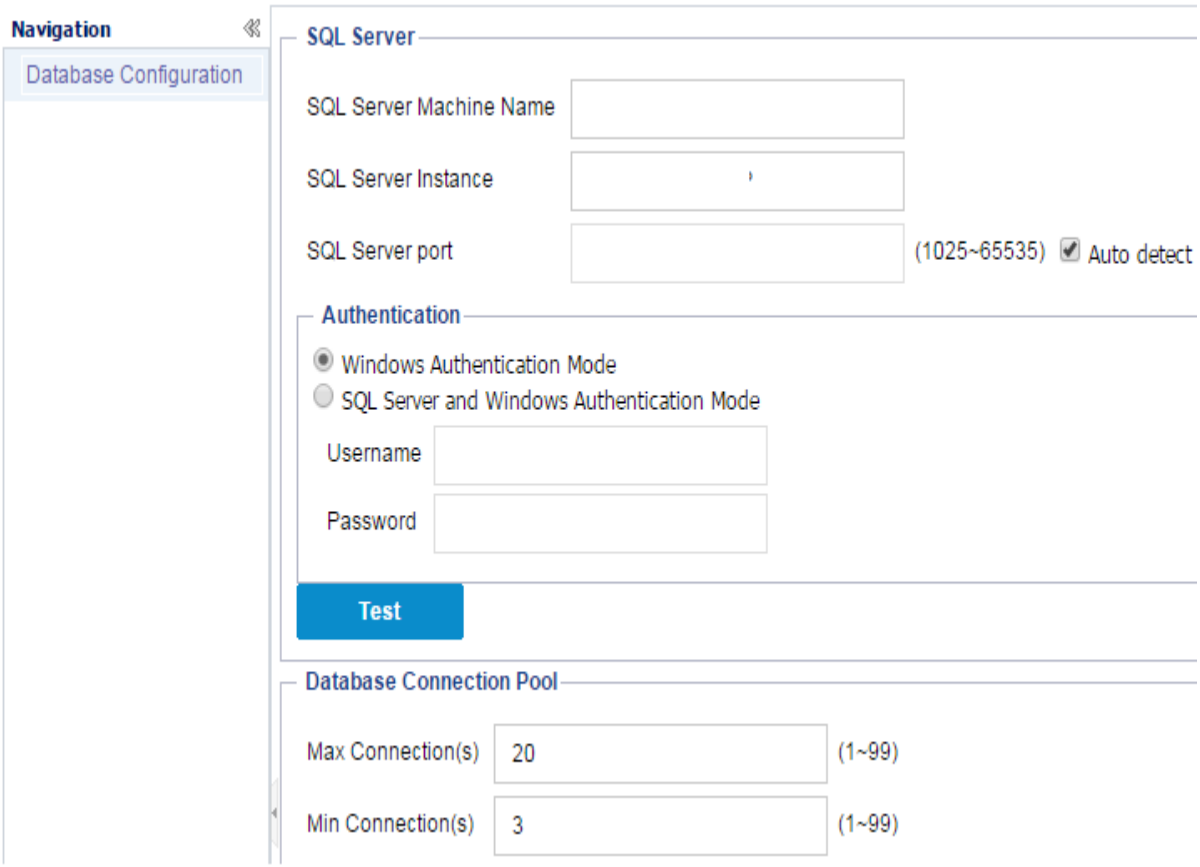
Configurazione del database

La pagina **Configurazione database** consente di immettere i dettagli sul database. Per la configurazione del database sono richiesti i dettagli su SQL Server, numero di connessioni e modalità di autenticazione.

Nota: prima della configurazione, è possibile creare nuovamente il database. Eliminare il database Arcserve Unified Data Protection mediante la procedura descritta in Ricreazione del database di Arcserve Unified Data Protection, quindi configurare il database.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Configurazione database**.



Ai fini della configurazione, completare i campi seguenti nella schermata di configurazione, quindi fare clic su **Salva**.

Nome del computer SQL Server

Specificare il nome del server che ospita l'istanza SQL Server.

Istanza SQL Server

Specificare il nome dell'istanza SQL Server.

Porta SQL Server

Specificare il numero di porta per l'istanza o abilitare l'opzione di **rilevamento automatico.** Il numero di porta è compreso nell'intervallo di valori da 1025 a 65535.

Rilevamento automatico

Selezionare la casella di controllo affinché l'applicazione rilevi automaticamente il numero di porta.

Autenticazione

Selezionare una delle opzioni seguenti per la modalità di autenticazione:

Modalità di autenticazione Windows: modalità predefinita:

(Facoltativo) **Verifica**: fare clic su Verifica per controllare la comunicazione tra l'applicazione e l'istanza di Microsoft SQL Server.

Modalità di autenticazione Windows e SQL Server:

selezionare l'opzione e immettere i dettagli nei campi Nome utente e Password.

Valori per Pool di connessioni di database

Per i campi del numero massimo e minimo di connessioni, immettere un valore da 1 a 99.

La configurazione del server di database è stata impostata.

Utilizzare l'opzione **Reimposta** per cancellare tutti i valori specificati e caricare i dati originali.

Ricreazione del database Arcserve Unified Data Protection

Per diversi motivi, potrebbe essere necessario ricreare il database Arcserve Unified Data Protection. Ad esempio, nel caso in cui il database contenga più di 10GB di dati. Per creare nuovamente il database, sarà necessario eliminare in primo luogo il database Arcserve Unified Data Protection esistente, quindi configurare un nuovo database per sostituire quello eliminato. La procedura viene applicata ai database Microsoft SQL Server e Microsoft SQL Server Express Edition.

Importante! Se il database Arcserve Unified Data Protection viene eliminato, tutti i dati correnti andranno persi.

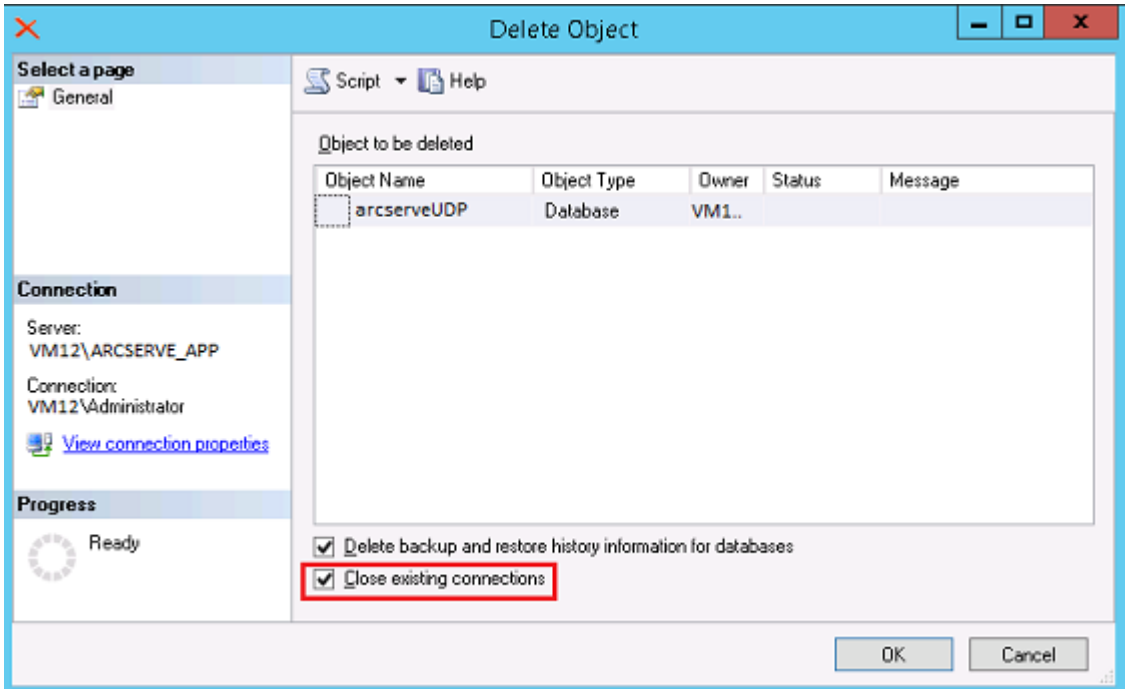
Per ricreare il database Arcserve Unified Data Protection

1. Aprire Microsoft SQL Server Management Studio Express e accedere all'istanza ARCSERVE_APP.

   Nota: Se Microsoft SQL Server Management Studio Express non è installato sul server Arcserve Unified Data Protection, è possibile scaricare l'utilità dall'Area download di Microsoft.

2. Fare clic con il pulsante destro del mouse su Arcserve UDP, quindi selezionare **Elimina** dalla finestra di dialogo pop-up.

   Verrà visualizzata la finestra di dialogo **Elimina oggetto**.



3. Dalla finestra di dialogo **Elimina oggetto**, fare clic su **Chiudi connessioni esistenti**, quindi selezionare **OK**.

   Il database Arcserve Unified Data Protection esistente viene eliminato.

4. Configurare il nuovo database. Per ulteriori informazioni, consultare la sezione Configurazione del database.

   La soluzione Arcserve Unified Data Protection consente di ricreare il database. Il nome dell'istanza di database corrisponderà a **ARCSERVE_APP**.

Configurazione della sincronizzazione dati di backup di Arcserve

È possibile configurare l'opzione di **pianificazione sincronizzazione dati di backup di Arcserve** .

Effettuare le operazioni seguenti:

1. Dalla console, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Sincronizzazione dati di Arcserve Backup**.
3. Dal riquadro a destra, fare clic su **Abilita**.

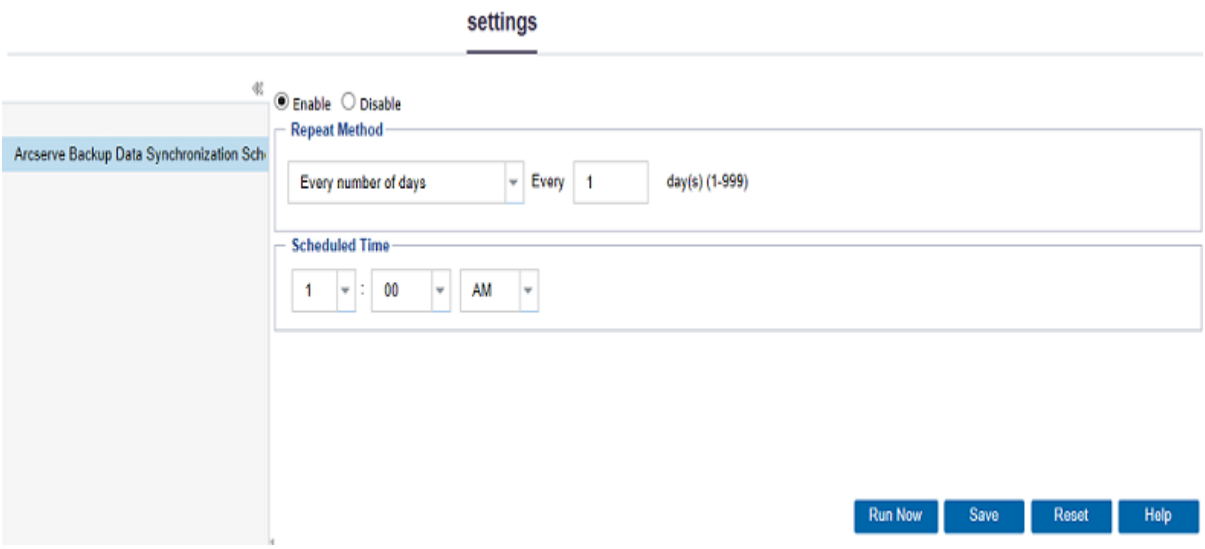
   Per impostazione predefinita, la configurazione della **sincronizzazione dei dati di Arcserve Backup** è abilitata.

   Nota: Fare clic su **Disabilita** per interrompere la pianificazione.
4. Specificare i parametri seguenti per la pianificazione della sincronizzazione dei dati di Arcserve Backup:
   - **Metodo di ripetizione**
   - **Ora pianificata**
5. Fare clic su **Salva**.

   La pianificazione della sincronizzazione dei dati di Arcserve Backup è stata applicata.

   Nota: Non fare clic su **Salva** se si desidera eseguire immediatamente la sincronizzazione.
6. (Facoltativo) Per eseguire immediatamente il processo, fare clic su **Esegui ora**.

   La finestra di dialogo **Nodo** viene visualizzata con l'elenco dei nodi disponibili per la sincronizzazione.



7. Selezionare i nodi da eseguire per la sincronizzazione, quindi fare clic su **OK**.

Configurazione di SRM

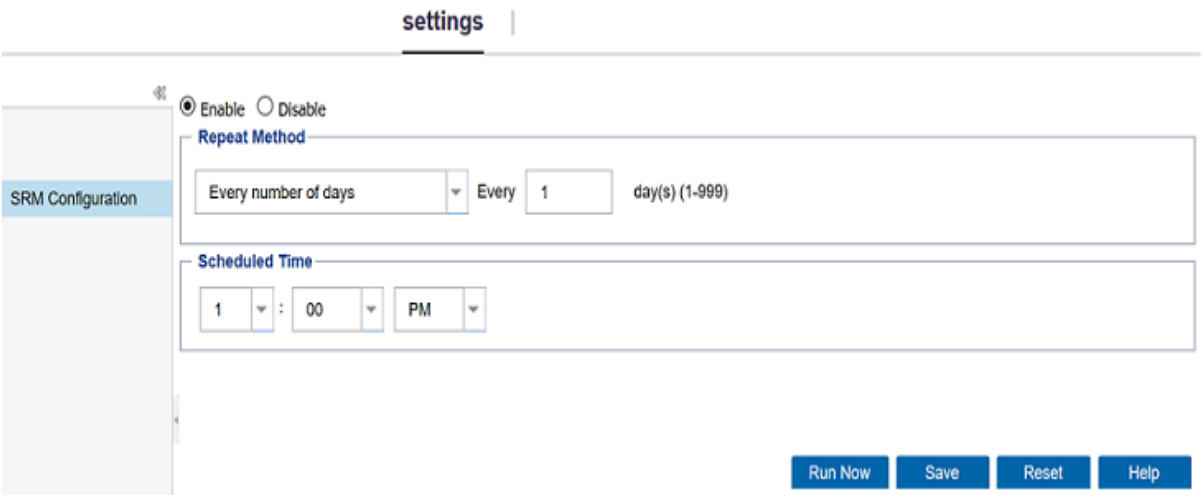
La pagina Configurazione SRM consente di configurare una pianificazione SRM dei nodi per definire l'avvio e la frequenza della raccolta dei dati SRM. La funzionalità SRM (Gestione delle risorse di archiviazione) consente di raccogliere informazioni sui dati seguenti:

- Dati hardware, software e delle applicazioni per le implementazioni di Microsoft SQL Server e Microsoft Exchange Server.
- Dati sugli indicatori di prestazioni chiave (PKI) dai nodi.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Configurazione SRM**.
3. Dal riquadro a destra, fare clic su **Abilita**.

   Per impostazione predefinita, la **configurazione della gestione delle risorse di archiviazione (SRM)** è abilitata.



   Nota: Fare clic su **Disabilita** per interrompere la pianificazione.

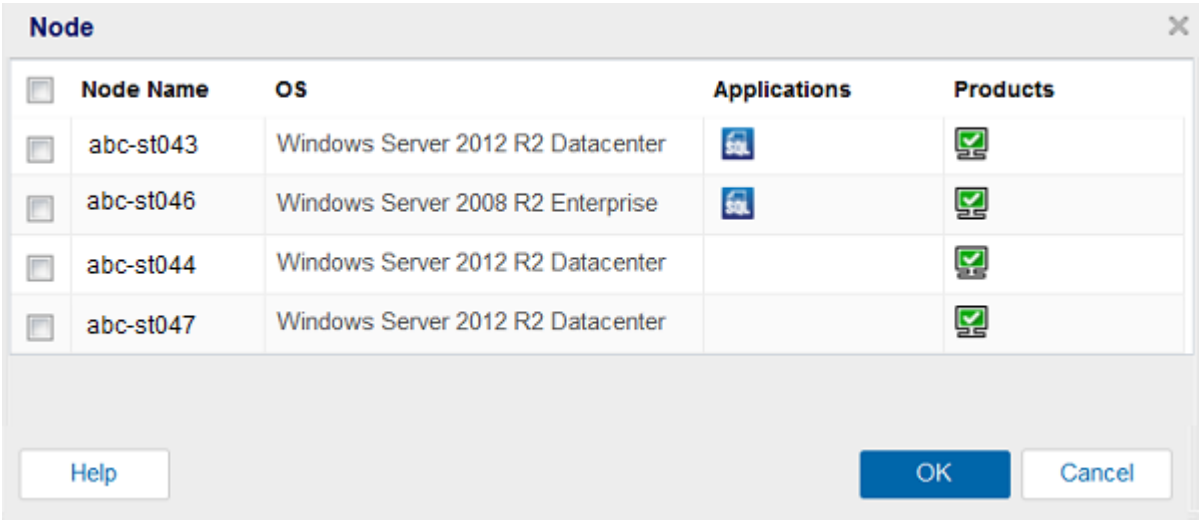
4. Specificare i parametri seguenti per la pianificazione della gestione delle risorse di archiviazione (SRM):
   - **Metodo di ripetizione**
   - **Ora pianificata**
5. Fare clic su **Salva**.

   Viene applicata la pianificazione per la gestione delle risorse di archiviazione (SRM).

Nota: Non fare clic su **Salva** se si desidera raccogliere immediatamente i dati SRM.

6. (Facoltativo) Per eseguire immediatamente il processo, fare clic su **Esegui ora**.

   La finestra di dialogo **Nodo** viene visualizzata con l'elenco dei nodi disponibili per la sincronizzazione.



7. Selezionare i nodi da eseguire per la sincronizzazione, quindi fare clic su **OK**.

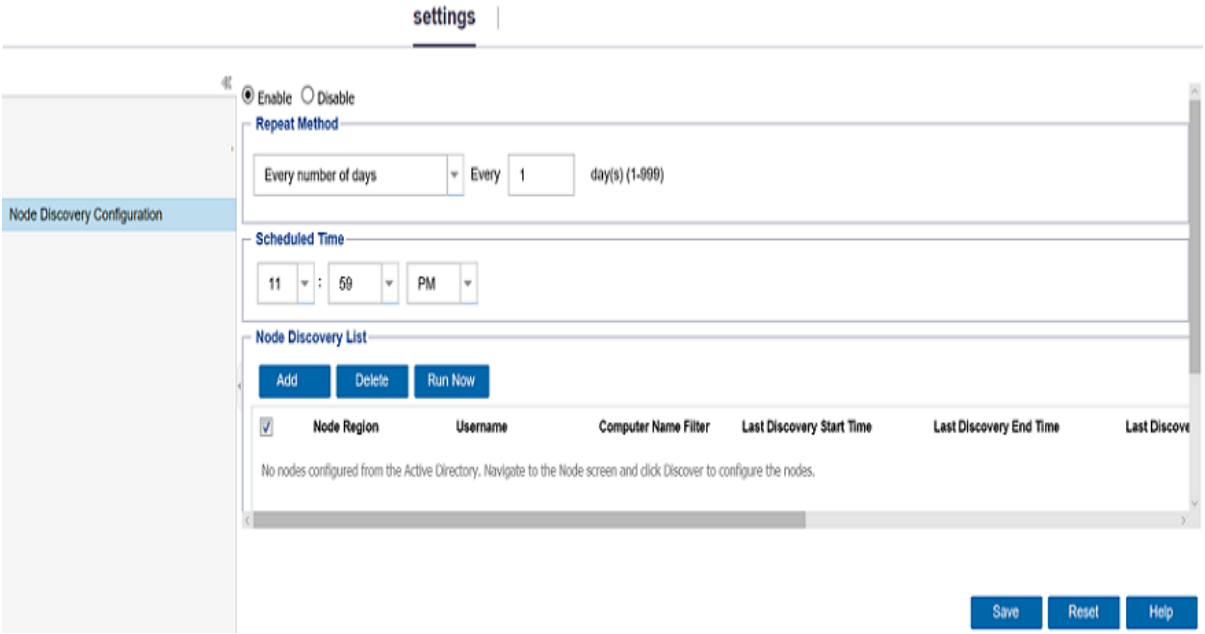
Configurazione rilevamento nodi

La pagina **Configurazione rilevamento nodi** consente di configurare la pianificazione di rilevamento dei nodi Active Directory, VMware vSphere e Microsoft Hyper-V su base ripetitiva e all'ora prestabilita. Quando vengono rilevati dei nodi nuovi, l'amministratore riceve un avviso di posta elettronica per l'aggiunta manuale di tali nodi. Per impostazione predefinita, la **configurazione del rilevamento** è disabilitata.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Configurazione rilevamento nodi**.

   Per abilitare la configurazione, fare clic sull'opzione **Abilita** per specificare il tipo di ricorrenza desiderato e l'ora pianificata per l'avvio del rilevamento nodi.



È possibile specificare i seguenti parametri di configurazione della pianificazione di rilevamento:

- **Ogni (numero di giorni)**: consente di ripetere il metodo in base al numero di giorni specificato. (Valore predefinito)
- **Ogni giorno della settimana selezionato**: consente di ripetere il metodo nei giorni della settimana specificati. Lunedì, martedì, mercoledì, giovedì e venerdì sono i giorni predefiniti della settimana.
- **Ogni giorno del mese selezionato**: consente di ripetere il metodo nel giorno del mese specificato. Il valore predefinito per il giorno del mese è 1.

- **Ora pianificata**: consente di specificare l'ora di esecuzione del rilevamento secondo la ripetizione pianificata.
- **Elenco Rilevamento nodi>Aggiungi:** Selezionare la posizione da cui aggiungere i nodi. Specificare quindi le credenziali necessarie.

  Nota: In via opzionale, fare clic su **Esegui ora** per eseguire il rilevamento immediatamente.

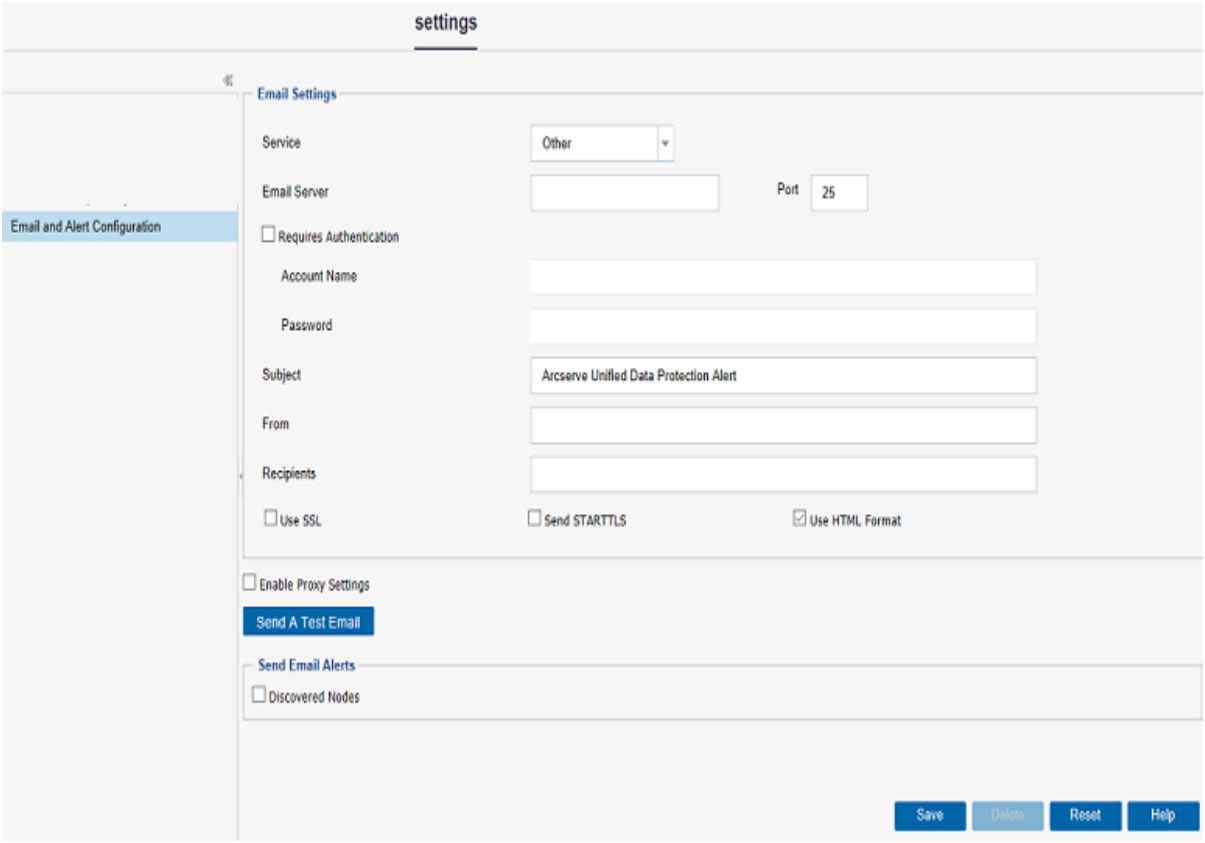
Configurazione di posta elettronica e avvisi

La pagina **Configurazione posta elettronica e avvisi** consente di specificare le impostazioni di posta elettronica e la configurazione degli avvisi da inviare tramite posta elettronica.

Nota: in via preliminare, installare Microsoft .NET Framework (versione 2.0 o successiva) nel computer in cui è installata la console per consentire la corretta esportazione delle immagini contenute nei rapporti tramite la funzionalità di esportazione per i grafici dei rapporti.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Configurazione posta elettronica e avvisi**.
3. Immettere i dettagli per le impostazioni predefinite.



Servizio

Selezionare i servizi di posta elettronica dalle opzioni disponibili.

Server di posta elettronica

Specificare il nome host del server di posta SMTP utilizzabile per l'invio degli avvisi tramite posta elettronica.

Porta

Specificare il numero di porta relativo al server di posta elettronica.

Richiede l'autenticazione

Selezionare la casella di controllo per immettere le credenziali.

Usa SSL/Invia STARTTLS/Usa formato HTML

Selezionare l'opzione desiderata per specificare i requisiti.

Abilita impostazioni proxy

Selezionare la casella di controllo per immettere i dettagli relativi al **server proxy** e alla modalità di autenticazione.

Messaggio di posta elettronica di verifica

Fare clic per verificare i dettagli inseriti nella sezione Impostazioni di posta elettronica.

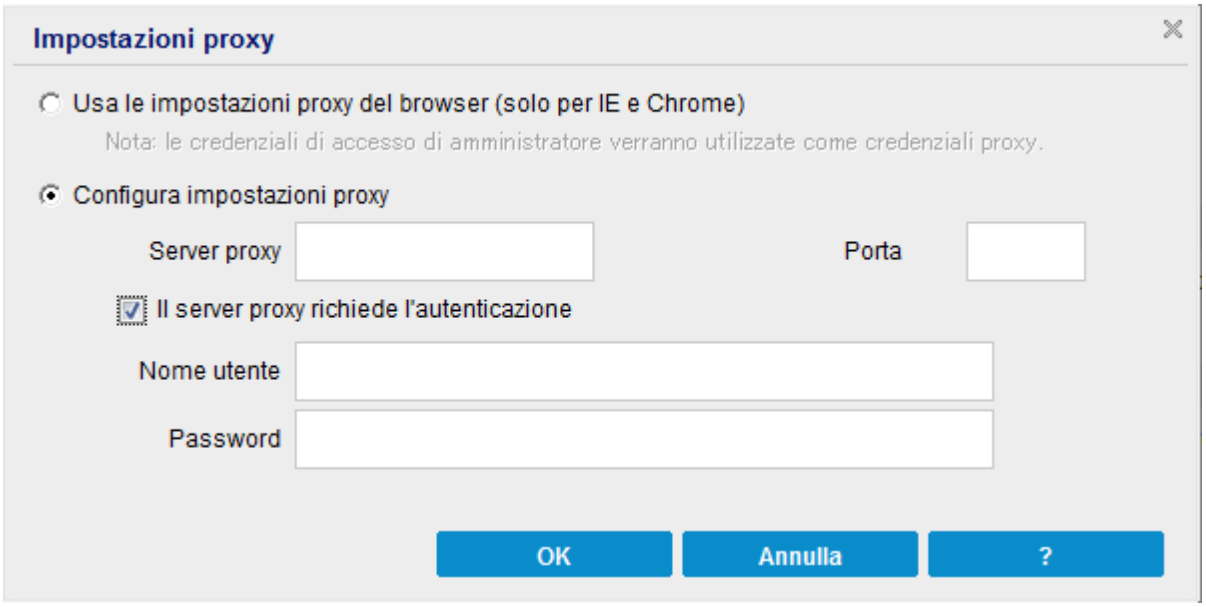
Invia avvisi tramite posta elettronica

Selezionare **Nodi rilevati** per configurare i nodi di **Active Directory** che è possibile trovare con la funzionalità di rilevamento disponibile per i nodi sotto la scheda **Risorse**.

Configurazione delle impostazioni proxy

Selezionare **Impostazioni proxy** per specificare se si desidera che Arcserve UDP comunichi tramite il server proxy. Un server proxy funge da intermediario tra il server in uso e il server Arcserve, al fine di garantire la protezione, le prestazioni e il controllo amministrativo. Le impostazioni immesse verranno utilizzate per la connessione al server Arcserve dal quale il server di download acquisisce gli aggiornamenti.

Se si seleziona il server Arcserve come server di download, viene visualizzata la finestra di dialogo **Impostazioni proxy**.



- **Utilizza le impostazioni proxy del browser**

  Questa opzione è applicabile soltanto per Windows Internet Explorer (IE) e Google Chrome.

  Se selezionata, Arcserve UDP rileva e utilizza automaticamente le stesse impostazioni proxy applicate al browser per stabilire la connessione al server Arcserve e acquisire le informazioni sull'aggiornamento di Arcserve UDP.

- **Configurazione delle impostazioni proxy**

  Se selezionata, questa opzione abilita la connessione del server proxy specificato al server Arcserve per le informazioni sull'aggiornamento di Arcserve UDP. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet.

Inoltre, sarà possibile specificare se il server proxy richiede l'autenticazione. Se selezionata, infatti, l'opzione indica che sono necessarie informazioni di autenticazione (ID utente e password) per l'utilizzo del server proxy.

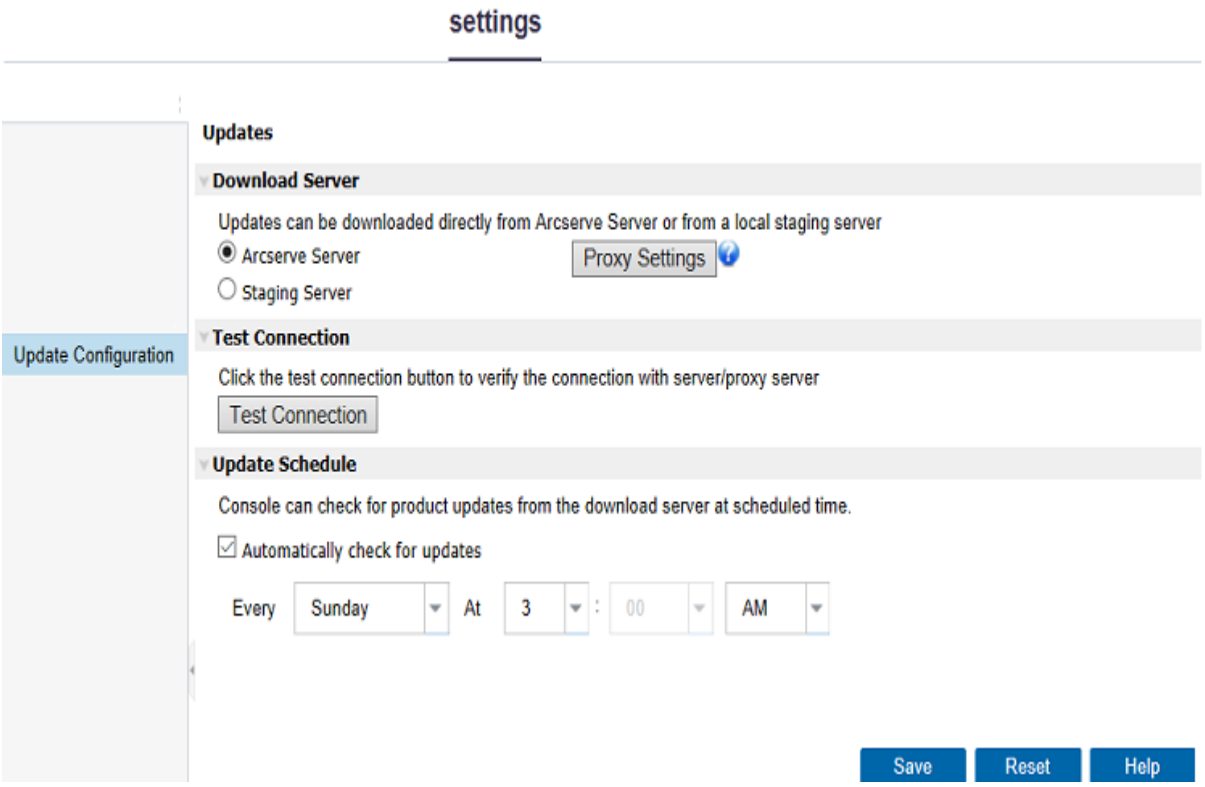
Nota: il nome utente del dominio deve essere completo e presentare il formato <nome dominio>\<nome utente>.

Configurazione aggiornamento

La pagina Configurazione aggiornamento consente di impostare la pianificazione del server di download e dell'aggiornamento per la configurazione degli aggiornamenti. È possibile fornire i dettagli sulle Arcserve impostazioni proxy del server o del server di gestione temporanea per l'opzione Server di download.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Configurazione aggiornamento**.



Fornire i dettagli sul tipo per il server di aggiornamento e la pianificazione degli aggiornamenti. Il server di aggiornamento può essere Arcserve il server o il server di gestione temporanea.

3. Per **Server di download**, selezionare una delle opzioni seguenti:
   - Per **Server Arcserve**, fare clic su **Impostazioni proxy** per completare la configurazione proxy.
   - Per **Server di gestione temporanea**, fare clic su **Aggiungi server** per fornire i dettagli sul server di gestione temporanea.

Per creare un server di gestione temporanea, consultare la sezione Creazione di un server di gestione temporanea.

Se il server di gestione temporanea è protetto da un firewall, preparare un computer che disponga dell'accesso a Internet, che disponga di un UDP installato e recuperare gli aggiornamenti più recenti dal Arcserve Server. Copiare quindi le cartelle **EngineUpdates** e **FullUpdates** dalla posizione seguente sul computer server di gestione temporanea:

<UDP install path>\ Arcserve\Unified Data Protection\Update Manager



Note:

- Come funzione di aggiornamento automatico non è necessario disporre della licenza, non è necessario attivare la licenza sul server di gestione temporanea.
- Per ulteriori informazioni sulle porte, consultare la sezione Porte di comunicazione utilizzate da Arcserve UDP.

È possibile aggiungere più server di gestione temporanea.

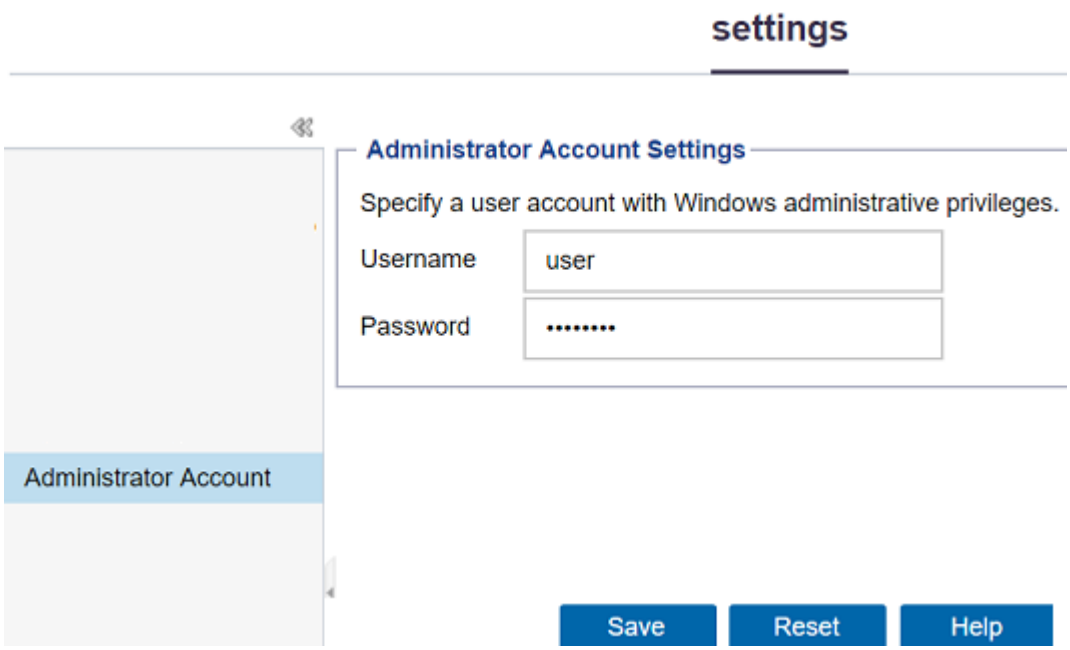
4. Fare clic su **Verifica connessione** per controllare i dettagli del **server di download**.
5. Immettere i dettagli per **Pianificazione aggiornamenti**.
6. Selezionare **Verifica aggiornamenti automaticamente**.
7. Fare clic su **Salva** per completare l'aggiornamento.

Configurazione dell'account di amministratore

La configurazione **Account di amministratore** consente di creare un account utente fornendo un **nome utente** e una **password**.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Account di amministratore**.



3. Fornire le credenziali dell'account di amministratore e fare clic su **Salva**.

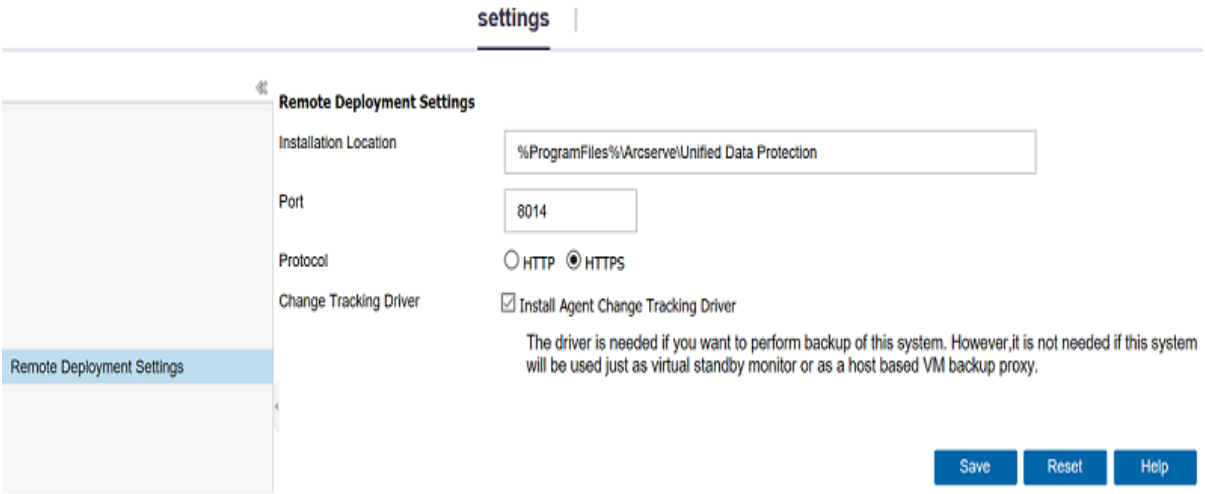
Impostazioni di distribuzione remota

La pagina **Impostazioni di distribuzione remota** consente di specificare le impostazioni predefinite per l'installazione dell'agente Arcserve Unified Data Protection e il Recovery Point Server Arcserve Unified Data Protection. Specificare le impostazioni di installazione predefinite per fornire la posizione dell'installazione.

Immettere i dettagli relativi a **percorso di installazione**, **protocollo** e **porta**, quindi fare clic su **Salva**.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Impostazioni di distribuzione remota**.



3. Immettere i dettagli richiesti, quindi fare clic su **Salva**.

Mapping del piano sull'account utente

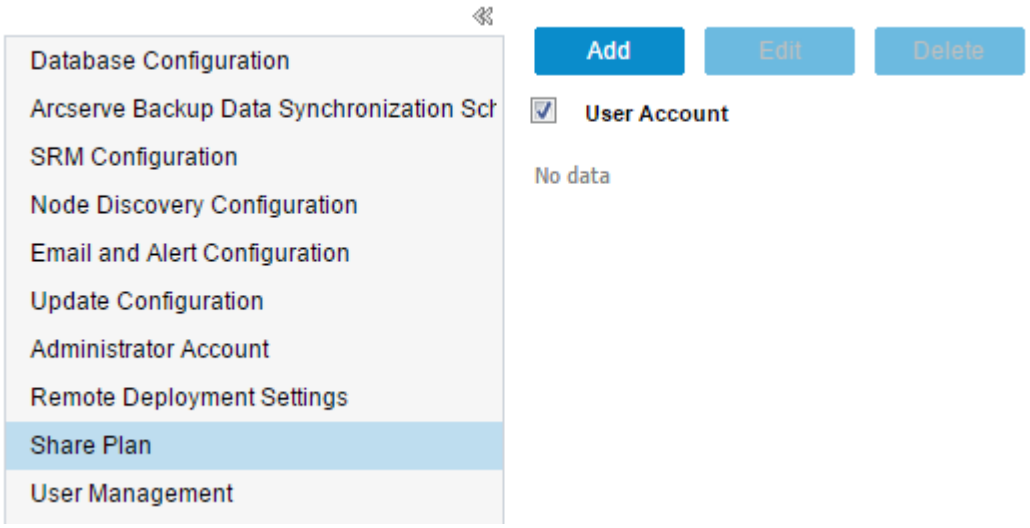
Amministratore della destinazione

L'account utente e il piano per la Console di origine sono stati creati precedentemente. Per identificare e gestire i dati replicati, assegnare il piano all'account utente.

Nota: è possibile assegnare più di un piano a un account utente. Tuttavia, due account diversi non possono condividere lo stesso piano. Si consiglia di assegnare un solo piano a ciascun account utente in modo da poter identificare e gestire facilmente i dati replicati.

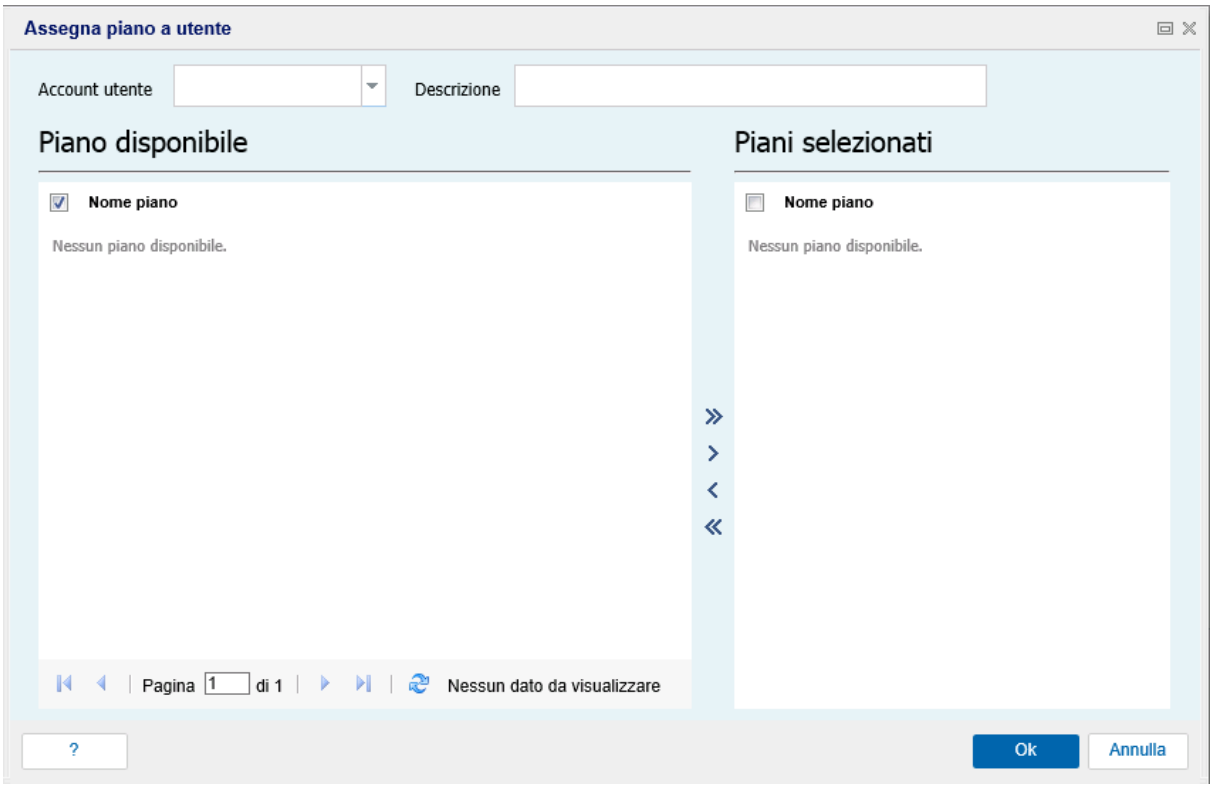
Effettuare le operazioni seguenti:

1. Dalla console, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Condividi piano**.



3. Dal riquadro centrale, fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo **Assegna piano a utente**.



4. Selezionare l'**account utente**.
5. Selezionare un piano dalla colonna **Piano disponibile**.

   Nota: Se un piano è già stato aggiunto a un nome utente, tale piano non viene visualizzato nella colonna **Piano disponibile**.
6. Fare clic su **Aggiungi tutti i piani** o **Aggiungi i piani selezionati** per aggiungere i piani nella colonna **Piani selezionati**.
7. Fare clic su **OK**.

   La finestra di dialogo **Assegna piano a utente** viene chiusa. Il nome utente e i piani associati vengono visualizzati nella pagina **Condividi piano**.

   Viene eseguito il mapping dell'account utente sul piano creato la Console di origine.

   È possibile utilizzare l'opzione **Modifica** per modificare la configurazione utente oppure l'opzione **Elimina** per rimuovere l'utente dall'elenco.

Gestione utenti

La pagina Gestione utenti consente di eseguire le seguenti operazioni:

- Accedere alla console di gestione degli utenti (console del servizio identità) dalla console Arcserve UDP. Per ulteriori informazioni, consultare la sezione Avvio della Console di gestione degli utenti di Arcserve UDP.
- Abilitare e configurare l'autenticazione a più fattori (MFA) per tutti gli utenti. Per ulteriori informazioni, consultare la sezione Configurazione dell'autenticazione a più fattori.

Configurazione della durata del timeout per la console

Se la console non è attiva per un determinato intervallo, l'utente viene disconnesso automaticamente dalla console. È possibile modificare il valore di timeout predefinito nel file ConsoleConfiguration.xml.

Effettuare le operazioni seguenti:

1. Accedere al computer in cui è stata installata la console.
2. Aprire il file ConsoleConfiguration.xml dal percorso seguente:

   <UDP_Home>\Management\Configuration\ConsoleConfiguration.xml
3. Modificare il valore per consoleUISessionTimeout.

   Il valore è espresso in secondi.

   Ad esempio:

   <consoleUISessionTimeout>3600</consoleUISessionTimeout> (il valore predefinito è 1 ora, il valore è espresso in secondi)

   3600 indica che la durata del timeout per la console è di 3600 minuti.
4. Salvare il file ConsoleConfiguration.xml.

Migrazione dei punti di ripristino di Arcserve r16.5 a Arcserve UDP

Importante! Se è in corso la replica da una cartella condivisa in un archivio dati selezionato sul Recovery Point Server, consultare la sezione Esecuzione di una replica di dati non in linea utilizzando JumpStart RPS.

Per eseguire la migrazione dei punti di ripristino Arcserve r16.5 in Arcserve UDP, procedere come segue:

1. Creazione di un archivio dati per la replica dei dati da Arcserve r16.5
2. Replica dei dati di Arcserve r16.5 nell'archivio dati UDP

Creazione di un archivio dati per la replica dei dati da un punto di ripristino Arcserve r16.5

Per replicare i dati da un punto di ripristino esistente di Arcserve r16.5 D2D, creare prima l'archivio dati dalla Console in cui verrà eseguita la replica dei dati.

Effettuare le operazioni seguenti:

1. Accedere alla console Arcserve UDP.
2. Accedere a **Destinazioni**, **Recovery Point Server**.
3. Selezionare il Recovery Point Server.
4. Fare clic con il tasto destro del mouse e selezionare **Aggiungi archivio dati**.
5. Immettere i dettagli nella pagina **Aggiungi archivio dati**.
6. Salvare l'archivio dati.

   L'archivio dati è stato creato.

Replica dei dati di Arcserve r16.5 nell'archivio dati UDP

Dopo aver creato l'archivio dati, è possibile replicare i dati dal punto di ripristino di Arcserve r16.5 in questo archivio dati mediante JumpStart RPS.

Effettuare le operazioni seguenti:

1. Fare clic su **Azioni**, quindi su **JumpStart RPS**.

   Viene visualizzata la **Procedura di installazione guidata di RPS.**

2. Selezionare Da una cartella condivisa a un archivio dati sul Recovery Point Server selezionato.
3. Specificare la cartella condivisa di origine.

   Vengono visualizzati i dettagli relativi al punto di ripristino.

   Nota: Se la sessione non è crittografata e l'archivio dati di destinazione non è crittografato, la password di sessione è facoltativa. Se la sessione non è crittografata e l'archivio dati di destinazione è crittografato, è necessario fornire la password di sessione nella pagina **Selezione dell'archivio dati di destinazione**.

4. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Selezione dell'archivio dati di destinazione.** Se i dati di origine sono crittografati, nell'elenco a discesa vengono mostrati soltanto gli archivi dati crittografati.

5. (Facoltativo) Specificare la password di sessione in caso di sessione non crittografata come nel passaggio 3.
6. Fare clic su **Avanti**.
7. Fare clic su **Fine**.

   I dati del punto di ripristino da Arcserve r16.5 vengono replicati nell'archivio dati Arcserve UDP.

Procedura guidata di configurazione

Usando la procedura guidata di configurazione, configurare l'ambiente di protezione dei dati appena si accede alla console. Se si utilizza Arcserve UDP per la prima volta, la procedura guidata di configurazione è la soluzione ideale per creare il primo piano di backup. La procedura guidata crea piani per definire le modalità di protezione dei dati. Un piano è composto da una o più attività per definire l'origine, la destinazione, la pianificazione e i parametri avanzati. Con il primo accesso alla Console, viene visualizzata la procedura di configurazione guidata. È possibile nascondere la pagina iniziale della procedura guidata selezionando l'opzione **Do not show this page next time (Non mostrare più questa pagina)**.

È possibile creare un piano per proteggere nodi fisici, ad esempio i nodi Windows e Linux, e computer virtuali quali VMware e Hyper-V.

La procedura seguente fornisce indicazioni generiche su come creare un piano basato su agente per Windows mediante la procedura guidata di configurazione.

1. Accedere alla console.

   Se si accede per la prima volta, viene visualizzata la procedura guidata di configurazione.

2. Se non viene visualizzata la procedura guidata, fare clic sulla scheda **Risorse** e fare clic su **Configuration Wizard (Procedura guidata di configurazione)** nel riquadro a destra.

   Verrà visualizzata la pagina iniziale della procedura guidata.

3. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Create Plan (Crea piano)**.

4. Specificare il nome utente.

5. Selezionare un tipo di nodo da proteggere.

   Ad esempio, selezionare **Backup: Windows basato su agente**.

6. Fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo **Add Nodes to Protect (Aggiungi nodi da proteggere)**. I campi della pagina Add Nodes to Protect (Aggiungi nodi da proteggere)) sono facoltativi.

7. Selezionare il metodo per l'aggiunta dei nodi dall'elenco a discesa.

   I campi variano a seconda della selezione.

8. Fornire i dettagli relativi al nodo, fare clic su **Aggiungi a elenco**, quindi fare clic su **Avanti**.

Viene visualizzata la pagina **Destinazione di backup**.

9. Specificare il tipo di destinazione dall'elenco a discesa.

   I campi restanti nella pagina **Destinazione di Backup** variano a seconda del tipo di destinazione. È inoltre possibile abilitare la password di sessione.

   Per creare un archivio dati, consultare la sezione Aggiunta di un archivio dati.

10. Specificare i restanti dettagli relativi alla destinazione, quindi fare clic su **Avanti**.

    Viene visualizzata la pagina **Pianificazione di backup**.

11. Specificare la pianificazione di backup, quindi fare clic su **Avanti**.

    Viene visualizzata la pagina **Conferma piano**.

12. Verificare il piano.
13. (Facoltativo) Fare clic su **Create Plan (Crea piano)** per aggiungere un altro piano.
14. Fare clic su **Avanti**

    La configurazione delle risorse viene completata.

15. Fare clic su **Fine**.

    La procedura guidata viene chiusa e viene creato un nuovo piano.

    È possibile visualizzare il piano in **Risorse**, **Piani**, **Tutti i piani**.

Chapter 6: Utilizzo delle funzionalità principali di Arcserve UDP

La presente sezione descrive i seguenti argomenti:

Nozioni fondamentali sulle funzionalità Nutanix in Arcserve UDP

Per esplorare le funzioni disponibili per la funzione Nutanix in Arcserve UDP, consultare la sezione Come utilizzare Nutanix con Arcserve UDP.

Nozioni fondamentali sulle funzionalità OneDrive in Arcserve UDP

Esplorare le opzioni disponibili per la funzionalità OneDrive in Arcserve UDP.

- Gestione dei nodi di OneDrive
- Creazione di un piano di backup per OneDrive Microsoft Office 365
- Ripristino dei dati di OneDrive

Informazioni sulla funzionalità di Exchange Online in Arcserve UDP

Exchange Online è un'applicazione di posta elettronica ospitata su cloud di Microsoft. Per proteggere gli elementi di posta di Exchange Online (messaggi di posta elettronica, gli elementi calendario, contatti e così via) da Microsoft Cloud, è necessario creare un piano in Arcserve UDP. Esplorare le opzioni disponibili per la funzionalità di Exchange Online in Arcserve UDP.

- Privilegi utente per Exchange Online in Arcserve UDP
- Aggiunta di un nodo Exchange Online
- Gestione dei nodi di Exchange Online
- Aggiunta di un ruolo e di un gruppo obbligatori all'account di backup di Exchange Online per l'esecuzione di backup e ripristini
- Creazione di un piano di backup di Exchange Online
- Ripristino dei dati della casella di posta di Exchange Online
- Procedura consigliata

Informazioni sulla funzionalità di snapshot hardware in UDP

Arcserve UDP ha la possibilità di utilizzare le snapshot di archiviazione hardware per il backup. È possibile specificare se si desidera utilizzare la snapshot hardware durante la creazione di un'attività di backup. Se si seleziona la snapshot hardware, Arcserve UDP prova innanzitutto a creare una snapshot hardware. In caso di errore della snapshot hardware, Arcserve UDP torna automaticamente alla snapshot software senza interrompere il processo di backup.

- Utilizzo della snapshot hardware per il backup
- Array di archiviazione supportato in UDP Arcserve
- Utilizzo della snapshot hardware per il backup senza agente VMware
- Utilizzo della snapshot hardware per il backup senza agente Hyper-V
- Utilizzo di una snapshot hardware per il backup basato sull'agente
- Verifica del backup completato utilizzando la snapshot hardware

Nimble

- Aggiunta di un array di archiviazione
- Considerazioni sull'archiviazione Nimble quando è abilitata l'autenticazione CHAP
- Utilizzo della snapshot hardware per il backup senza agente VMware

Server di archiviazione HPE 3PAR

- Aggiunta di un array di archiviazione
- Utilizzo della snapshot hardware per il backup senza agente VMware

NetApp

- Aggiunta di un array di archiviazione
- Considerazioni sul supporto NetApp iSCSI/FC per VMware
- Condizioni applicate alla snapshot hardware per NetApp NFS VMware
- Utilizzo della snapshot hardware per il backup senza agente VMware

Informazioni sulla funzionalità cloud in UDP

La funzionalità cloud di Arcserve UDP garantisce la protezione dei dati nel cloud in caso di eliminazione accidentale. L'utilizzo delle funzionalità cloud di Arcserve UDP consente di copiare i file e i punti di ripristino specificati, creare istanze tramite i punti di ripristino, creare computer virtuali Virtual Standby nel cloud e così via.

Visualizzare i collegamenti per l'utilizzo del cloud in Arcserve UDP:

- Aggiunta di un account cloud
- Gestione dei nodi per il cloud
  - Download del punto di ripristino dal cloud
  - Caricamento del punto di ripristino su cloud
  - Copia del punto di ripristino su disco locale o condivisione di rete
- Configurazione di un server RPS nel cloud
  - Definizione della configurazione cloud per il ripristino da un percorso cloud di copia file
  - Definizione della configurazione cloud per il ripristino da un percorso cloud di archiviazione file
- Come eseguire il backup dei dati dal cloud
  - Creazione di un piano di Virtual Standby su AWS EC2
  - Modalità di creazione e gestione di un computer virtuale istantaneo su Amazon EC2
  - Creazione di un piano di copia dei punti di ripristino
- Cloud per Linux
  - Installazione dell'agente Arcserve UDP (Linux) in AWS Cloud
  - Esecuzione di un ripristino bare metal per computer Linux nel cloud AWS
  - Esecuzione di un ripristino bare metal di migrazione per computer Linux da Amazon EC2 sul computer locale
  - Migrazione di un computer virtuale istantaneo da cloud a locale
- Piano di Backup di Microsoft Office 365
  - Creazione di un piano di backup di Exchange Online
  - Ripristino dei dati della casella di posta di Exchange Online

- Creazione di un piano di backup per OneDrive Microsoft Office 365
- Ripristino dei dati di OneDrive
- Creazione di un piano di backup SharePoint Online (Guarda il video)
- Ripristino dei dati di una raccolta siti di SharePoint Online

- Microsoft Azure
  - Creazione di un computer Virtual Standby su un piano Microsoft Azure
  - Creazione e gestione di un computer virtuale istantaneo su Microsoft Azure
- Risoluzione dei problemi
  - Aggiunta di una password di crittografia per una destinazione crittografata esistente
  - Configurazione del registro per il processo di copia del punto di ripristino
  - Congestione della larghezza di banda con i processi di copia del punto di ripristino su cloud
  - Errore di connessione al cloud

Informazioni sulla funzionalità di percorso UNC/NFS in UDP

Il percorso UNC/NFS è stato introdotto come nuovo tipo di nodo. Per utilizzare la funzionalità, è possibile fare riferimento alle sezioni seguenti:

- Privilegi utente per il percorso UNC/NFS in Arcserve UDP
- Aggiunta e gestione del percorso UNC/NFS
- Creazione di un piano di backup del percorso UNC/NFS
- Ripristino da un percorso UNC/NFS

Informazioni sulla funzionalità di SharePoint Online in UDP

Arcserve UDP v6.5 Aggiornamento 2 (o versioni successive) supporta l'utilizzo di un ambiente Microsoft SharePoint Online. Per utilizzare la funzionalità, è possibile fare riferimento alle sezioni seguenti:

- Prerequisiti
- Aggiunta di un nodo di SharePoint
- Gestione dei nodi di SharePoint Online
- Creazione di un piano di backup di SharePoint Online
- Ripristino dei dati di una raccolta siti di SharePoint Online

Prerequisiti

Per utilizzare Arcserve UDP 8.0 con l'ambiente Microsoft SharePoint Online, deve essere soddisfatto il prerequisito seguente:

Assicurarsi di disporre dei privilegi utente appropriati per le funzioni Arcserve UDP. Per ulteriori informazioni, consultare la sezione Privilegi dell'utente per SharePoint Online in Arcserve UDP.

Chapter 7: Utilizzo dell'amministrazione basata sui ruoli di Arcserve UDP

L'amministrazione basata sui ruoli consente agli amministratori assegnare ruoli e autorizzazioni diversi a utenti diversi per l'utilizzo della console Arcserve UDP. Ciascun ruolo può avere le proprie autorizzazioni. Un ruolo di amministratore con privilegi può creare ruoli e autorizzazioni personalizzati per gli altri utenti della console Arcserve UDP.

Tramite l'autorizzazione basata sui ruoli è possibile assegnare variabili a livello di protezione per ciascun ruolo.

La presente sezione descrive i seguenti argomenti:

Accesso alla console Gestione utenti

La pagina Gestione utenti consente di eseguire le seguenti operazioni:

- Accedere alla console di gestione degli utenti (console del servizio identità) dalla console Arcserve UDP.
- Abilitare e configurare l'autenticazione a più fattori (MFA) per tutti gli utenti.

La presente sezione descrive i seguenti argomenti:

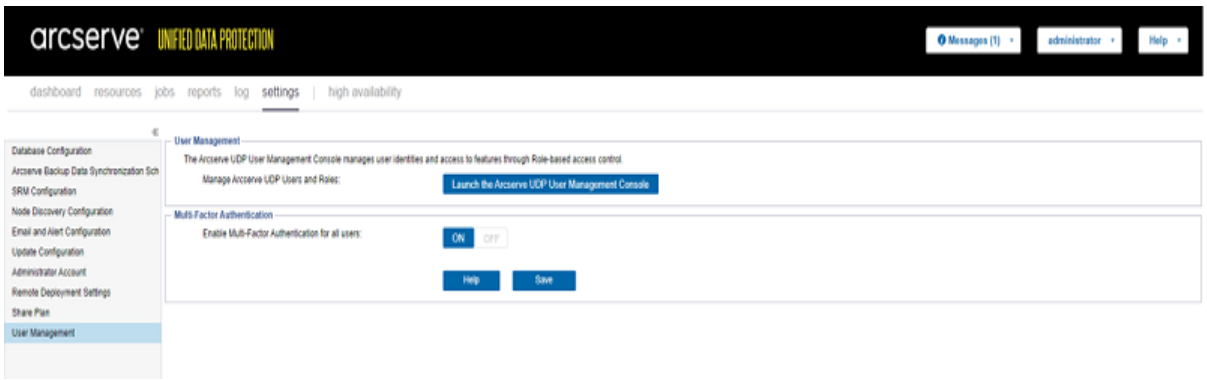
Avvio della console di gestione degli utenti Arcserve UDP

La console Gestione utenti di Arcserve UDP gestisce le identità utente e consente di controllare l'accesso alle funzionalità mediante il controllo di accesso basato sui ruoli. In questa sezione vengono fornite informazioni su come avviare la Console di gestione utenti di Arcserve UDP.

Effettuare le operazioni seguenti:

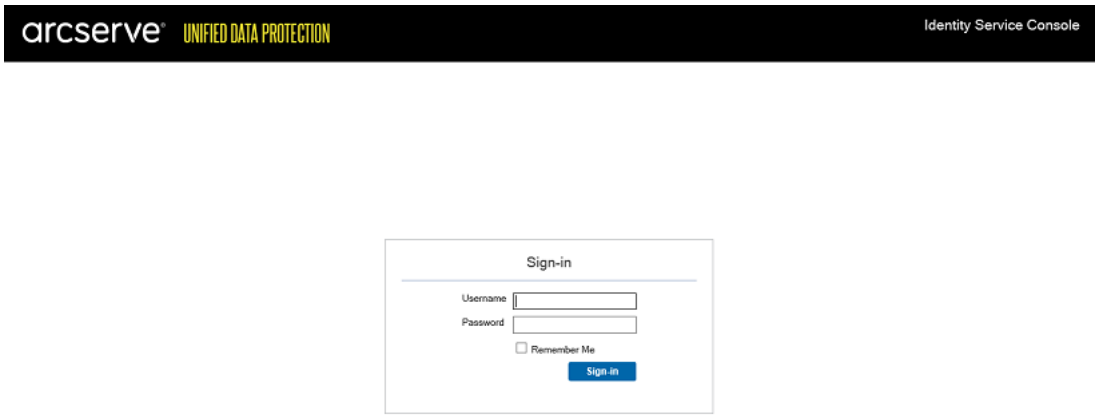
1. Accedere alla console Arcserve UDP.
2. Accedere a **Impostazioni** > **Gestione utenti**.

   Viene visualizzata la pagina Gestione utenti nel riquadro centrale.



3. Fare clic su **Avvia console Gestione utenti Arcserve UDP**.

   La console del Servizio identità viene visualizzata in una nuova finestra.



4. Specificare il nome utente e la password, quindi fare clic su **Accedi**.

   Viene visualizzata la pagina principale Console Servizio identità.

   L'accesso alla console Gestione utenti di Arcserve UDP è stato eseguito correttamente.

   In alternativa, è possibile accedere anche alla console del Servizio identità. Per effettuare l'accesso, immettere l'indirizzo nel seguente formato nella nuova finestra:

   http (o https)://(indirizzo IP o nome host): (numero porta console)/carbon

Configurazione dell'autenticazione a più fattori

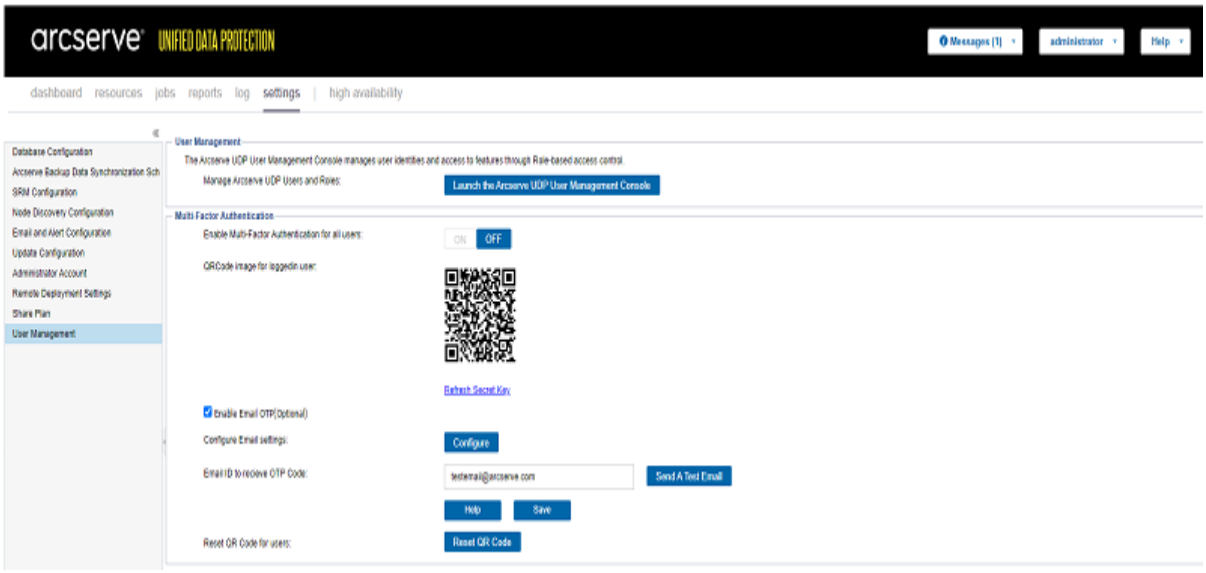
La presente sezione descrive i seguenti argomenti:

Configurazione dell'autenticazione a più fattori come utente amministratore

In questa sezione vengono fornite informazioni sulla configurazione dell'autenticazione a più fattori per tutti gli utenti.

Effettuare le operazioni seguenti:

1. Accedere alla Console Arcserve UDP utilizzando le credenziali di amministratore.
2. Accedere a **Impostazioni** > **Gestione utenti**.



3. Per attivare l'autenticazione a più fattori per tutti gli utenti, nella sezione Autenticazione a più fattori, abilitare l'impostazione su **Attivo**.

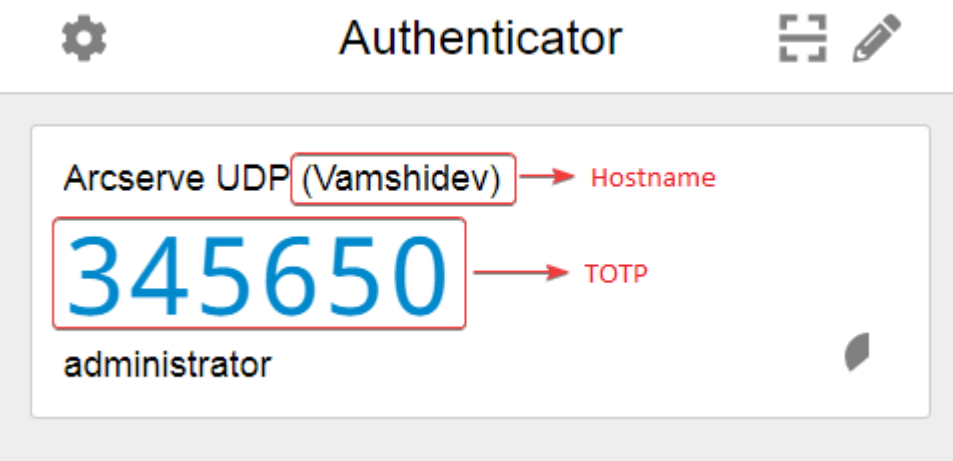
   Viene visualizzata l'immagine del codice QR per l'utente connesso.

   Nota: se si desidera disattivare l'autenticazione a più fattori per tutti gli utenti, selezionare l'impostazione **Disattiva**.

4. Per generare il TOTP, eseguire la scansione dell'immagine del codice QR utilizzando un'app di autenticazione.

   Note:

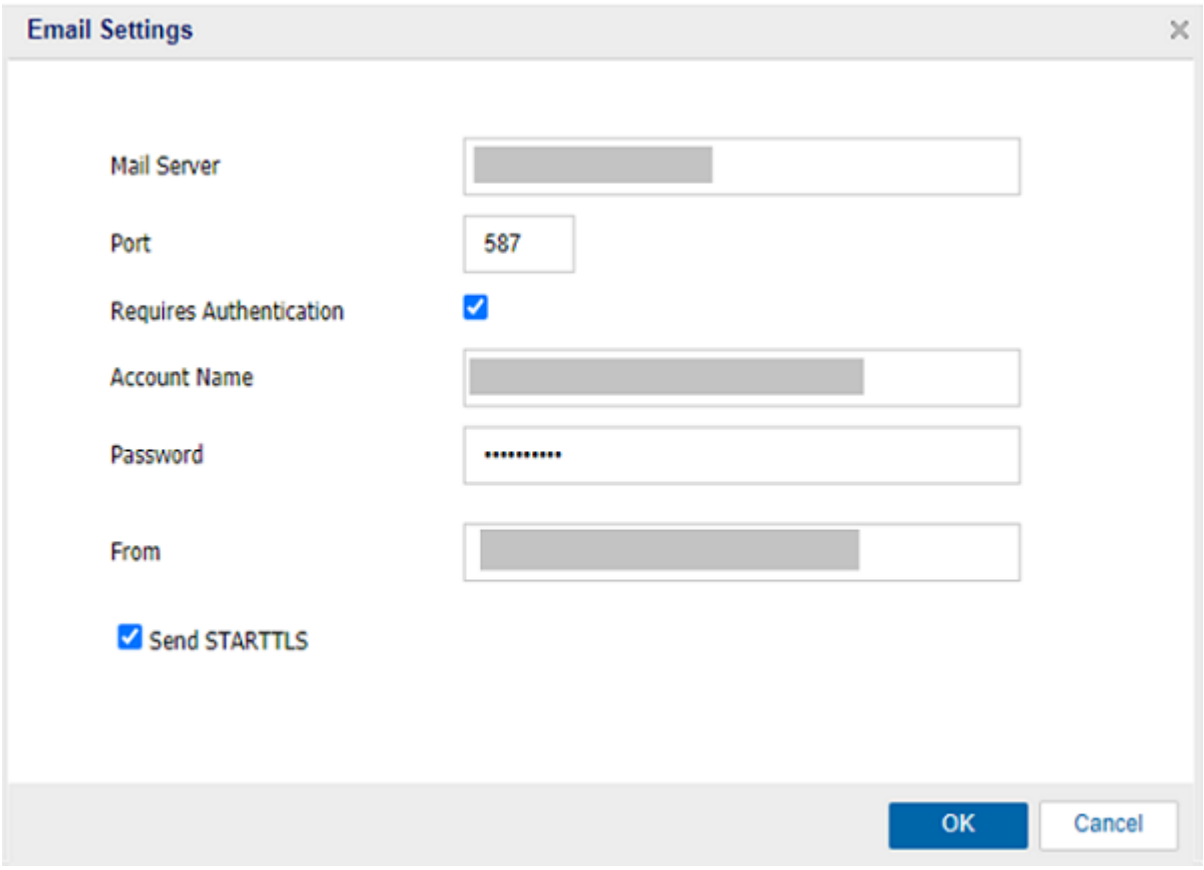
   - È possibile utilizzare qualsiasi app di autenticazione mobile, ad esempio l'app Google Authenticator o l'app Microsoft Authenticator sul proprio dispositivo mobile. In alternativa, è possibile utilizzare anche l'estensione Authenticator sul browser Chrome.
   - Per generare un nuovo TOTP, fare clic sul collegamento **Aggiorna chiave segreta** sotto l'immagine del codice QR.
   - Quando si utilizza un'app di autenticazione per più account utente, il nome host dell'account utente distingue i TOTP. Nell'app di autenticazione è possibile visualizzare il nome host e il rispettivo TOTP.



5. (Facoltativo) Se si desidera abilitare l'OTP di posta elettronica, selezionare **Attiva codice OTP di posta elettronica (Facoltativo)**, quindi procedere come segue:

    a. Per configurare le impostazioni di posta elettronica, fare clic sul pulsante **Configura**.

    Viene visualizzata la finestra di dialogo Impostazioni di posta elettronica.



b. Nella finestra di dialogo Impostazioni di posta elettronica, eseguire le seguenti operazioni, quindi fare clic su **OK**:

- **Server di posta elettronica**: immettere l'indirizzo del server di posta elettronica.
- **Porta**: immettere il numero di porta per il server di posta elettronica.
- Se il server di posta elettronica specificato richiede l'autenticazione, selezionare la casella di controllo **Richiede l'autenticazione**.
- **Nome account**: immettere il nome utente o l'indirizzo di posta elettronica del server di posta elettronica specificato.
- **Password**: immettere la password per l'autenticazione.
- **Da**: digitare l'indirizzo di posta elettronica del mittente, se necessario.
- Se il server di posta elettronica specificato richiede il comando di protocollo STARTLS, selezionare la casella di controllo **Invia STARTLS**.

c. Per l'*ID di posta elettronica per la ricezione del codice OTP*, immettere uno o più indirizzi di posta elettronica.

Nota: è necessario fornire un indirizzo di posta elettronica per ricevere l'OTP durante il processo di accesso. Se si desidera fornire più indirizzi di posta elettronica, utilizzare il punto e virgola (;) per separarli.



d. Per verificare che gli indirizzi di posta elettronica configurati stiano ricevendo OTP, fare clic su **Invia messaggio di posta elettronica di test**.

6. Fare clic su **Salva**.

   Viene visualizzata la finestra di dialogo di conferma.

   Nota: la finestra di dialogo di conferma viene visualizzata per riavviare il Servizio identità solo quando si configurano, modificano o rimuovono le impostazioni di posta elettronica.

7. Nella finestra di dialogo Conferma, per riavviare il Servizio identità, fare clic su **Sì**.

   Dopo aver riavviato il Servizio identità, aggiornare il browser. Questa operazione è necessaria per applicare le impostazioni di posta elettronica.

Per reimpostare il codice QR, consultare la sezione Reimpostazione del codice QR.

Come reimpostare il codice QR

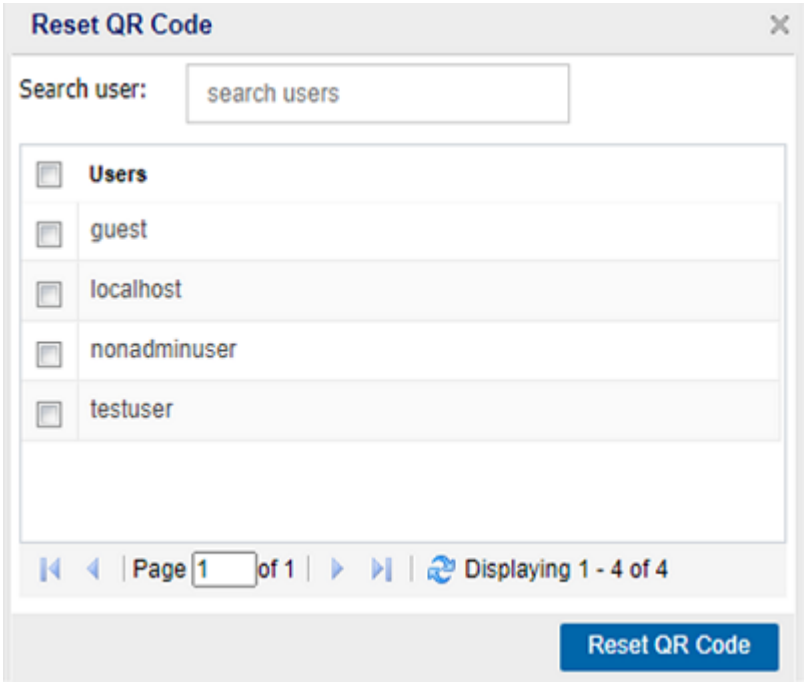
Questa sezione fornisce informazioni sulla reimpostazione del codice QR per gli utenti.

Nota: un utente amministratore può reimpostare il codice QR per tutti gli utenti ad eccezione del proprio.

Effettuare le operazioni seguenti:

1. Accedere alla Console Arcserve UDP utilizzando le credenziali di amministratore.
2. Accedere a **Impostazioni** > **Gestione utenti**.
3. Per *reimpostare il codice QR per gli utenti*, fare clic sul pulsante **Reimposta codice QR**.

Viene visualizzata la finestra di dialogo Reimposta codice QR.



4. Nella finestra di dialogo Reimposta codice QR, dall'elenco degli utenti, selezionare gli utenti per i quali si desidera reimpostare il codice QR, quindi fare clic su **Reimposta codice QR**.

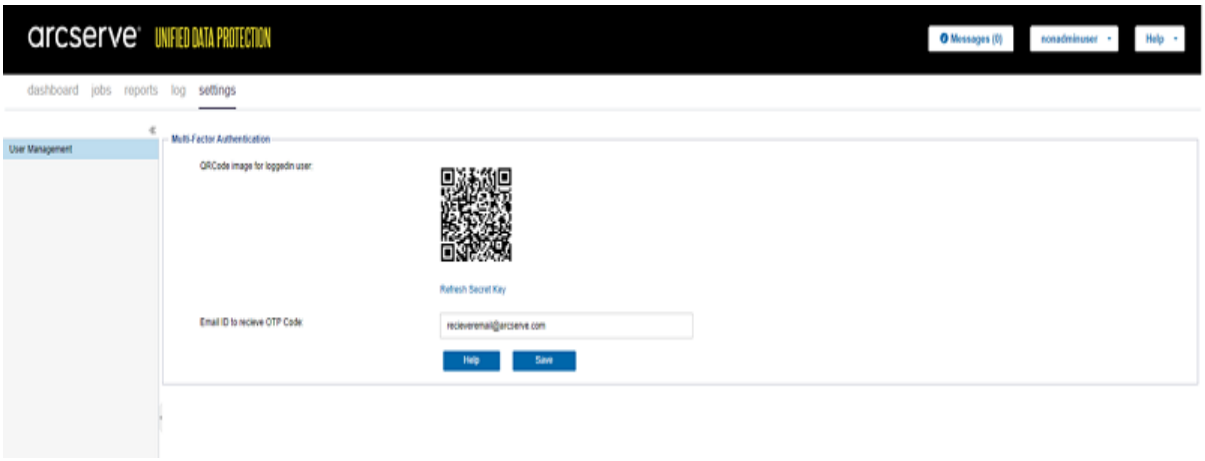
Nota: dopo aver reimpostato il codice QR, all'accesso successivo gli utenti selezionati dovranno eseguire nuovamente la scansione del codice QR per ottenere un nuovo TOPT e registrarsi nuovamente.

Configurazione dell'autenticazione a più fattori come utente non amministratore

In questa sezione vengono fornite informazioni su come configurare le impostazioni di autenticazione a più fattori per il proprio profilo utente.

Effettuare le operazioni seguenti:

1. Accedere alla console Arcserve UDP utilizzando le credenziali non di amministratore.
2. Accedere a **Impostazioni** > **Gestione utenti**.



Nota: la pagina *Impostazioni > Gestione utenti* non è disponibile per gli utenti che non dispongono dell'autorizzazione Gestione utenti. Tuttavia, l'amministratore può assegnare questa autorizzazione a tutti gli utenti non amministratori. Per ulteriori informazioni, vedere Assegnazione di ruoli predefiniti.

3. Per generare un nuovo TOTP, fare clic sul collegamento **Aggiorna chiave segreta** sotto l'immagine del codice QR.
4. Per l'*ID di posta elettronica per la ricezione del codice OTP*, immettere uno o più indirizzi di posta elettronica.

   Nota: è necessario fornire un indirizzo di posta elettronica per ricevere l'OTP durante il processo di accesso. Se si desidera fornire più indirizzi di posta elettronica, utilizzare il punto e virgola (;) per separarli.



5. Fare clic su **Salva**.

   Verrà effettuato il salvataggio delle nuove impostazioni.

Aggiunta di un utente, eliminazione di un utente e modifica della password

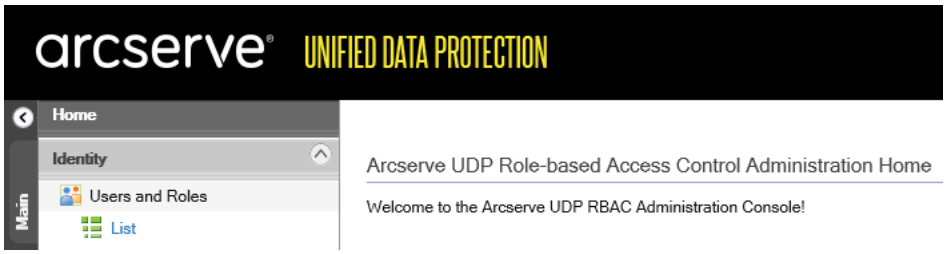
È possibile aggiungere o eliminare gli utenti locali o di dominio dal controllo utente di Windows. L'elenco di gestione degli utenti della console Server di identità viene aggiornato immediatamente.

Utilizzare il controllo utente di Windows per modificare la password dell'utente. Quando si aggiorna la password dell'utente, l'utente deve effettuare l'accesso alla console Server di identità con la password più recente. Il ruolo dell'utente viene conservato.

Configurazione della Gestione utenti

È possibile assegnare ruoli diversi a utenti diversi e fornire autorizzazioni diverse a ruoli diversi. Configurare la gestione utenti per poter completare le seguenti operazioni:

- Ruoli predefiniti
- Assegnazione di ruoli predefiniti
- Visualizzazione e annullamento di un ruolo
- Aggiunta di un nuovo ruolo
- Ricerca di utenti e ruoli

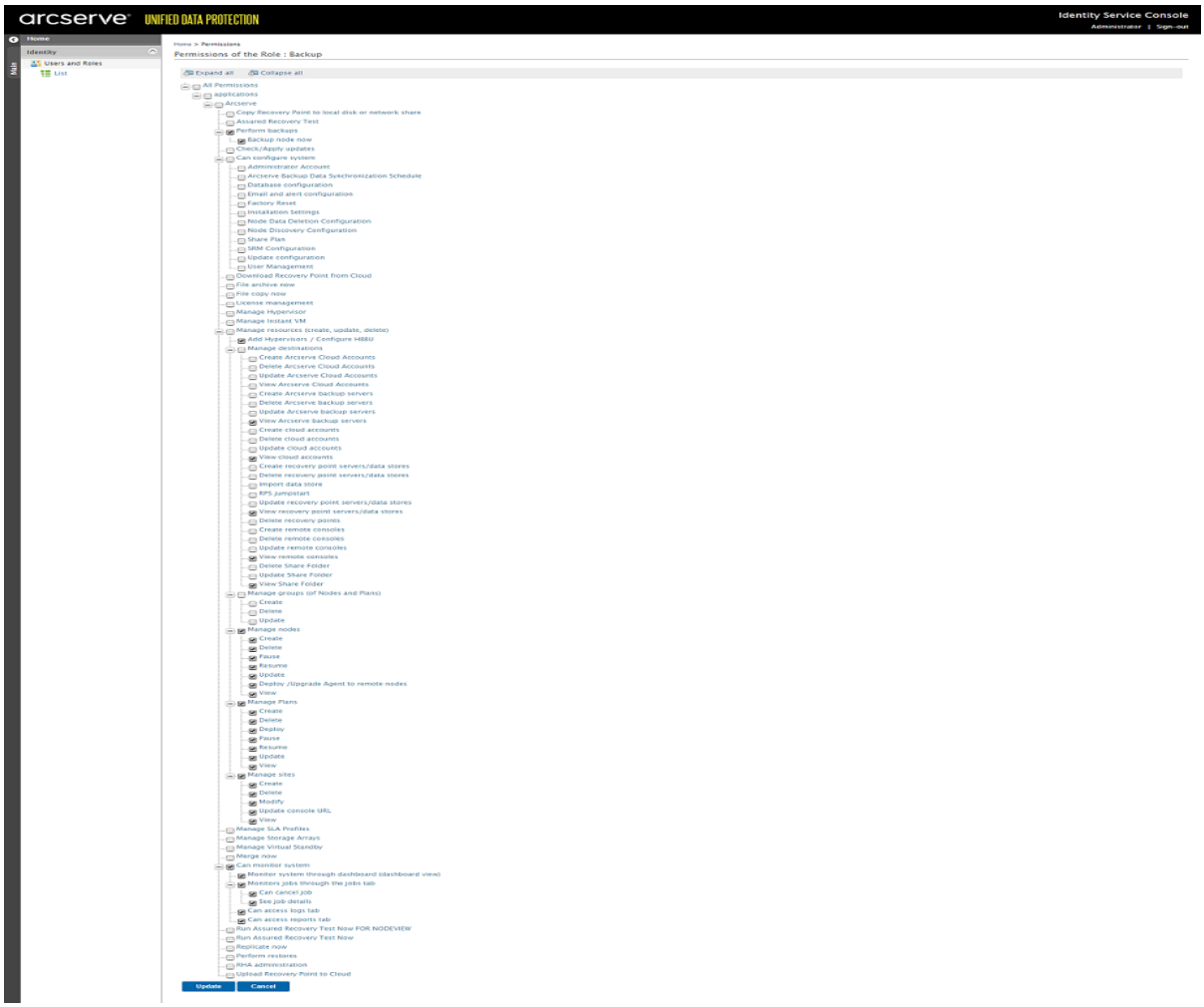


Ruoli predefiniti

I ruoli predefiniti servono da riferimento per la definizione di alcuni ruoli tipici. Ogni ruolo prevede un insieme predefinito di autorizzazioni assegnate.

Per il ruolo di amministratore sono selezionate tutte le opzioni di autorizzazione. Gli utenti con ruolo di amministratore possono accedere a tutte le funzioni di Arcserve UDP.

Fare clic sull'autorizzazione per il ruolo di backup per visualizzare le autorizzazioni predefinite selezionate.


arcserve
UNIFIED DATA PROTECTION
Identity Service Console
Administrator | Sign-out
Home
Identity
Users and Roles
List
Main
Home > Permissions
Permissions of the Role : Backup
Expand all
Collapse all
All Permissions
applications
Arcserve
Copy Recovery Point to local disk or network share
Assured Recovery Test
Perform backups
Backup node now
Check/Apply updates
Can configure system
Administrator Account
Arcserve Backup Data Synchronization Schedule
Database configuration
Email and alert configuration
Factory Reset
Installation Settings
Node Data Deletion Configuration
Node Discovery Configuration
Share Plan
SRM Configuration
Update configuration
User Management
Download Recovery Point from Cloud
File archive now
File copy now
License management
Manage Hypervisor
Manage Instant VM
Manage resources (create, update, delete)
Add Hypervisors / Configure HBBU
Manage destinations
Create Arcserve Cloud Accounts
Delete Arcserve Cloud Accounts
Update Arcserve Cloud Accounts
View Arcserve Cloud Accounts
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
Create recovery point servers/data stores
Delete recovery point servers/data stores
Import data store
RPS jumpstart
Update recovery point servers/data stores
View recovery point servers/data stores
Delete recovery points
Create remote consoles
Delete remote consoles
Update remote consoles
View remote consoles
Delete Share Folder
Update Share Folder
View Share Folder
Manage groups (of Nodes and Plans)
Create
Delete
Update
Manage nodes
Create
Delete
Pause
Resume
Update
Deploy /Upgrade Agent to remote nodes
View
Manage Plans
Create
Delete
Deploy
Pause
Resume
Update
View
Manage sites
Create
Delete
Modify
Update console URL
View
Manage SLA Profiles
Manage Storage Arrays
Manage Virtual Standby
Merge now
Can monitor system
Monitor system through dashboard (dashboard view)
Monitors jobs through the jobs tab
Can cancel job
See job details
Can access logs tab
Can access reports tab
Run Assured Recovery Test Now FOR NODEVIEW
Run Assured Recovery Test Now
Replicate now
Perform restores
RHA administration
Upload Recovery Point to Cloud
Update
Cancel

Le autorizzazioni seguenti sono predefinite per il ruolo di backup:

- Esecuzione del backup
- Visualizzazione della destinazione
- Gestione di nodi, piano, siti
- Monitoraggio del funzionamento di sistema

Gli utenti con ruolo di amministratore possono deselezionare le autorizzazioni selezionate o selezionarne altre. Facendo clic sull'opzione di aggiornamento, l'autorizzazione appena aggiunta diventa quella predefinita per il ruolo di backup. È inoltre possibile rinominare il ruolo.

Per il ruolo di monitoraggio, vengono preselezionate le autorizzazioni di monitoraggio e registrazione/segnalazione del processo del dashboard.



Per il ruolo di ripristino, sono preselezionate le autorizzazioni seguenti:

- Gestione del computer virtuale istantaneo
- Visualizzazione della destinazione
- Visualizzazione del nodo
- Visualizzazione del piano
- Gestione Virtual Standby
- Monitoraggio dei processi
- Accesso ai registri
- Esecuzione del ripristino

Se si assegna il ruolo di ripristino a un utente, questo può accedere e disporre delle autorizzazioni corrispondenti. Ad esempio, se un utente svolge il ruolo di ripristino e si completa il backup di un nodo, è possibile creare un computer virtuale istantaneo o eseguire il ripristino per passare all'attività successiva.



Per il ruolo di _Admin, le autorizzazioni di amministrazione RHA permettono l'accesso alla funzione High Availability.

Assegnazione di ruoli predefiniti

Quando un amministratore con privilegi assegna un ruolo a un utente, soltanto tale utente potrà accedere alla console. Il pulsante Utenti mostra l'elenco completo degli utenti, compresi gli utenti di dominio e gli utenti locali.

È possibile assegnare i ruoli (predefiniti) disponibili o auto-definiti a qualsiasi utente locale o di dominio.

Nota: Soltanto un amministratore con privilegi (l'amministratore che esegue l'installazione di Arcserve UDP) può assegnare il ruolo di amministratore agli altri utenti. Gli amministratori possono assegnare soltanto i ruoli non di amministratore agli altri utenti.

Effettuare le operazioni seguenti:

1. Fare clic su **Utenti e ruoli** dal riquadro **Configura**.

   Gli utenti e i ruoli vengono visualizzati nella pagina Gestione utenti.

2. Fare clic su **Utenti** dalla pagina Gestione utenti.

   Viene visualizzato l'elenco degli utenti.

3. Fare clic su **Assegna ruolo** per un utente.

   Viene visualizzata la pagina **Elenco ruoli dell'utente**.

4. Selezionare uno o più ruoli e fare clic su **Aggiorna**.

   Il ruolo per l'utente è stato aggiornato correttamente.

5. Fare clic su **Fine** per tornare alla schermata precedente.

   Il ruolo è stato assegnato correttamente all'utente.

Visualizzazione e annullamento di un ruolo

È possibile visualizzare il ruolo corrente a cui è assegnato a un utente. È possibile annullare un ruolo assegnato deselezionando la casella di controllo per tale ruolo.

Effettuare le operazioni seguenti:

1. Fare clic su **Utenti e ruoli** dal riquadro **Configura**.

   Gli utenti e i ruoli vengono visualizzati nella pagina **Gestione utenti**.

2. Dalla pagina Gestione utenti, fare clic su Utenti.

   Viene visualizzato l'elenco degli utenti.

3. Deselezionare la casella di controllo per annullare un ruolo e fare clic su **Aggiorna**.

   I ruoli vengono rimossi dall'utente.

   Nota: Se non è stato assegnato alcun ruolo, un utente non può accedere alla Console Arcserve UDP.

4. Fare clic su **Fine** per accedere alla pagina precedente.

   Il ruolo viene visualizzato e annullato correttamente.

Aggiunta di un nuovo ruolo

È possibile creare un ruolo personalizzato e selezionare le autorizzazioni correlate.

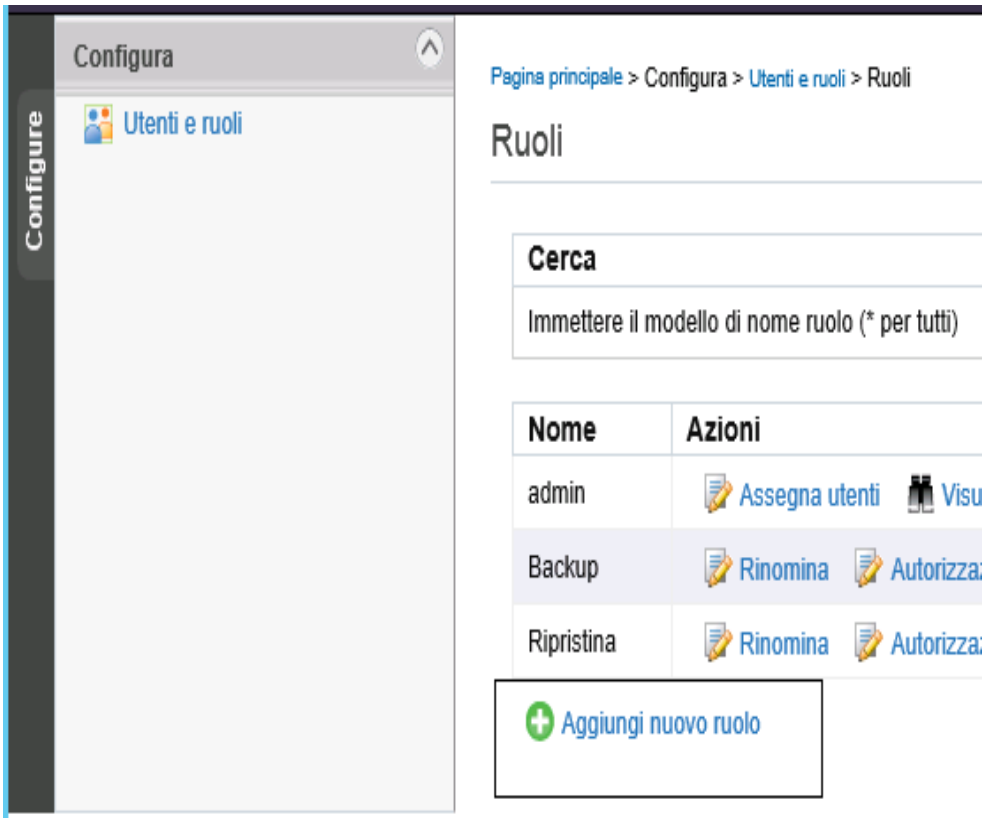
Effettuare le operazioni seguenti:

1. Fare clic su **Utenti e ruoli** dalla pagina **Configura**.

   Gli utenti e i ruoli vengono visualizzati nella pagina **Gestione utenti**.

2. Fare clic su **Ruoli**.

   Viene visualizzata la pagina **Ruoli** con l'elenco di tutti i ruoli disponibili.



3. Fare clic su **Aggiungi nuovo ruolo**.

   Viene visualizzata la pagina **Aggiungi ruolo**.

4. Immettere il nome del ruolo e fare clic su **Avanti**.

   Nota: Non utilizzare caratteri speciali come **~!@#$%^&*** e altri nel nome di un ruolo.

5. Selezionare le caselle di controllo relative alle autorizzazioni richieste e fare clic su **Avanti**.

6. Selezionare gli utenti per questo ruolo.

7. Fare clic su **Fine**.

Un nuovo ruolo è stato creato e le autorizzazioni correlate sono state assegnate.

Nota: Alcune autorizzazioni funzionano solo quando vengono selezionate anche le autorizzazioni correlate. Ad esempio, per configurare un ruolo per la gestione di Virtual Standby, per assicurarsi che quest'ultimo funzioni normalmente, selezionare l'autorizzazione per la gestione di Virtual Standby e quella per la visualizzazione del nodo.

Ricerca di utenti e ruoli

È possibile filtrare gli utenti e i ruoli per individuare l'utente o il ruolo richiesti. Immettere * per la ricerca di tutti gli utenti e di tutti i ruoli.

Per cercare un ruolo, attenersi alle seguenti istruzioni:

1. Fare clic su **Utenti e ruoli** dalla pagina **Configura**.

   Gli utenti e i ruoli vengono visualizzati nella pagina **Gestione utenti**.

2. Fare clic su **Ruoli**.

   Viene visualizzata la pagina **Ruoli**.



3. Specificare il modello del nome del ruolo e fare clic su **Cerca**.

   Viene visualizzato il risultato filtrato.

Per cercare un utente, attenersi alle seguenti istruzioni:

1. Fare clic su **Utenti e ruoli** dalla pagina **Configura**.

   Gli utenti e i ruoli vengono visualizzati nella pagina **Gestione utenti**.

2. Fare clic su **Utenti**.

   Viene visualizzata la pagina **Utenti**.

3. Specificare il modello del nome dell'utente e fare clic su **Cerca**.

   Viene visualizzato il risultato filtrato.

Integrazione di Arcserve UDP con Active Directory

Arcserve UDP supporta l'integrazione di Active Directory (AD) mediante i gruppi Windows e AD.

La presente sezione descrive i seguenti argomenti:

- Integrazione di Arcserve UDP 8.0 con Active Directory mediante i gruppi Windows
- Integrazione di Arcserve UDP 8.0 con Active Directory mediante i gruppi Active Directory

Integrazione di Arcserve UDP 8.0 con Active Directory mediante i gruppi di Windows

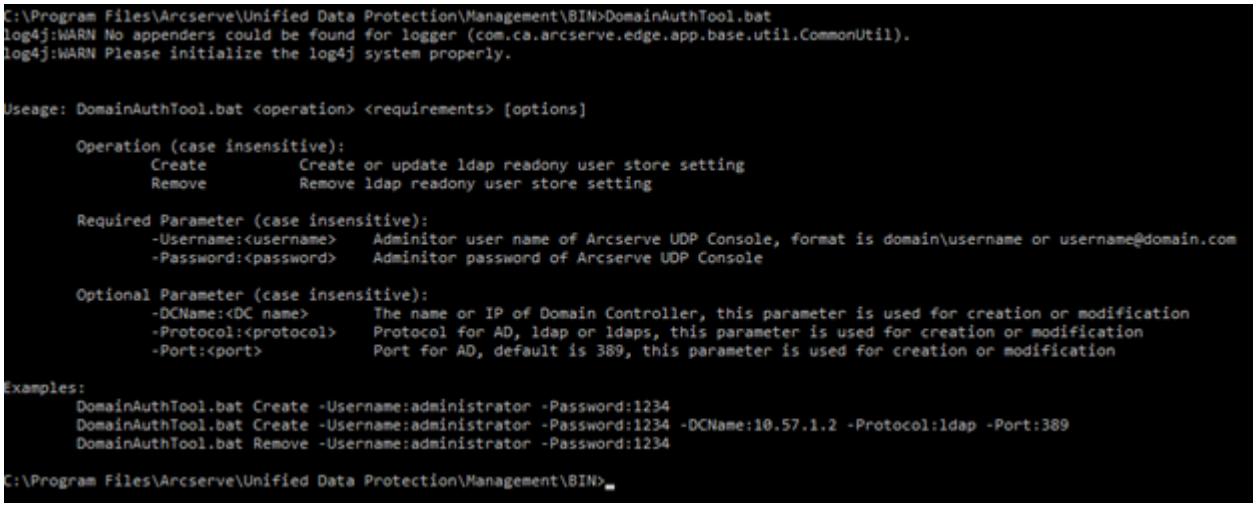
La funzionalità esistente di amministrazione basata sui ruoli (UDP-RBA) consente di gestire le autorizzazioni UDP in base a gruppi Active Directory (AD). Nella versione precedente di UDP-RBA, erano supportati solo account utente AD singoli. Adesso, i gruppi Active Directory possono fungere da ruoli RBA.

L'archivio utenti secondario in modalità di sola lettura di LDAP viene aggiunto automaticamente eseguendo un'utilità.

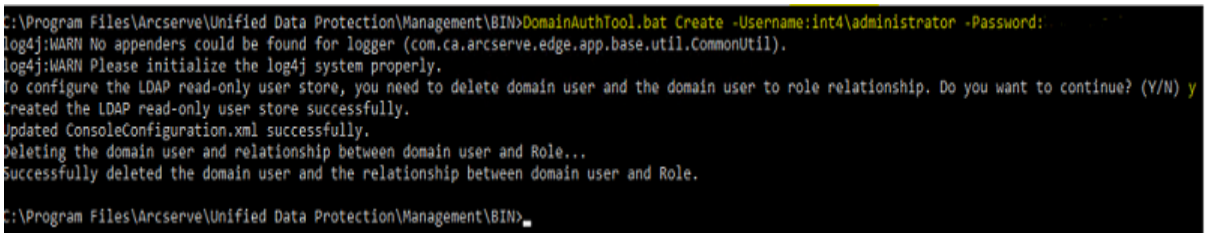
Effettuare le operazioni seguenti:

1. Avviare il prompt dei comandi ed eseguire *C:\Programmi\Arcserve\Unified dati Protection\Management\BIN*.
2. Eseguire l'utilità *DomainAuthTool.bat*.

   Sullo schermo vengono visualizzate le seguenti informazioni:



3. Creare un archivio utenti secondario in modalità di sola lettura di LDAP e contemporaneamente modificare i parametri facoltativi. Ad esempio: fare riferimento al comando giallo nella figura riportata di seguito.



4. Assegnare il ruolo di utente locale.

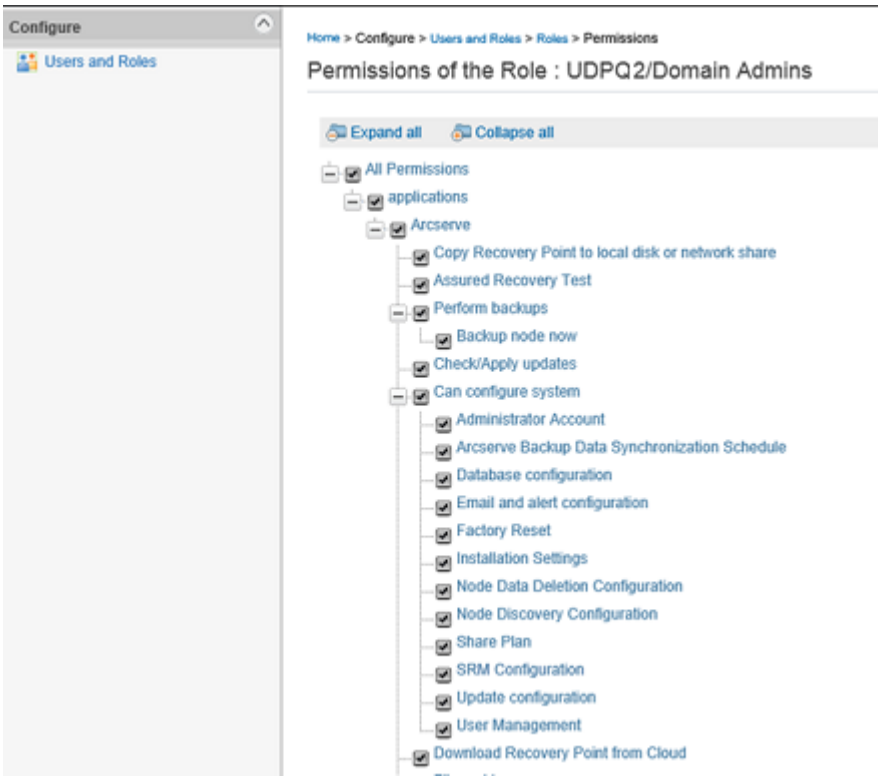
Per ulteriori informazioni, vedere Assegnazione di ruoli predefiniti.

5. Per aggiungere autorizzazioni per gli utenti di dominio in modalità di sola lettura di LDAP, effettuare le seguenti operazioni:

   a. Partecipare al gruppo dal Controller di dominio.

   b. Aggiungere l'autorizzazione Arcserve UDP per il gruppo corrispondente come visualizzato nella schermata riportata di seguito.

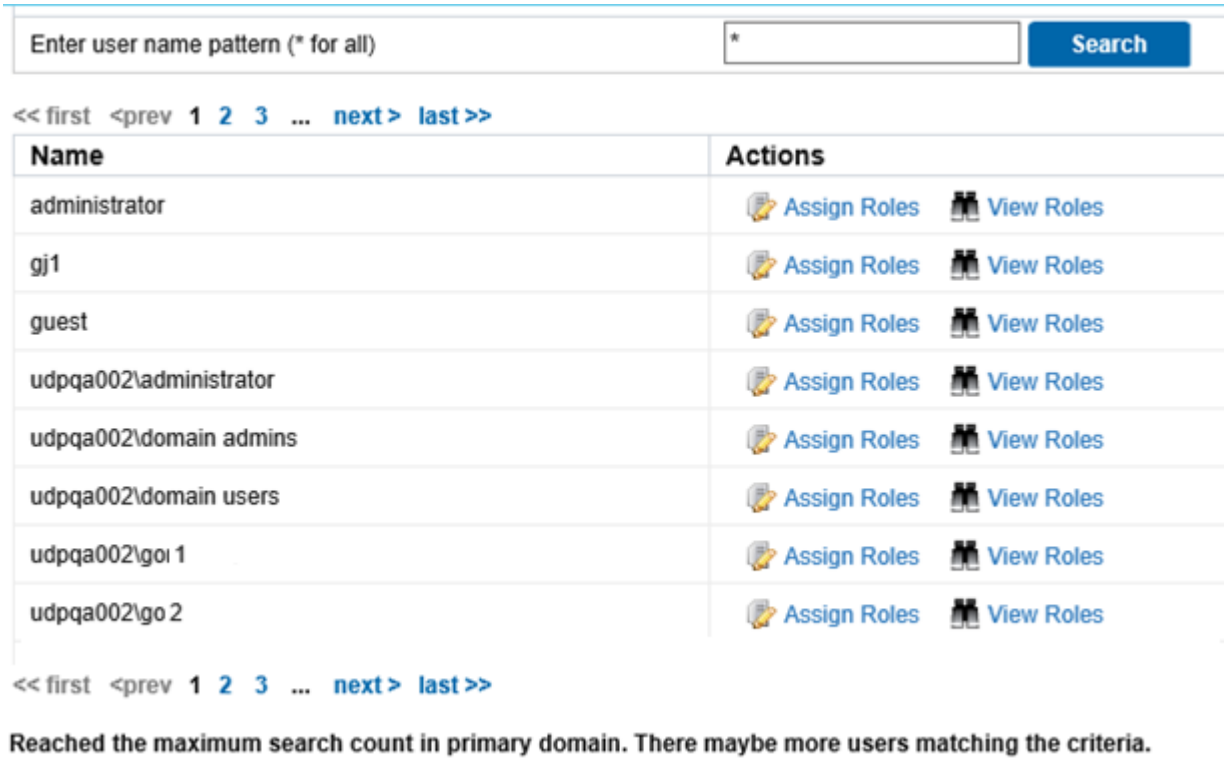
   Nota: Non è possibile assegnare il ruolo predefinito locale direttamente agli utenti del dominio in modalità di sola lettura.



   L'utente può ora accedere alla console Arcserve UDP con autorizzazioni specifiche.

6. (Facoltativo) Rimuovere l'archivio utenti di LDAP con l'utilità.

   Eseguire l'utilità per rimuovere l'archivio utenti di LDAP. Quindi, riavviare il servizio di gestione: l'utente del dominio precedente viene elencato come mostrato di seguito.


Enter user name pattern (* for all)
*
Search
<< first <prev 1 2 3 ... next > last >>
Name
Actions
administrator
gj1
guest
udpqa002\administrator
udpqa002\domain admins
udpqa002\domain users
udpqa002\go 1
udpqa002\go 2
Assign Roles
View Roles
<< first <prev 1 2 3 ... next > last >>
Reached the maximum search count in primary domain. There maybe more users matching the criteria.

Integrazione di Arcserve UDP 8.0 con Active Directory mediante i gruppi di Active Directory

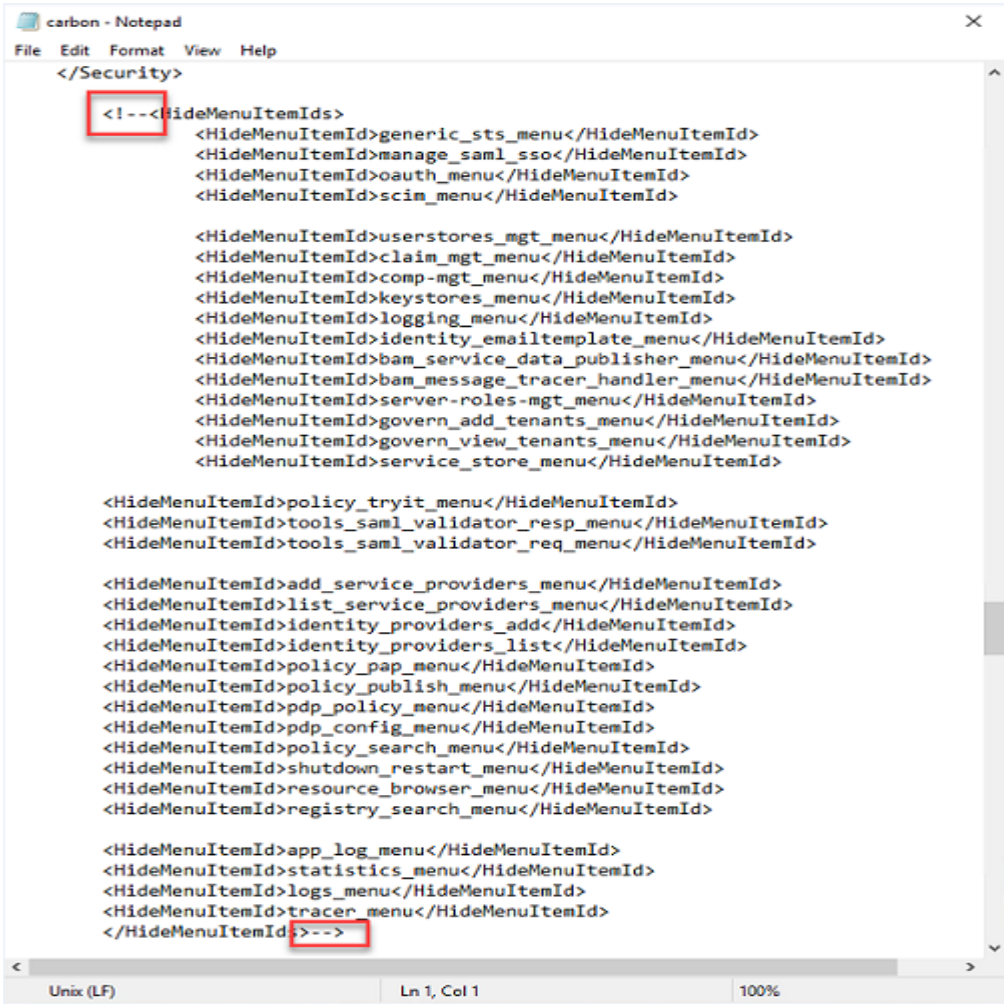
L'amministrazione basata sui ruoli di Arcserve UDP 8.0 consente l'autorizzazione a livello di utente in cui la funzionalità Active Directory (AD) non è abilitata per impostazione predefinita. Tuttavia, la piattaforma WSO2 Carbon in Arcserve UDP 8.0 non supporta i gruppi di AD che dispongono di un archivio utenti secondario. È possibile abilitare l'estensione per Arcserve UDP 8.0 per configurare i gruppi AD come ruoli di Arcserve UDP e consentire l'assegnazione automatica delle autorizzazioni per i membri del gruppo AD.

Effettuare le operazioni seguenti:

1. Accedere al percorso di installazione seguente Arcserve UDP e aprire il file *carbon.xml*:

   …\Programmi\Arcserve\Unified Data Protection\Management\IdentityServer\repository\conf\carbon.xml

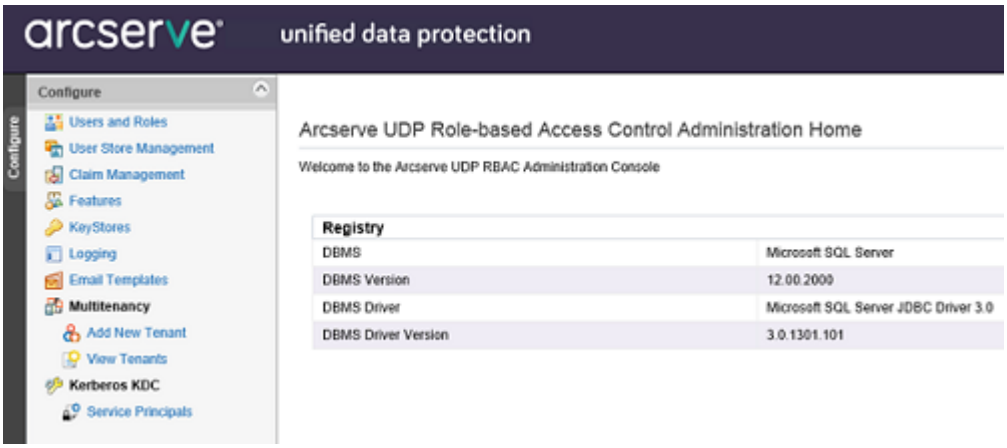
2. Dal file *carbon.xml*, disattivare il contenuto di HideMenuItemIds utilizzando <!-- e -->, come illustrato nella schermata successiva.



3. Salvare il file *carbon.xml* e riavviare il servizio di Gestione di Arcserve UDP.
4. Aprire la Console di gestione degli utenti tramite il collegamento seguente:

   https://localhost:8015/carbon

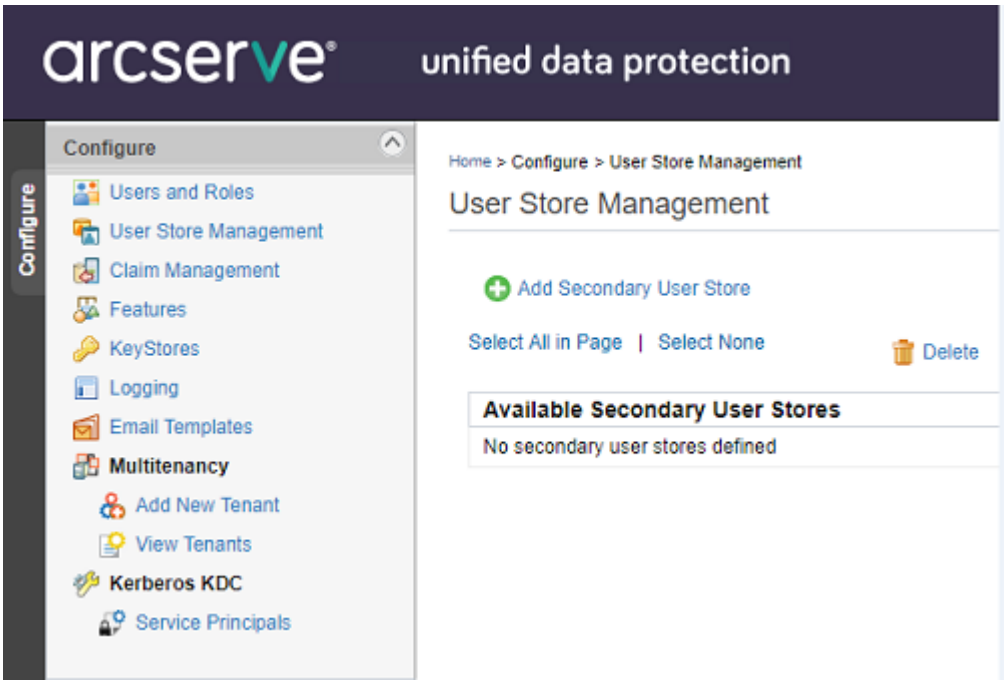
   Viene visualizzata la pagina iniziale di *Arcserve UDP*Amministrazione del controllo degli accessi basato sui ruoli di .



5. Fare clic sull'opzione **Gestione archivio utenti** disponibile nel riquadro sinistro.

   Viene visualizzata la pagina **Gestione archivio utenti**.

6. Fare clic su **Aggiungi archivio utenti secondario**.

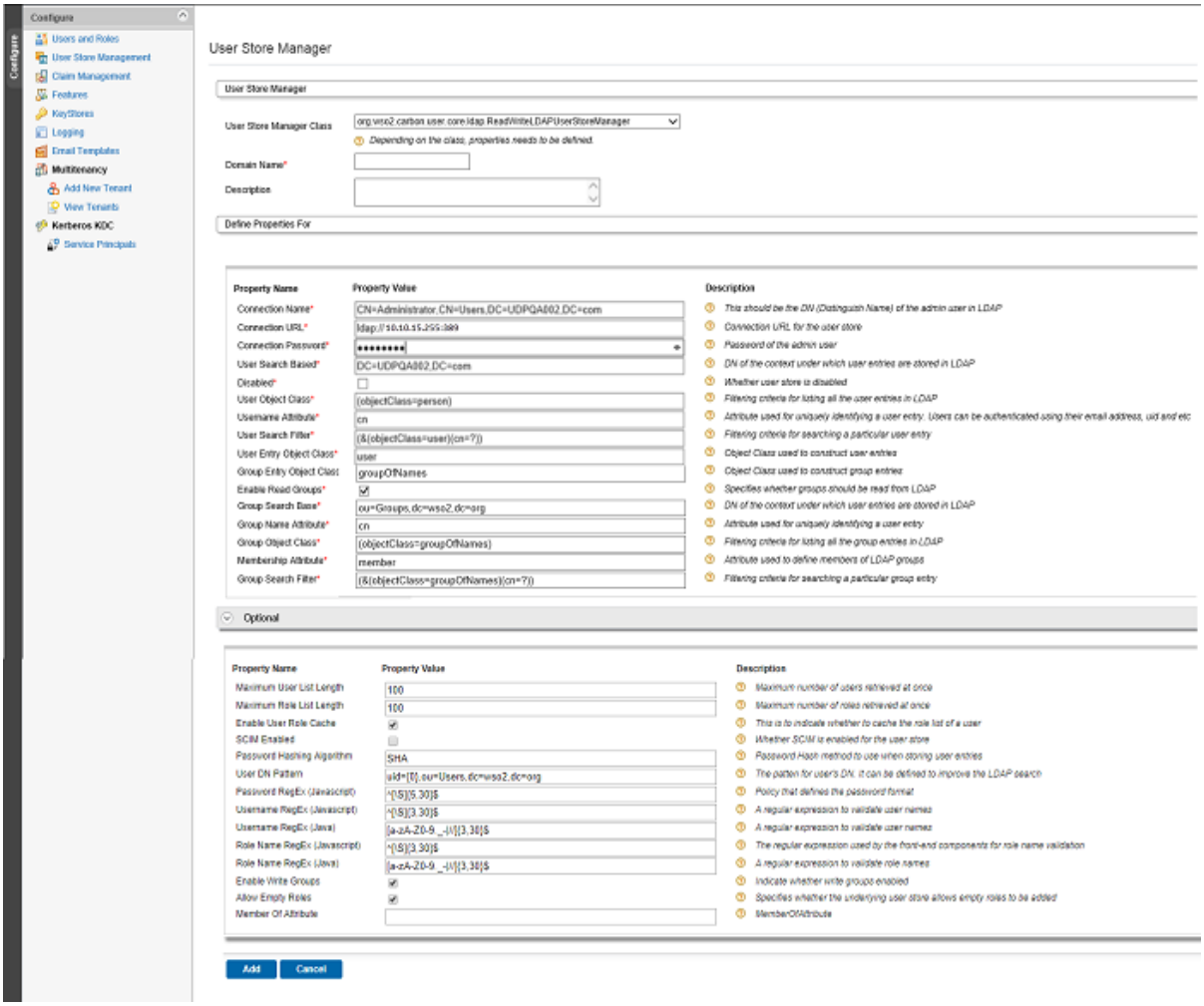


   Viene visualizzata la pagina **Gestione archivio utenti**.

7. Selezionare l'opzione **Classe della Gestione archivio utenti** dall'elenco a discesa e immettere il nome di dominio nel campo **Nome dominio**.

8. Immettere i dettagli nei campi obbligatori nei gruppi **Definisci proprietà per** e **Facoltativo**.

Nella schermata seguente è riportato un esempio di pagina della Gestione archivio utenti dopo aver immesso i dettagli.



9. Fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo **Gestione utenti UDP**.

10. Fare clic su **OK**.

    Verrà visualizzata la pagina Gestione archivio utenti contenente l'archivio utenti secondario aggiunto.



Nota: se l'archivio utenti secondario non viene visualizzato, aggiornare il browser.

11. (Facoltativo) Fare clic sull'opzione **Utenti e ruoli** dal riquadro sinistro per visualizzare l'elenco di utenti e ruoli.

    Nota: è necessario definire i ruoli nel dominio utilizzando Active Directory.

12. A questo punto, procedere come segue per aggiungere le autorizzazioni del ruolo UDP:

    a. Selezionare un utente Active Directory o un gruppo Active Directory.

    b. Assegnare un ruolo dall'elenco di ruoli disponibili.

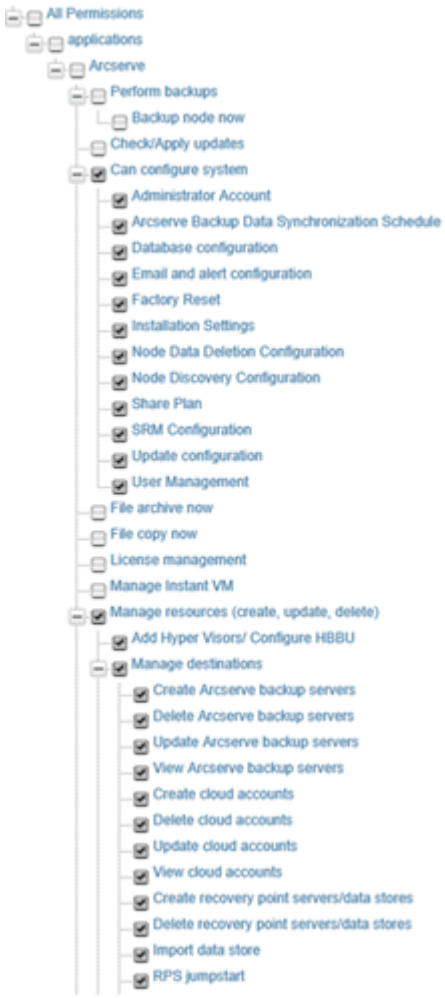
    c. Fare clic su **Visualizza ruolo**.

    Viene visualizzata la pagina **Elenco ruoli dell'utente**.



    d. Fare clic su **Autorizzazioni**.

    Viene visualizzato l'elenco delle autorizzazioni.



e. Selezionare le autorizzazioni necessarie.

L'utente secondario può ora accedere alla Console Arcserve UDP con le autorizzazioni assegnate.

Accesso a Arcserve UDP tramite l'autenticazione integrata di Windows

Gli utenti di Arcserve UDP possono ora effettuare l'accesso tramite l'autenticazione integrata di Windows (IWA). IWA facilita le operazioni di accesso basate su browser. Se l'autenticazione viene eseguita una volta, IWA consente al browser Web di salvare le credenziali dell'utente che esegue l'accesso tramite Windows. Sarà necessario immettere soltanto l'URL dell'applicazione Web protetta nel browser. Il browser e il server eseguono l'autenticazione e l'utente viene connesso automaticamente.

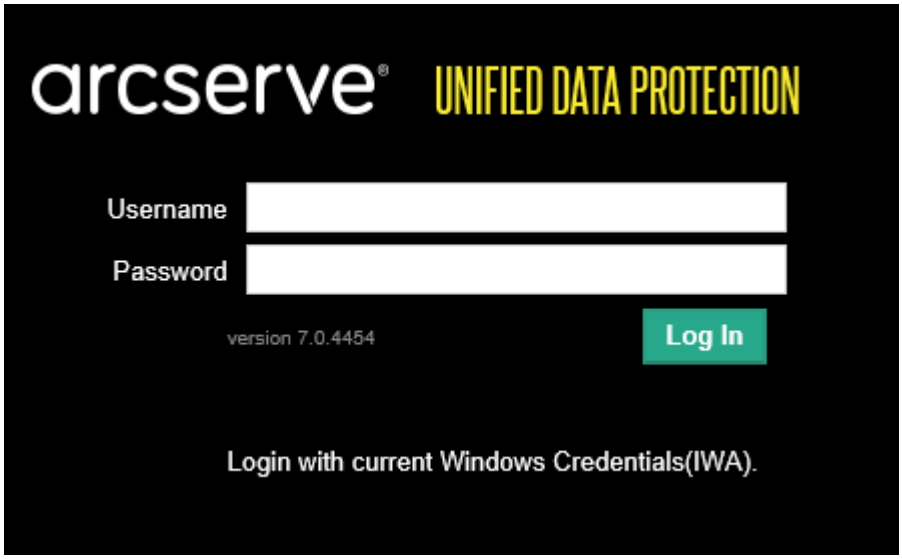
Nota: Autenticazione integrata di Windows non supportata dalla Console Arcserve UDP se la connessione al database della Console utilizza la modalità di autenticazione di Windows. Per risolvere il problema, visualizzare il collegamento di risoluzione dei problemi.

Con l'introduzione di IWA, è possibile utilizzare la stessa funzionalità e accedere a Arcserve UDP.

Effettuare le operazioni seguenti:

1. Aprire la pagina di accesso alla Console Arcserve UDP.

   Il collegamento a IWA è visibile nella pagina di accesso.



2. Fare clic sul collegamento: **Accedere con le credenziali correnti di Windows (IWA)**.

   L'utente viene indirizzato alla pagina principale.

   Per risolvere eventuali problemi, consultare la Risoluzione dei problemi.

Risoluzione dei problemi relativi all'autenticazione integrata di Windows (IWA)

Se il collegamento IWA non riesce ad aprire la pagina della Console, è possibile adottare la seguente procedura per risolvere il problema:

1. Verificare che sia in uso IWA sul computer locale invece che sul computer remoto.
2. Se dopo aver fatto clic sul collegamento IWA viene visualizzata una schermata bianca, verificare che l'utente venga assegnato al ruolo nella Console di amministrazione di RBAC.

   Nota: Se la connessione al database della console utilizza la modalità di autenticazione di Windows, fare riferimento al seguente collegamento.
3. Configurare la procedura indicata di seguito se si verifica un problema durante l'accesso con IWA utilizzando Firefox per aprire l'URL console.

   Effettuare le operazioni seguenti:

   a. Nel campo Posizione del browser, immettere about:config.

   b. Fare clic su **Starò attento, lo prometto!** per continuare nella pagina about:config.

   c. Impostare i valori delle opzioni seguenti in modo che il browser ritenga attendibile il dispositivo ProxySG e negozi l'autenticazione:

      network.automatic-ntlm-auth.trusted-uris, network.negotiate.auth.delegation-uris, network.negotiate-auth.trusted-uris

      Per ogni opzione, completare i passaggi seguenti:

      - Individuare l'opzione da impostare scorrendo o inserendo il nome dell'opzione nel campo Filtro.
      - Fare doppio clic sull'opzione per aprire la finestra di dialogo Immetti valore stringa.
      - Immettere l'URL virtuale per le distribuzioni note.

        Se si dispone di più dispositivi ProxySG che richiedono le credenziali di autenticazione, separare le voci con una virgola. Ad esempio, se l'URL aperto per la console è https://localhost:8015, è possibile immettere localhost come valore della stringa o http-

s://10.57.60.9:8015, quindi immettere 10.57.60.9 come valore della stringa.

- Fare clic su **OK**.

4. Usando Internet Explorer per aprire una Console con IWA sul computer remoto le cui credenziali Windows uguali a quelle del computer locale installate da UDP, potrebbe essere necessario utilizzare la seguente procedura:
   a. Selezionare Strumenti > Opzioni Internet.
   b. Selezionare la scheda Protezione.
   c. Selezionare l'area intranet locale e fare clic su Siti > **Avanzate**.
   d. Immettere il nome di dominio completo del dispositivo ProxySG (per le distribuzioni esplicite) o l'URL virtuale (per le distribuzioni trasparenti) nel campo Aggiungi il sito Web all'area e quindi fare clic su Aggiungi > Chiudi > OK.
   e. Selezionare la scheda Avanzate e assicurarsi che sia selezionata l'opzione Sicurezza > Abilita autenticazione di Windows integrata.
   f. Fare clic su **OK** per salvare le modifiche e chiudere la finestra di dialogo Opzioni Internet.

Autenticazione integrata di Windows non supportata dalla Console Arcserve UDP se la connessione al database della Console utilizza la modalità di autenticazione di Windows

Per utilizzare l'autenticazione integrata di Windows (IWA) è necessario modificare la modalità di autenticazione della configurazione al database della Console su Server SQL e Modalità di autenticazione di Windows.

Effettuare le operazioni seguenti:

1. Dallo strumento di gestione SQL Server, verificare se il database della Console supporta SQL Server e la modalità di autenticazione Windows. Se il database della Console non supporta queste opzioni, passare a SQL Server e a Modalità di autenticazione, quindi riavviare SQL Server.
2. Eseguire i passaggi riportati di seguito per creare l'account Arcserve UDP in SQL Server:
    a. Dalla cartella seguente, fare clic con il tasto destro del mouse su **DBAccountUpdate.bat**, quindi fare clic sull'opzione **Esegui come amministratore**:

    <UDP Installation Folder>\Management\BIN

    Viene visualizzata l'interfaccia di comando.

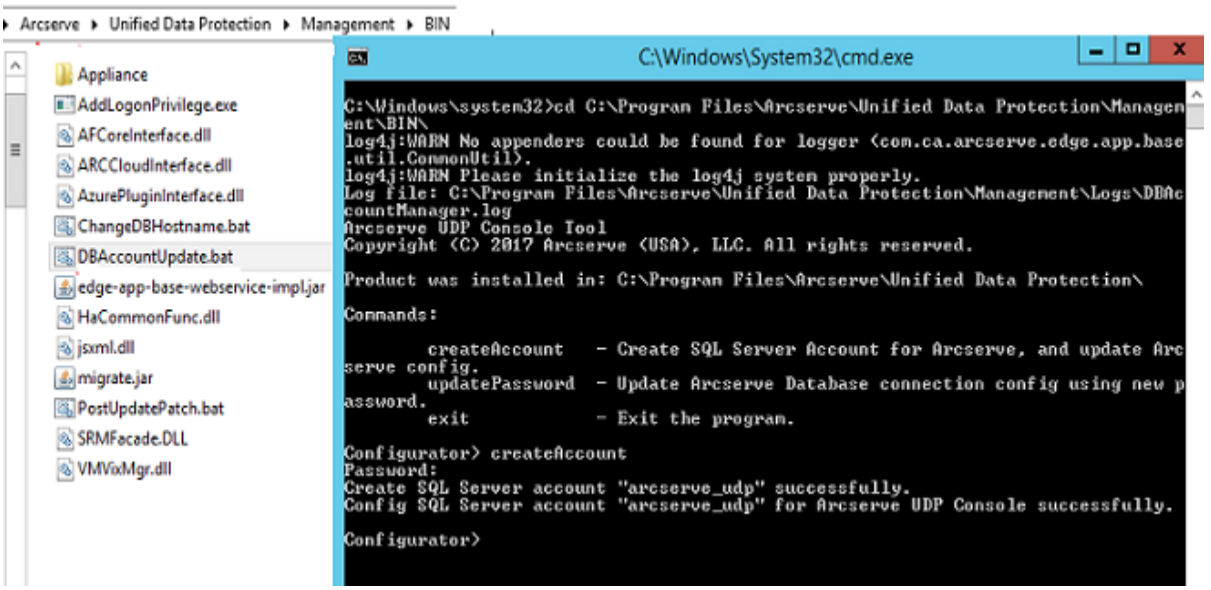
    b. Nell'interfaccia di comando, digitare *createAccount*e premere Invio.

    L'interfaccia della riga di comando richiede di specificare una password.

    c. Specificare la password desiderata per l'account *arcserve_udp* e premere Invio.

    La Console Arcserve UDP crea l'account SQL Server *arcserve_udp*.

    d. Digitare *exit* per chiudere l'interfaccia della riga di comando.



3. Riavviare il servizio di gestione Arcserve UDP.

Risoluzione dei problemi

L'elenco seguente fornisce la possibile risoluzione degli errori che possono essere visualizzati con la Console di gestione utenti:

- **Sintomo**

  Impossibile accedere alla Console di gestione utenti

  Soluzione

  Verificare che l'utente abbia effettuato l'accesso come amministratore. Gli utenti non amministratori non si dispongono dell'autorizzazione per accedere alla Console di gestione utenti. Verificare che il nome utente e la password siano corretti.

- **Sintomo**

  Errore di autenticazione: Impossibile accedere alla Console

  Soluzione

  Verificare se l'utente sia assegnato a un ruolo. Se non è stato assegnato alcun ruolo, un utente non può accedere alla Console Arcserve UDP.

- **Sintomo**

  Timeout della Console di gestione utenti.

  Soluzione

  Il tempo di mantenimento di accesso per la pagina Gestione utenti è 15 minuti. Se la Console non rileva alcuna operazione sulla pagina per 15 minuti, l'utente viene disconnesso automaticamente.

Chapter 8: Aggiunta e gestione dei nodi di origine

La presente sezione descrive i seguenti argomenti:

Aggiunta di nodi alla console

Per nodo si intende un computer di origine fisico o virtuale su un hypervisor che si desidera proteggere. Un nodo può essere protetto mediante l'esecuzione del backup dei dati in una destinazione. Arcserve Unified Data Protection consente di aggiungere i seguenti tipi di nodi:

- Windows
- Linux
- Computer virtuali in server VMware ESX/vCenter e Microsoft Hyper-V

I nodi vengono aggiunti specificando manualmente i dettagli del nodo, rilevandoli da Active Directory o importandoli da un file o dagli hypervisor.

Nota: È inoltre possibile aggiungere i nodi creando un piano.

Come procedere?

- Verifica dei prerequisiti
- Aggiunta di nodi
- Rilevamento dei nodi
- Importazione dei nodi

Verifica dei prerequisiti

Prima di aggiungere un nodo, completare le seguenti operazioni preliminari:

1. Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.
2. Accedere alla console.
3. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.
4. Dal riquadro centrale, fare clic su **Aggiungi nodi**.

   Viene visualizzata la finestra di dialogo **Aggiungi nodi alla Console di Arcserve UDP**.

   La finestra di dialogo include diverse opzioni per l'aggiunta dei nodi.

Aggiunta di nodi

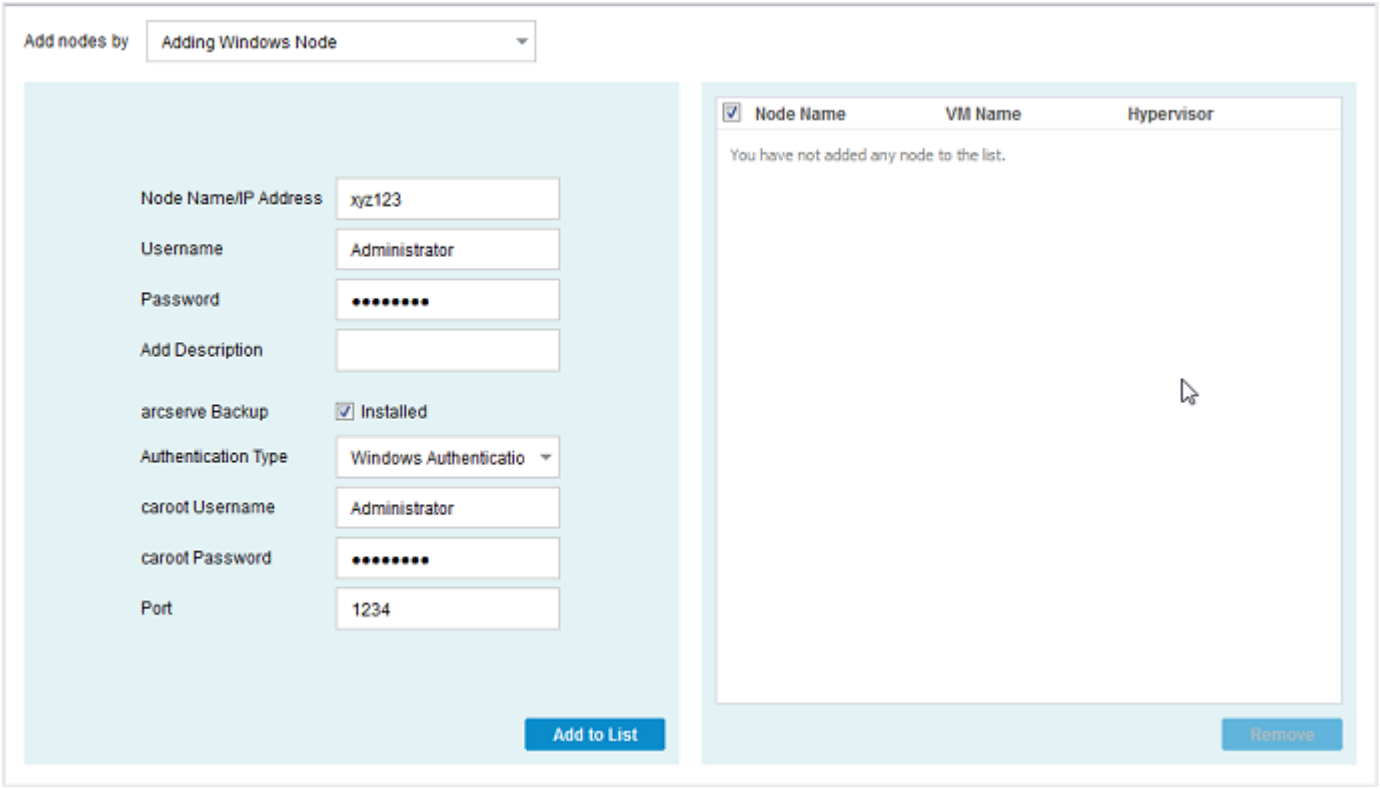
Quando si dispone dell'indirizzo IP o del nome di un nodo o di un set di nodi, è possibile aggiungerli alla Console specificandone i dettagli manualmente. È possibile aggiungere i seguenti tipi di nodi:

- **Windows:** nodi di origine Windows che si desidera proteggere. Se il nodo di origine di Windows con porta SMB è bloccato, l'agente Arcserve UDP (Windows) viene installato sul nodo.
- **Linux:** nodi di origine Linux che si desidera proteggere. Agente Arcserve Unified Data Protection per Linux viene installato sul server di backup Linux e non sui nodi di origine Linux.
- **Server di backup Linux:** server Linux che gestisce i nodi di origine di Linux. Agente Arcserve Unified Data Protection per Linux viene installato su questo server.

Effettuare le operazioni seguenti:

1. Dall'elenco a discesa **Aggiungi nodi per**, selezionare una delle seguenti opzioni:

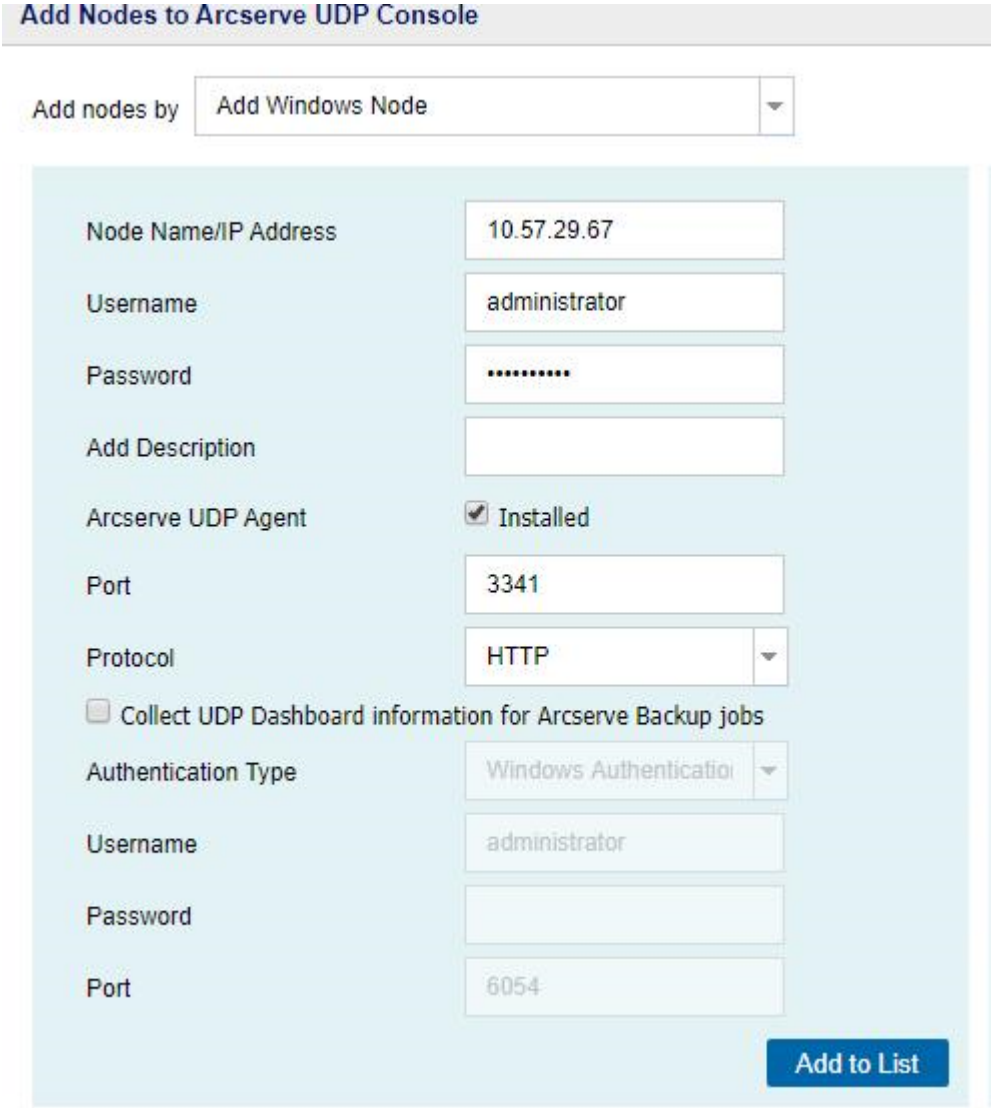
Aggiunta di un nodo Windows



Nota: Per abilitare i dettagli di Arcserve Backup, selezionare **Installato**.

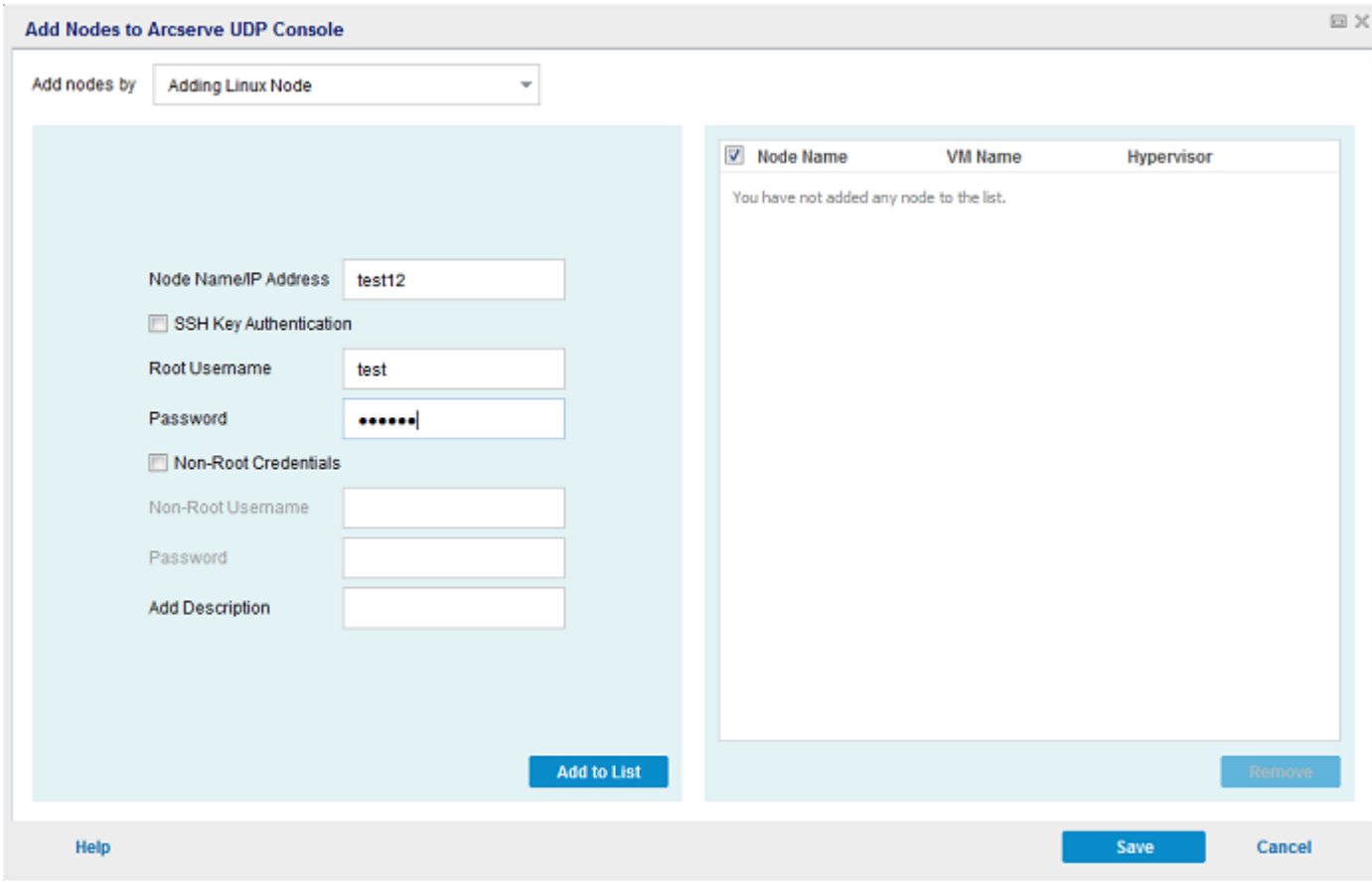
2. Per aggiungere il nodo di una porta SMB bloccata, accedere all'elenco a discesa **Aggiungi nodi per**, quindi selezionare una delle seguenti opzioni:

Aggiunta di un nodo Windows



Nota: immettere i dettagli relativi alla porta e al protocollo personalizzati, quindi selezionare Installato.

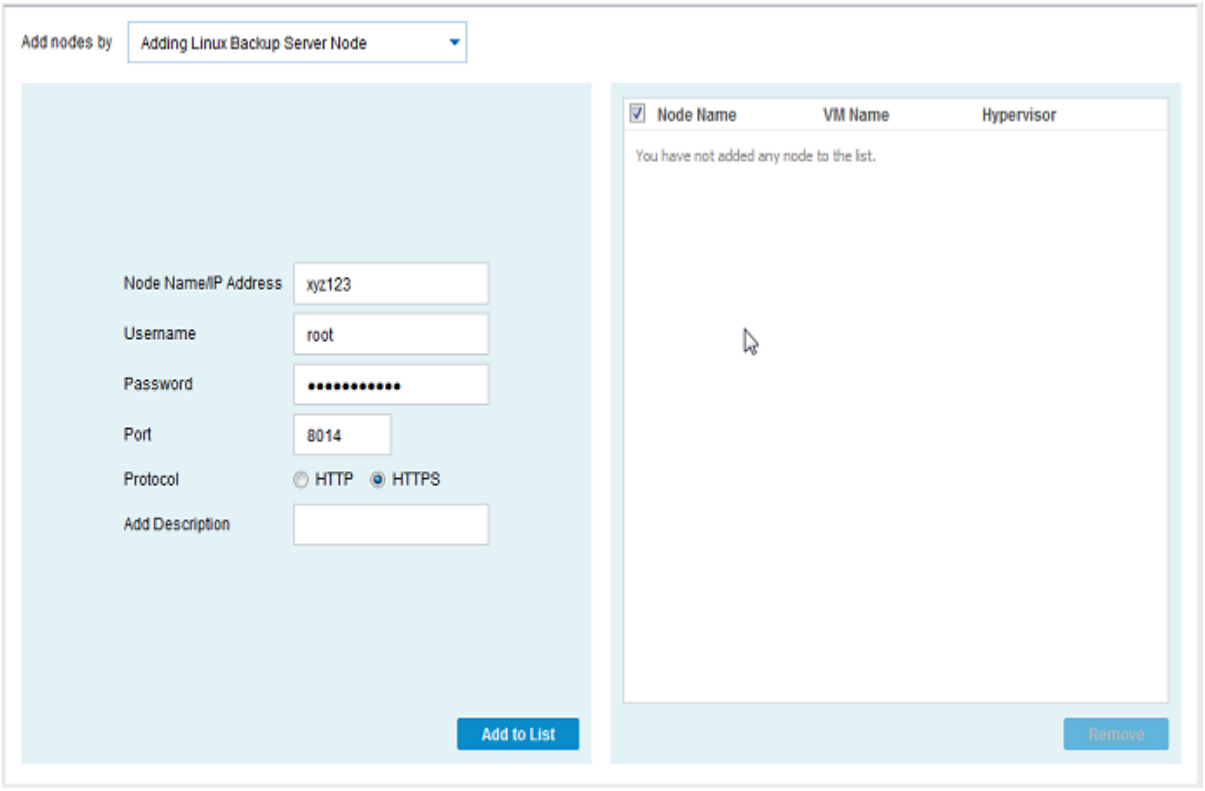
Aggiunta di un nodo Linux



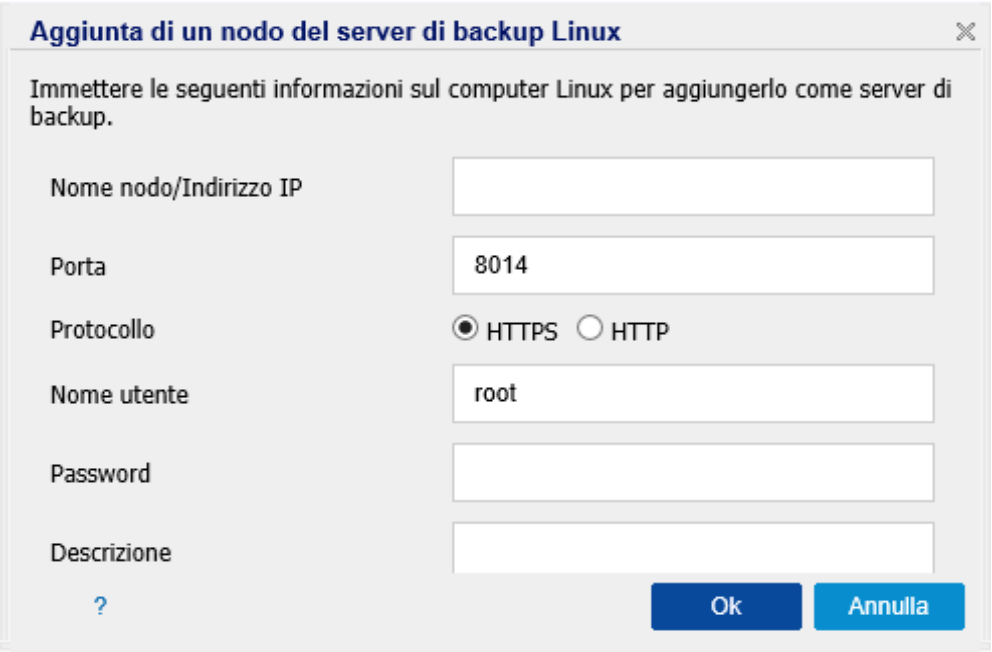
Note:

- Per Linux, durante la selezione della **chiave SSH di autenticazione**, non sarà necessario immettere i dettagli della password. Tuttavia, è richiesta l'immissione del nome utente. Per ulteriori informazioni sulla configurazione della chiave SSH, consultare la sezione Configurazione dell'autenticazione con chiave pubblica e chiave privata.
- Prima di aggiungere un nodo di Linux, è necessario aggiungere un **server di backup di Linux** per la gestione di nodi di Linux.
- Per il nodo Debian Linux, le credenziali non root non sono supportate. Per aggiungere il nodo Debian Linux con l'utente non root, utilizzare sudoer. Per ulteriori informazioni sulla configurazione di Sudo, consultare la sezione Configurazione di sudo in Debian.
- È possibile accedere al server di backup Linux dalla console Arcserve UDP solo se si esegue il ripristino.

Aggiunta di un nodo al server di backup di Linux



Quando si aggiunge il nodo del server di backup Linux dall'attività **Backup: Linux basato su agente**, viene visualizzata la finestra di dialogo seguente:



Vengono visualizzati i dettagli dell'opzione selezionata.

3. Immettere i dettagli del nodo e fare clic su **Aggiungi a elenco**.

Il nodo viene aggiunto al riquadro destro. Per aggiungere più nodi, seguire nuovamente la procedura. Tutti i nodi aggiunti vengono elencati nel riquadro destro.

4. (Facoltativo) Per rimuovere i nodi aggiunti dall'elenco nel riquadro destro, selezionare i nodi e fare clic su **Rimuovi**.
5. Selezionare i nodi da aggiungere e fare clic su **Salva**.

   I nodi vengono aggiunti e visualizzati nella pagina **Nodi: Tutti i nodi.**

   Se il server di backup Linux si trova nell'ambiente NAT, attenersi alla seguente procedura prima di aggiungerlo alla console Arcserve UDP:

   1. Creare il file *server.cfg* nella cartella del server di backup Linux seguente:

      /opt/Arcserve/d2dserver/configfiles/.
   2. Aggiungere la riga seguente nel file server.cfg:

      nat_enable=true
   3. Riavviare l'agente per Linux utilizzando la riga di comando seguente:

      /opt/Arcserve/d2dserver/bin/d2dserver restart

   Nota: Se il server di backup Linux è già stato aggiunto, è sufficiente aggiornarlo sulla console UDP.

Rilevamento dei nodi

Per aggiungere dei nodi che si trovano in un'Active Directory, è possibile innanzitutto rilevarli inserendo i dettagli di Active Directory e aggiungendo i nodi alla Console.

Effettuare le operazioni seguenti:

1. Dall'elenco a discesa **Aggiungi nodi per**, selezionare **Rilevamento nodi da Active Directory**.
2. Specificare le credenziali utente e fare clic su **Aggiungi.**

   Nome utente

   Specifica il dominio e il nome utente nel formato di dominio\nomeutente.

   Password

   Specifica la password utente.

   Filtro nome computer

   Specifica il filtro per il rilevamento dei nomi dei nodi.

   Dopo la convalida, il nome utente viene aggiunto all'elenco.
3. Selezionare il nome utente aggiunto e fare clic su **Sfoglia**.

   Il rilevamento corretto del nodo genera la finestra di dialogo **Conferma** che chiede all'utente se desidera aggiungere i nodi dal risultato del **rilevamento**.

   Nota: il processo di rilevamento potrebbe richiedere del tempo che dipende da fattori quali la rete e il numero di computer nella rete.
4. Fare clic su **Sì**.

   I nodi rilevati vengono elencati.
5. Selezionare il nodo, immettere il nome utente e la password, quindi fare clic su **Applica**.

   Nota: facendo clic su Applica, le credenziali vengono verificate. È necessario verificare ciascun nodo prima di aggiungerlo all'elenco.

   I segni di spunta verdi vengono visualizzati per i nodi verificati.
6. Fare clic su **Aggiungi a elenco**.

   Il nodo selezionato viene elencato nel riquadro destro.
7. Per aggiungere i nodi alla Console, dal riquadro destro, selezionare il nodo e fare clic su **Salva**. Per aggiungere tutti i nodi, selezionare la casella di controllo **Nome**

nodo.

I nodi verificati vengono aggiunti e sono disponibili nella pagina **Nodi: Tutti i nodi**.

Risoluzione dei problemi: Il dominio specificato non esiste o non è stato possibile contattarlo

Sintomo

Durante l'aggiunta di nodi mediante il rilevamento da Active Directory, viene visualizzato il seguente messaggio di errore:

"The specified domain either does not exist or could not be contacted. Verify that the Console server can access the domain controller through the network." (Il dominio specificato non esiste o non è stato possibile contattarlo. Verificare che il server della Console sia in grado di accedere al controller di dominio tramite la rete.)

Soluzione

Verificare in primo luogo la connettività tra Arcserve UDP e il controller di dominio. Se non ci sono problemi di connettività, utilizzare il comando riportato di seguito con l'argomento "dsgetdc" per verificare se Windows è in grado di individuare il controller di dominio dal nome di dominio:

nltest.exe

Ad esempio, "nltest /dsgetdc:sample_domain", dove sample_domain è il nome di dominio.

Se il comando non riesce, potrebbe essersi verificato un problema DNS nel proprio ambiente.

Nota: È necessario eseguire il comando riportato sopra sul computer UDP. Per ulteriori informazioni, fare riferimento all'articolo Microsoft seguente.

Importazione dei nodi

Arcserve Unified Data Protection consente di aggiungere più nodi fisici e virtuali mediante il metodo di importazione. A seconda dei requisiti, è possibile utilizzare uno dei metodi di importazione seguenti:

- Importazione di nodi da file CSV o TXT
- Importazione di nodi da un server vCenter/ESX
- Importazione di nodi da un server Hyper-V

Importazione di nodi da un server vCenter/ESX

Mediante questo metodo di importazione, è possibile importare nodi di computer virtuali da server ESX o vCenter. Questa opzione elenca tutti i computer virtuali rilevati sul server specificato, inclusi quelli già gestiti in Arcserve Unified Data Protection.

Effettuare le operazioni seguenti:

1. Dall'elenco a discesa **Aggiungi nodi per**, selezionare l'opzione **Importazione da vCenter/ESX**.
2. Specificare i dettagli del server vCenter/ESX, quindi fare clic su **Connetti**.

   Nel riquadro sinistro, viene visualizzata una struttura ad albero del nodo.

   Nota: VMware Virtual Disk Development Kit (VDDK) 6.x.x è fornito in bundle con Arcserve UDP versione 7.0. Tuttavia, VDDK 6.x.x non supporta il protocollo HTTP. Inoltre, vCenter e ESX in genere supportano la connessione HTTPS solo per impostazione predefinita. Selezionare HTTPS salvo quando si sostituisce manualmente la versione VDDK 6.x.x integrata con un'altra e si configura manualmente vCenter/ESX per consentire la connessione HTTP.
3. Espandere la struttura del nodo.

   (Facoltativo) È possibile digitare il nome del nodo nel campo del filtro per localizzare il nodo nella struttura ad albero.
4. Selezionare i nodi che si desidera aggiungere.

   Nota: Arcserve UDP permette di eseguire le operazioni seguenti:

   - Aggiungere e proteggere oggetti contenitore nell'infrastruttura di vSphere (ad esempio, datacenter e pool di risorse).
   - Aggiungere e proteggere modelli di computer virtuale e proteggere il computer virtuale mediante tag.

   Tuttavia, al momento questa operazione è consentita solo utilizzando la procedura guidata di creazione del piano. Per ulteriori informazioni, consultare la sezione *Aggiunta di nodi da vCenter/ESX* nel capitolo Definizione dell'origine.
5. Selezionare la casella di controllo **Provide credentials for the selected nodes** (Fornire credenziali per i nodi selezionati) e inserire le credenziali utente.

   Nota: Le credenziali utente sono obbligatorie per funzioni quali la verifica preliminare, il troncamento del registro applicazioni e i comandi precedenti e successivi al backup.
6. Fare clic su **Aggiungi a elenco**.

I nodi selezionati vengono aggiunti al riquadro destro.

7. Selezionare i nodi e fare clic su **Salva**.

   I nodi vengono aggiunti e visualizzati nella pagina **Nodi: Tutti i nodi**.

Importazione di nodi da un server Hyper-V

Mediante questo metodo di importazione, è possibile importare nodi di computer virtuali da server Microsoft Hyper-V.

Effettuare le operazioni seguenti:

1. Dall'elenco a discesa **Aggiungi nodi per**, selezionare l'opzione **Importazione da Hyper-V**.
2. Completare i seguenti campi, quindi fare clic su **Connetti**.

   Hyper-V

   Specifica il nome del server Hyper-V o l'indirizzo IP. Per importare i computer virtuali compresi in cluster Hyper-V, specificare il nome del nodo cluster o il nome host di Hyper-V.

   Nome utente

   Specifica il nome dell'utente Hyper-V che dispone di diritti di amministratore.

   Nota: Per i cluster Hyper-V, utilizzare un account di dominio con privilegi amministrativi sul cluster. Per gli host Hyper-V standalone, si consiglia di utilizzare un account di dominio.

   Password

   Specifica la password del nome utente.

   La soluzione Arcserve Unified Data Protection ricerca e visualizza la struttura del nodo nel riquadro sinistro.
3. Espandere la struttura del nodo.

   (Facoltativo) È possibile digitare il nome del nodo nel campo del filtro per localizzare il nodo nella struttura ad albero.

   Nota: I computer virtuali configurati come ruolo cluster vengono elencati direttamente sotto il nome del nodo cluster nella struttura. I computer virtuali non compresi nel cluster vengono elencati sotto il nome del singolo host Hyper-V.
4. Selezionare i nodi che si desidera aggiungere.
5. Selezionare la casella di controllo **Provide credentials for the selected nodes** (Fornire credenziali per i nodi selezionati) e inserire le credenziali utente.

   Nota: Le credenziali utente sono obbligatorie per funzioni quali la verifica preliminare, il troncamento del registro applicazioni e i comandi precedenti e successivi al backup. Senza credenziali utente, la verifica preliminare non viene eseguita correttamente per i nodi selezionati.
6. Fare clic su **Aggiungi a elenco**.

I nodi selezionati vengono aggiunti al riquadro destro.

7. Selezionare i nodi e fare clic su **Salva**.

   I nodi vengono aggiunti e visualizzati nella pagina **Nodi: Tutti i nodi**.

Importazione di computer virtuali con un account amministrativo aggiuntivo

L'account amministrativo aggiuntivo fa riferimento agli account che non utilizzano amministratori predefiniti. Tali account vengono detti anche account amministrativi non integrati. Per importare un computer virtuale da un host Hyper-V, utilizzare l'account di amministratore integrato dell'host Hyper-V, un account di dominio compreso nel gruppo degli amministratori locali dell'host Hyper-V oppure un account utente amministrativo non integrato.

L'utente con un account amministrativo aggiuntivo può attenersi alle procedure illustrate successivamente per disabilitare l'accesso UAC remoto.

Note:

- Questa procedura non è analoga alla disabilitazione del controllo accesso utente. Permette di disabilitare alcune funzioni UAC.
- Poiché la tecnologia WMI remota viene utilizzata per l'importazione, verificare che non sia bloccata dal firewall.

Effettuare le operazioni seguenti:

1. Fare clic su Start, digitare regedit nel campo Cerca programmi e file e premere Invio.

   Viene visualizzato l'editor del Registro di sistema di Windows.

   Nota: Potrebbe essere necessario fornire le credenziali di amministratore per accedere all'editor del Registro di sistema di Windows.

2. Individuare e fare clic sulla chiave di registro seguente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. Dal menu Modifica, fare clic su Nuovo e selezionare Valore DWORD (a 32 bit).
4. Specificare LocalAccountTokenFilterPolicy come nome della nuova voce e premere Invio.
5. Fare clic con il pulsante destro del mouse su LocalAccountTokenFilterPolicy, quindi selezionare Modifica.
6. Specificare 1 nel campo Dati valore e fare clic su OK.
7. Uscire dall'editor del Registro di sistema.

   Per ulteriori informazioni sul comportamento di Windows, consultare la documentazione di Microsoft.

Importazione di nodi da file CSV o TXT

Quando è necessario aggiungere più nodi fisici, invece di aggiungerli uno alla volta, è possibile creare un file .csv o .txt nel formato <NomeNodo>, <NomeUtente> o <Password>. Successivamente, è possibile selezionare e importare il file .txt o .csv nella Console utilizzando le opzioni di ricerca e caricamento.

Effettuare le operazioni seguenti:

1. Dall'elenco a discesa **Azioni**, selezionare **Importa.**
2. Fare clic su **Sfoglia** per selezionare il file salvato in formato .txt o .csv.
3. Fare clic su **Carica**.

   I nodi vengono aggiunti e visualizzati nella pagina **Nodi: Tutti i nodi**.

Gestione dei nodi

Con Arcserve UDP è possibile eseguire varie azioni di gestione di un nodo come ad esempio aggiornamento di nodi e hypervisor, esportazione di nodi, eliminazione verifiche preliminari.

Come procedere?

- Verifica dei prerequisiti
- Aggiornamento delle informazioni Hypervisor
- Definizione dell'hypervisor
- Aggiornamento delle informazioni del computer virtuale
- Aggiornamento dei nodi
- Esportazione del nodo
- Sospensione del nodo
- Ripresa del nodo
- Sincronizzazione dei dati
- Eliminazione di nodi dalla Console
- Distribuzione dell'agente sui nodi
- Esecuzione di verifiche preliminari per i processi di backup

Verifica dei prerequisiti

Prima di cominciare a gestire i nodi, completare i prerequisiti seguenti:

- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.
- Accedere alla console.
- Aggiungere un nodo.

Aggiornamento delle informazioni Hypervisor

Dopo aver aggiunto un nodo del computer virtuale a Arcserve Unified Data Protection, le informazioni relative alla connessione, come il nome host o le credenziali dell'hypervisor del computer virtuale, potrebbero subire delle modifiche. In tali casi, Arcserve Unified Data Protection consente di aggiornare le informazioni sull'hypervisor.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Fare clic con il tasto destro del mouse sul gruppo di nodi in **Gruppi vCenter/ESX** o **Gruppi Hyper-V**.
3. Fare clic su **Aggiorna vCenter/ESX** o **Aggiorna Hyper-V.**

   Viene visualizzata la finestra di dialogo **Aggiorna vCenter/ESX** o **Aggiorna Hyper-V**.
4. Immettere i nuovi dettagli nella finestra di dialogo e fare clic su **OK**.

   Viene chiusa la finestra di dialogo **Aggiorna vCenter/ESX** o **Aggiorna Hyper-V**.

   Le informazioni sull'hypervisor sono state correttamente aggiornate.

Definizione dell'hypervisor

È possibile specificare i dettagli dell'hypervisor per evitare l'utilizzo di altre licenze per la protezione di un computer virtuale. Quando si protegge un computer virtuale mediante un piano di backup senza agente basato su host, la licenza dell'host dell'hypervisor viene utilizzata per proteggere il computer virtuale. Non è necessario installare nessun agente sul computer virtuale. In alcuni casi è possibile decidere di installare l'agente sul computer virtuale e creare un piano di backup basato su agente per proteggere il computer virtuale. In tali casi, il computer virtuale utilizza un'altra licenza, oltre alla licenza dell'host dell'hypervisor. Specificare i dettagli dell'hypervisor permettendo al computer virtuale di utilizzare la licenza dell'host dell'hypervisor invece di utilizzarne un'altra.

Esempi che descrivono i casi in cui specificare le informazioni dell'hypervisor:

- Si dispone di un piano di backup senza agente basato su host per proteggere i computer virtuali ESX o un server Hyper-V. Il piano utilizza la licenza dell'hypervisor per la protezione del computer virtuale. È necessario installare l'Agente UDP in un computer virtuale dell'hypervisor specificato e creare un piano basato su agente per proteggere il computer virtuale. Il piano utilizza generalmente un'altra licenza per la protezione del computer virtuale. Se si specifica l'hypervisor per il computer virtuale, il piano utilizza la licenza dell'hypervisor.
- Si dispone di un piano di Linux basato su agente per proteggere i nodi dell'agente del computer virtuale di Linux. Se si specifica l'hypervisor per il computer virtuale, tutti i computer virtuali sullo stesso hypervisor utilizzano la licenza dell'hypervisor.

Considerare i punti seguenti prima di specificare l'hypervisor:

- Non è possibile specificare l'hypervisor per un nodo fisico.
- Non è possibile specificare l'hypervisor per un nodo di computer virtuale importato da vCenter/ESX o Hyper-V.
- È possibile specificare l'hypervisor per più computer virtuali che appartengono allo stesso hypervisor allo stesso tempo.
- Verificare che gli ultimi strumenti VMware o il servizio di integrazione Hyper-V sia installato e che il computer virtuale sia attivo. Assicurarsi inoltre che Windows Management Instrumentation (WMI) sia nell'elenco delle eccezioni del firewall sul nodo dell'agente del computer virtuale.

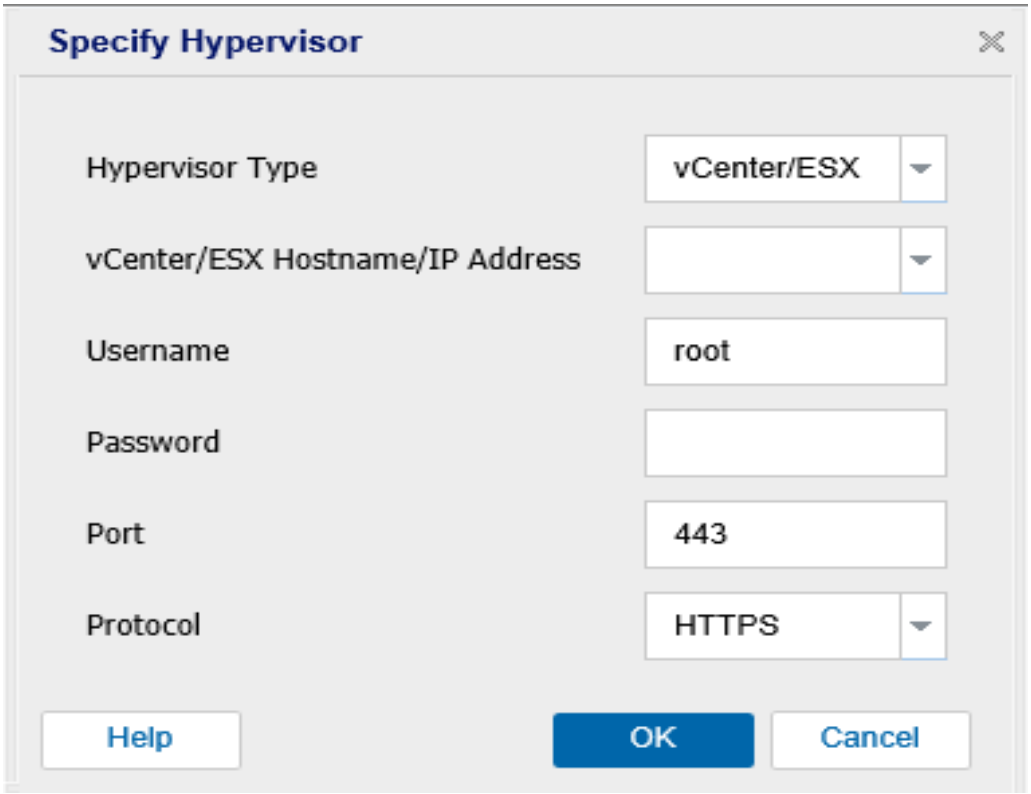
Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.
3. Eseguire una delle seguenti operazioni:
   - Fare clic con il tasto destro del mouse sul nome del nodo.
   - Selezionare il nome del nodo e dal riquadro centrale fare clic sull'elenco a discesa **Azioni**.

   Viene visualizzato un elenco di opzioni.
4. Fare clic su **Specifica hypervisor**.

   Viene visualizzata la finestra di dialogo Specifica hypervisor. Il **tipo di hypervisor** può essere **Hyper-V**, **vCenter/ESX** o **altro** (Xen, computer virtuale basato su Kernel, Red Hat Enterprise Virtualization).



5. Immettere i dettagli dell'hypervisor e fare clic su **OK**.

   Le informazioni dell'hypervisor sono state specificate.

Aggiornamento delle informazioni del computer virtuale

Arcserve Unified Data Protection consente di aggiornare alcune delle proprietà dei nodi del computer virtuale dai rispettivi hypervisor. È possibile attivare l'aggiornamento manualmente o automaticamente. Le proprietà seguenti dei nodi del computer virtuale vengono aggiornate e sincronizzate con i computer virtuali corrispondenti nell'hypervisor:

- Nome nodo
- Nome computer virtuale
- Sistema operativo

Per attivare manualmente l'aggiornamento, utilizzare l'opzione **Aggiorna informazioni sul computer virtuale**.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

2. Dal riquadro centrale, fare clic sull'elenco a discesa **Azioni**, quindi fare clic su **Aggiorna informazioni sul computer virtuale**.

   Viene visualizzata la finestra di dialogo **Aggiorna informazioni sul computer virtuale**.

3. Fare clic su **OK**.

   È stato attivato il rilevamento manuale per aggiornare i nodi del computer virtuale.

   La funzione di aggiornamento automatico viene attivata automaticamente quando si eseguono le azioni seguenti:

   - Aprire la scheda **Risorse** della Console.
   - Inviare un rapporto pianificato.

   Nota: Anche se si attivano più aggiornamenti automatici, viene eseguito solo un aggiornamento automatico alla volta. Gli aggiornamenti automatici restanti vengono messi in coda.

Aggiornamento dei nodi

È possibile aggiornare le informazioni relative ai nodi esistenti. È possibile aggiornare il nodo in qualsiasi momento. Di seguito vengono riportate alcune soluzioni in cui è necessario l'aggiornamento di un nodo:

- Nel nodo viene installato un nuovo prodotto dopo la registrazione del nodo in Arcserve Unified Data Protection.
- È stato eseguito l'aggiornamento del nome utente o della password dopo la registrazione del nodo in Arcserve Unified Data Protection.

Nota: se un nodo funge da Recovery Point Server e da agente e vengono modificate le credenziali o il protocollo per tale nodo, eseguire l'aggiornamento del nodo dalla pagina **Destinazioni: Recovery Point Server.** Il piano verrà distribuito automaticamente sull'agente dopo l'aggiornamento del Recovery Point Server. Se si aggiorna il nodo dalla pagina **Nodi: Tutti i nodi**, i piani relativi a tali nodi non verranno distribuiti correttamente. Per effettuare la distribuzione del piano, aggiornare nuovamente il nodo dalla pagina **Destinazioni: Recovery Point Server**.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

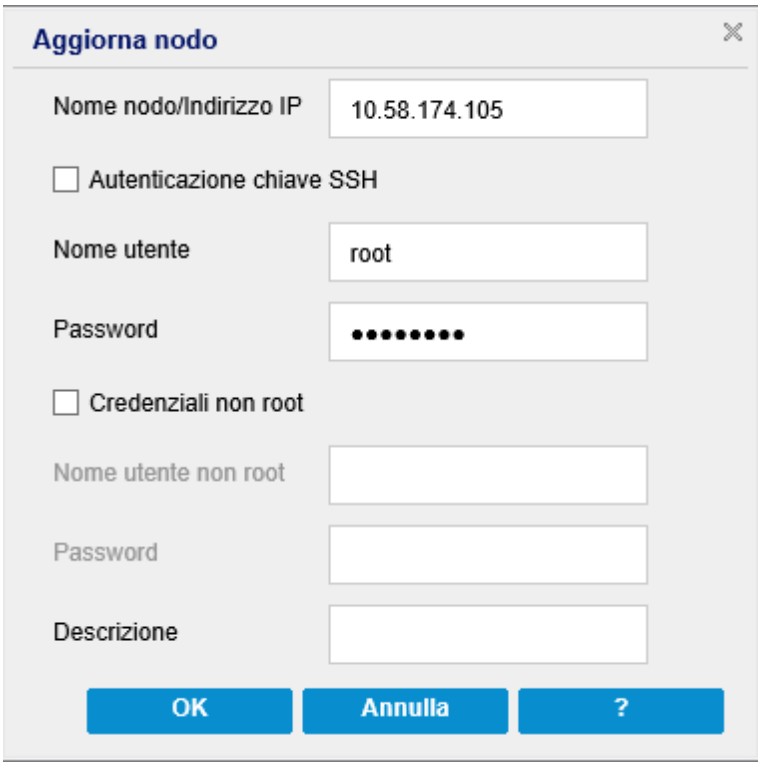
2. Eseguire una delle seguenti operazioni:

   - Fare clic con il tasto destro del mouse sul nome del nodo.
   - Selezionare il nome del nodo e dal riquadro centrale fare clic sull'elenco a discesa **Azioni**.

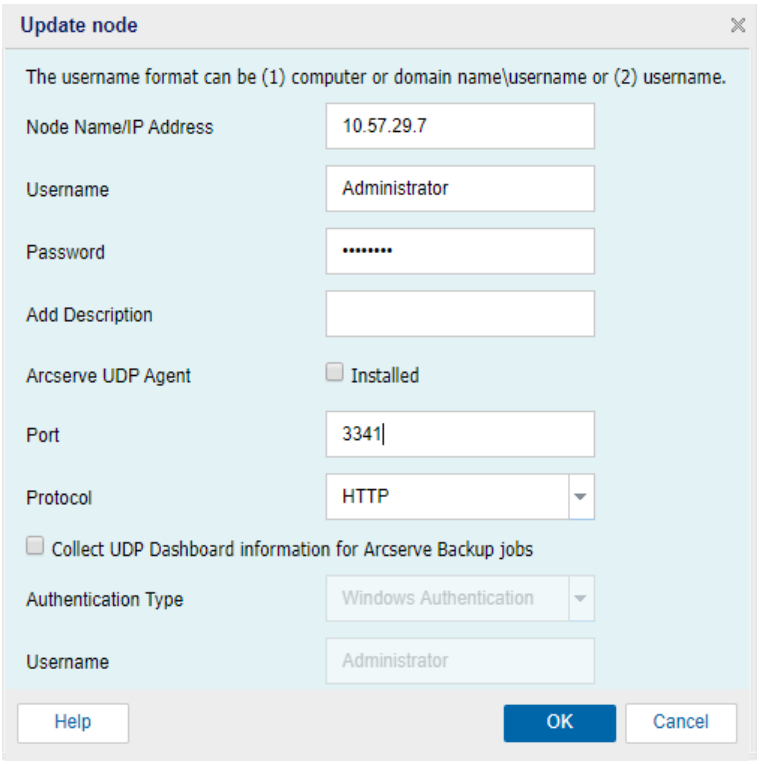
3. Fare clic su **Aggiorna**.

   Viene visualizzata la finestra di dialogo **Aggiorna nodo**.

   La finestra di dialogo seguente riguarda i nodi Linux:



La finestra di dialogo seguente per il nodo Windows (quando la porta SMB è bloccata) viene visualizzata con una porta personalizzata:



4. Aggiornare i dettagli e fare clic su **OK**.

   Le informazioni sul nodo sono state aggiornate.

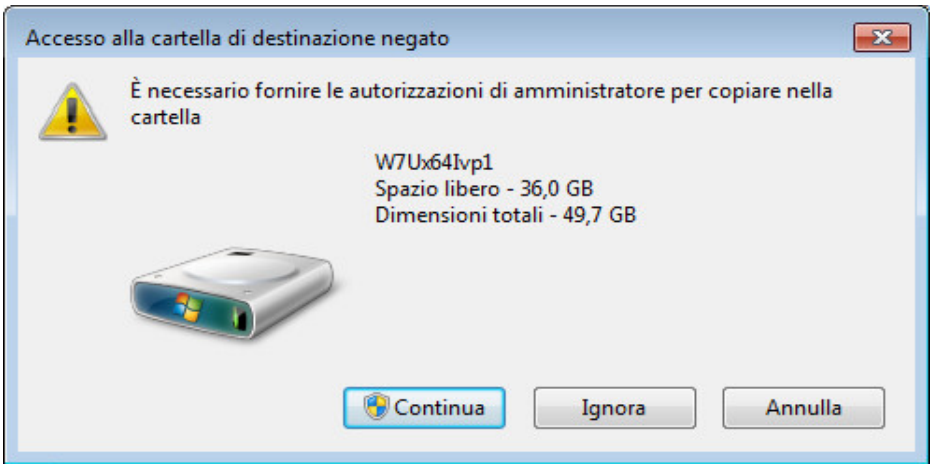
Aggiornamento dei nodi con un account amministrativo aggiuntivo

L'account amministrativo aggiuntivo fa riferimento agli account che non utilizzano amministratori predefiniti. Tali account vengono detti anche account amministrativi non integrati. Le funzioni di aggiornamento nodo e verifica preliminare utilizzano l'account specificato in Aggiorna nodo per connettersi a un computer virtuale ed eseguire i controlli correlati.

Nota: Utilizzare o l'account di amministratore integrato o l'account di amministratore di dominio integrato durante l'esecuzione della funzione Aggiorna nodo. Se necessario, è possibile utilizzare un amministratore non integrato, ma occorre prima verificare che tale account disponga delle autorizzazioni di amministratore richieste.

Effettuare le operazioni seguenti:

1. Verificare che sia possibile accedere a \\[VM host name]\ADMIN$ mediante l'account di amministratore aggiuntivo da un altro computer. In caso di problemi, verificare se l'opzione di condivisione file e stampante sia bloccata dal firewall. Se le impostazioni del firewall sono corrette, può essere necessario disabilitare l'accesso al controllo account utente (UAC) remoto. Per disabilitare l'accesso UAC remoto, consultare la sezione Importazione di computer virtuali con un account amministrativo aggiuntivo.
2. In VMware, durante l'aggiornamento dei nodi, Arcserve UDP installa automaticamente alcuni strumenti nel computer virtuale per eseguire le verifiche preliminari. Per verificare che l'account disponga delle autorizzazioni richieste, completare i passaggi seguenti:
    a. Accedere al computer virtuale con l'account di amministratore non integrato.
    b. Copiare un file da C:\Windows in C:\ e controllare che il messaggio seguente non sia visualizzato:



c. Se si verificano problemi, è possibile modificare le configurazioni di controllo account utente (UAC). A tale scopo, nel Local Security Policy disattivare l'impostazione di **esecuzione di tutti gli amministratori nella modalità di approvazione dell'amministratore** in secpol.msc -> Criteri locali -> Opzioni di protezione. (Secpol.msc è l'editor delle policy di protezione di Microsoft).

Nota: Non disabilitare l'UAC nella finestra di dialogo Impostazioni di Controllo account utente accessibile dal pannello di controllo.

Per ulteriori informazioni sulla modifica delle impostazioni di configurazione UAC, consultare la relativa documentazione di Microsoft.

3. Per i computer virtuali Hyper-V, l'account di amministratore aggiuntivo deve disporre di autorizzazioni analoghe a quelle descritte nella sezione Importazione di computer virtuali con un account amministrativo aggiuntivo.

Esportazione del nodo

È possibile esportare dei nodi come file ZIP (.zip). Se necessario, è possibile importare il file ZIP per memorizzare i nodi. Ad esempio, esportare i nodi prima degli aggiornamenti o dei riavvii consente di importare lo stesso insieme di nodi.

È possibile esportare soltanto i nodi con credenziali validi e in esecuzione su sistemi operativi Windows.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

2. Selezionare un nodo.
3. Dal riquadro centrale, fare clic sull'elenco a discesa **Azioni**, quindi fare clic su **Esporta**.

   Viene visualizzata una finestra di dialogo che richiede l'intervento dell'utente nel file list.zip.

4. Fare clic su **Apri** o **Salva**.

   L'elenco di nodi viene esportato.

Sospensione del nodo

Arcserve UDP consente di sospendere soltanto i nodo selezionati anziché il piano completo. Per impedire l'esecuzione di un processo pianificato, adesso non è necessario sospendere e riprendere il piano completo arrestando tutti i nodi associati.

Importante: la sospensione del nodo funziona solo se il nodo è associato a un piano di Windows basato su agente o un piano senza agente basato su host. Per gli altri piani, non è possibile sospendere un nodo.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

2. Selezionare i nodi desiderati associati a un piano.

3. Dal riquadro centrale, fare clic sull'elenco a discesa **Azioni**, quindi fare clic su **Sospendi**.

   Viene visualizzata una finestra di dialogo di conferma, in cui si indica che è possibile eseguire solo processi manuali per i nodi sospesi.

4. Fare clic su **Sì**.

   I nodi vengono sospesi. Se un nodo non è in pausa, viene visualizzato un messaggio con il motivo.

Ripresa del nodo

Arcserve UDP consente di riprendere un nodo sospeso. In questa versione, invece di sospendere e riprendere un intero piano, è possibile sospendere e riprendere solo nodi specifici associati ad esso.

Importante: è possibile sospendere e riprendere un nodo solo se il nodo è associato a un piano di Windows basato su agente o a un piano senza agente basato su host. Per gli altri piani, non è possibile sospendere o riprendere un nodo.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

2. Selezionare i nodi sospesi.

3. Dal riquadro centrale, fare clic sull'elenco a discesa **Azioni**, quindi fare clic su **Riprendi**.

   Viene visualizzata una finestra di dialogo di conferma dell'operazione.

4. Fare clic su **Sì**.

   Il nodo riprende l'esecuzione.

Sincronizzazione dei dati

La sincronizzazione dei dati mantiene i dati di diversi database coerenti e aggiornati.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.
3. (Livello di gruppo) Selezionare uno dei gruppi di nodi visualizzati nel riquadro sinistro e fare clic con il pulsante destro del mouse.
4. Selezionare una delle seguenti opzioni:

   Nota: È possibile visualizzare solamente le opzioni che sono già state aggiunte per la sincronizzazione con Arcserve Unified Data Protection.

   - Sincronizzazione completa di Arcserve Backup
   - Sincronizzazione incrementale di Arcserve Backup

   La finestra di dialogo **Informazioni** descrive l'invio del metodo di sincronizzazione selezionato.

Eliminazione di nodi dalla Console

Arcserve Unified Data Protection consente l'eliminazione di un nodo. Se i nodi vengono eliminati, le cronologie dei registri e dei processi associati verranno eliminati di conseguenza. Se necessario, sarà possibile aggiungere il nodo eliminato in un secondo momento.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

2. Selezionare il nodo che si desidera eliminare.
3. Eseguire una delle seguenti operazioni:
   - Fare clic con il tasto destro del mouse sul nome del nodo.
   - Selezionare il nome del nodo e dal riquadro centrale fare clic sull'elenco a discesa **Azioni**.
4. Fare clic su **Elimina**.

   Viene visualizzata la finestra di dialogo **Conferma**.

5. Fare clic su **Sì**.

   Il nodo viene cancellato della Console.

Distribuzione dell'agente sui nodi

Per eseguire l'aggiornamento o l'installazione dell'agente Arcserve Unified Data Protection per un nodo, utilizzare l'opzione **Installa/Aggiorna agente**. Se il computer di destinazione contiene una versione precedente dell'agente Arcserve Unified Data Protection, utilizzare l'opzione di aggiornamento per acquisire l'ultima versione. In caso contrario, utilizzare l'opzione di installazione.

Nota: È possibile effettuare la distribuzione degli agenti Arcserve Unified Data Protection su più nodi. È possibile eseguire un massimo di 16 attività contemporaneamente. Se sono presenti più di 16 attività, lo stato delle altre attività rimarrà in sospeso. Tali attività verranno eseguite al completamento di alcune delle 16 attività di distribuzione predefinite. Per modificare il conteggio di attività massime, aggiornare la chiave di registro seguente:

deployMaxThreadCount

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

2. Selezionare uno o più nodi.
3. Dal riquadro centrale, fare clic sull'elenco a discesa **Azioni**, quindi fare clic su **Installa/Aggiorna agente**.

   I dettagli dell'installazione o dell'aggiornamento vengono visualizzati sopra il nome del nodo sul riquadro centrale.

4. Verificare i dettagli.
5. Specificare la pianificazione per l'installazione/aggiornamento, quindi fare clic su **OK**.

   Il nodo viene aggiornato all'ultima versione dell'agente Arcserve Unified Data Protection.

   Nota: È possibile annullare la distribuzione di un agente se pianificata per l'esecuzione in un secondo momento. Per annullare la distribuzione di un agente, selezionare l'agente e fare clic su **Azioni, Cancel Agent Deployment** (Annulla distribuzione agente).

Esecuzione di verifiche preliminari per i processi di backup

Arcserve Unified Data Protection include un'utilità denominata Verifica preliminare che consente di eseguire verifiche fondamentali su nodi specifici per rilevare eventuali condizioni che possono causare l'errore dei processi di backup. La verifica preliminare è applicabile solo ai nodi dei computer virtuali importati da vCenter/ESX, da Hyper-V o da Nutanix AHV. La Verifica preliminare non funziona per i modelli di computer virtuale VMware. La Verifica preliminare viene eseguita automaticamente durante l'esecuzione delle azioni seguenti:

- Importazione di computer virtuali da un sistema vCenter Server/ESX Server, Hyper-V o Nutanix AHV.
- Esecuzione di un processo di backup.

Altri riferimenti:

- Soluzioni per gli elementi di verifica preliminare dei computer virtuali VMware
- Soluzioni per gli elementi di verifica preliminare dei computer virtuali Hyper-V
- Soluzioni per gli elementi di verifica preliminare dei computer virtuali Nutanix AHV

Inoltre, è possibile la funzionalità di Verifica preliminare può essere eseguita manualmente.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzata la pagina **Tutti i nodi: Nodo**.
3. Fare clic con il tasto destro del mouse sul un nodo, e fare clic su **Verifica preliminare**.

   Nota: è inoltre possibile eseguire la **Verifica preliminare** mediante una delle seguenti opzioni:

   - (Livello di nodo) Fare clic sulle caselle di controllo dei nodi su cui si desidera eseguire una verifica preliminare, quindi fare clic su **Azioni** e selezionare **Verifica preliminare**.

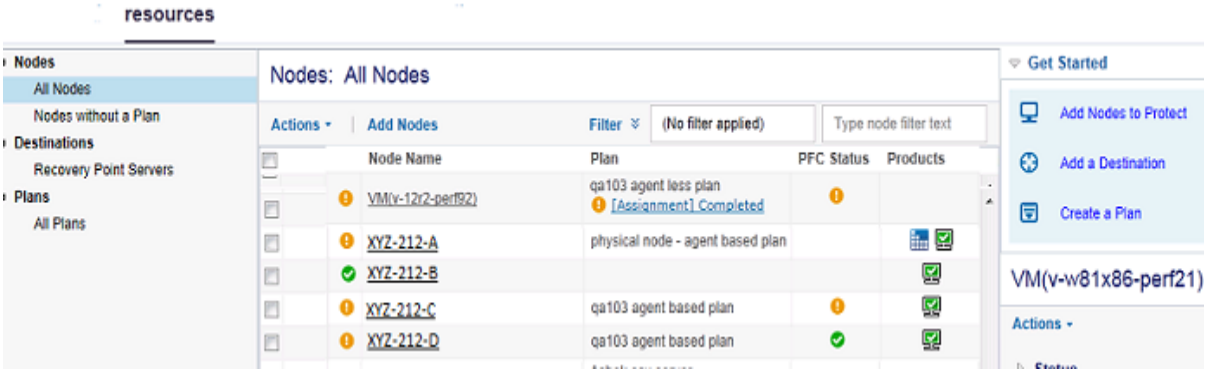
- (Livello di gruppo) Fare clic con il pulsante destro del mouse sul gruppo contenente i nodi, quindi fare clic su **Verifica preliminare**.

Viene visualizzato il messaggio seguente: **Avvio della verifica preliminare del computer virtuale in corso**.

4. Scorrere la pagina per visualizzare la colonna **Stato verifica preliminare** e visualizzare lo stato della verifica preliminare.

   Nota: Per impostazione predefinita, la colonna Stato verifica preliminare non è visibile nell'interfaccia utente. Abilitare manualmente la colonna Stato verifica preliminare nell'interfaccia utente.

   È inoltre possibile visualizzare lo stato della verifica preliminare facendo clic su **Visualizza registri** nel riquadro sinistro.



La tabella seguente descrive le verifiche eseguite dalla funzionalità di verifica preliminare per il computer virtuale VMware:

Elemento	Descrizione
Funzionalità di traccia dei blocchi modificati	Una funzionalità per tracciare i settori del disco che si trovano su un computer virtuale che è stato modificato. Questa funzionalità consente di ridurre le dimensioni dei backup. Questo elemento verifica l'abilitazione della funzionalità di traccia dei blocchi modificati.
Strumenti VMware	Questo elemento verifica che gli strumenti VMware siano installati sui computer virtuale.
Disco	Questo elemento verifica i dischi del computer virtuale.
Stato di alimentazione	Questo elemento verifica che il computer virtuale sia attivato.
Coerenza dei dati	Questo elemento verifica se è possibile acquisire una snapshot coerente con l'applicazione per il computer virtuale.
Server ESX	Questo elemento verifica se un server è in grado di rilevare il computer virtuale. L'opzione è visualizzata solo quando il nodo non è disponibile in ESX.

La tabella seguente descrive le verifiche eseguite dalla funzionalità di verifica preliminare per il computer virtuale Hyper-V:

Elemento	Descrizione
Credenziali Hyper-V	Il prodotto necessita di distribuire un'utilità di backup e un'utilità di traccia dei blocchi modificati sul server Hyper-V attraverso la condivisione di sistema ADMIN$. L'azione consente di verificare se il prodotto dispone dell'autorizzazione necessaria per la condivisione. Il processo di backup/ripristino produce un errore se le credenziali Hyper-V non sono corrette o se la condivisione ADMIN$ viene chiusa dall'amministratore.
Servizi integrazione	Questo elemento verifica che i servizi di integrazione Hyper-V siano installati e abilitati su ciascun computer virtuale. Senza i servizi di integrazione, Arcserve Unified Data Protection non è in grado di completare le seguenti azioni: ▪ Eseguire il comando pre/post e le azioni di eliminazione del registro dell'applicazione. ▪ Eseguire un backup coerente con l'applicazione. I servizi di integrazione contengono numerosi servizi. Arcserve Unified Data Protection controlla gli stati dei due servizi seguenti: ▪ Servizio Scambio di dati Hyper-V: richiesto per raccogliere le informazioni sul computer virtuale, eseguire i comandi pre/post e le azioni di eliminazione del registro dell'applicazione. ▪ Richiedente Copia Shadow del volume Hyper-V: richiesto per il backup coerente con l'applicazione.
Stato di alimentazione	Questo elemento verifica che il computer virtuale sia attivato. Un avviso Sospeso viene visualizzato quando il computer virtuale si trova in uno stato diverso da Attivato e Disattivato, come lo stato Salvato. Arcserve Unified Data Protection non è in grado di eseguire i comandi pre-/post-operazione né le azioni di eliminazione del registro dell'applicazione quando il computer virtuale non si trova nello stato Attivato. In aggiunta, Arcserve Unified Data Protection non può eseguire il backup coerente con l'applicazione quando il computer virtuale si trova nello stato Sospeso.
Disco	Questo elemento verifica se un disco non supportato è connesso al computer virtuale.
Coerenza dei dati	Questo elemento verifica se è possibile acquisire una snapshot coerente con l'applicazione per il computer virtuale.

La tabella seguente descrive le verifiche eseguite dalla funzionalità di Verifica preliminare per il computer virtuale Nutanix AHV:

Elemento	Descrizione
Stato di ali-	Questo elemento verifica che il computer virtuale sia attivato.

mentazione	
Coerenza dei dati	Questo elemento verifica se è possibile acquisire una snapshot coerente con l'applicazione per il computer virtuale.
Server AVS	Questo elemento verifica se un server è in grado di rilevare il computer virtuale. L'opzione è visualizzata solo quando il nodo non è disponibile in Nutanix AHV.

Soluzioni per gli elementi di verifica preliminare dei computer virtuali VMware

Altri riferimenti:

- Soluzioni per gli elementi di verifica preliminare dei computer virtuali Hyper-V
- Soluzioni per gli elementi di verifica preliminare dei computer virtuali Nutanix AHV

Le tabelle seguenti descrivono le soluzioni per gli errori e gli avvisi contenuti nei risultati della verifica preliminare per i computer virtuali VMware:

Funzionalità di traccia dei blocchi modificati

Stato	Messaggio	Soluzione
Errore	Impossibile abilitare la registrazione del blocco modificato.	Se il computer virtuale non dispone di hardware versione 7 o successiva, è possibile eseguirne l'aggiornamento o creare un piano di backup basato su agente in Arcserve Unified Data Protection e utilizzare l'Agente Arcserve Unified Data Protection per Windows per eseguire il backup del computer virtuale.
Avviso	La funzionalità di traccia dei blocchi modificati viene abilitata e contiene snapshot. Verrà applicato un backup completo del disco per i processi di backup completo e di verifica.	**Nota:** il comportamento interessa soltanto i processi di backup completo e di verifica. Per un processo di backup incrementale, viene eseguito soltanto il backup dei dati modificati. Per applicare il backup dei blocchi utilizzati per i processi di backup completi e di verifica, procedere come segue: 1. Eliminare tutte le snapshot associate al computer virtuale. 2. Accedere al server proxy di backup. 3. Aprire l'editor del Registro di sistema e cercare la seguente chiave: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\ARCserve Unified Data Protection\Engine\AFBackupDll\<VM-InstanceUUID>* **Nota:** sostituire <VM-InstanceUUID> con il valore dell'UUID del computer virtuale su cui si verifica l'errore della funzionalità di traccia dei blocchi modificati. Il valore può essere reperito nell'URL del computer virtuale utilizzato durante la connessione all'agente Arcserve UDP (Windows). 4. Impostare la chiave del Registro di sistema su "full disk

		backupForFullBackup"=0. 5. Creare/impostare il registro di sistema su ResetCBT=1. 6. Inoltrare il processo di backup.

Strumenti VMware

Stato	Messaggio	Soluzione
Avviso	Non aggiornato.	Installare la versione più recente degli strumenti VMware.
Avviso	Non installato o non in esecuzione.	Installare la versione più recente degli strumenti VMware e verificarne l'esecuzione.

Disco

Stato	Messaggio	Soluzione
Errore	Le snapshot di computer virtuale non sono supportate dal computer virtuale perché il controller SCSI è stato configurato per la configurazione della condivisione dei bus.	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'Agente Arcserve Unified Data Protection per Windows per eseguire il backup del computer virtuale.
Avviso	Non verrà eseguito il backup del disco fisico di mapping della periferica non formattata.	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'Agente Arcserve Unified Data Protection per Windows per eseguire il backup del computer virtuale.
Avviso	Il backup del disco virtuale di mapping della periferica non formattata verrà eseguito come disco completo.	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'Agente Arcserve Unified Data Protection per Windows per eseguire il backup del computer virtuale.
Avviso	Non verrà eseguito il backup del disco indipendente.	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'Agente Arcserve Unified Data Protection per Windows per eseguire il backup del computer virtuale.
Avviso	Per i processi di backup completi o di verifica, il disco sull'archivio dati NFS viene sottoposto a backup come disco completo.	**Nota**: il comportamento interessa soltanto i processi di backup completo e di verifica. Per un processo di backup incrementale, viene eseguito soltanto il backup dei dati modificati. Spostare il disco virtuale in un archivio dati o in una periferica di archiviazione di blocco, oppure creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'Agente Arcserve Unified Data Protection per Windows per eseguire il backup del computer virtuale.

Stato di alimentazione

Stato	Messaggio	Soluzione
Avviso	Disattivato	Avviare il computer virtuale.

Avviso	Sospeso	Avviare il computer virtuale.

Coerenza dei dati

Stato	Messaggio	Soluzione
Avviso	VMware non supporta la disattivazione a livello di applicazione per un computer virtuale con dischi IDE.	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'Agente Arcserve Unified Data Protection per Windows per eseguire il backup dei dati di Microsoft SQL Server e di Exchange Server.
Avviso	VMware non supporta la disattivazione a livello di applicazione per un computer virtuale con dischi SATA.	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'agente Arcserve Unified Data Protection per eseguire il backup dei dati di Microsoft SQL Server e di Exchange Server.
Avviso	VMware non supporta la disattivazione a livello di applicazione perché la versione del server ESX è precedente alla versione 4.1.	Eseguire l'aggiornamento di ESX Server alla versione 4.1 o successiva, oppure creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'Agente Arcserve Unified Data Protection per Windows per eseguire il backup dei dati di Microsoft SQL Server e di Exchange Server.
Avviso	VMware non supporta la disattivazione a livello di applicazione perché gli slot SCSI disponibili non sono sufficienti	Aggiungere un controller SCSI al computer virtuale dal client Web vSphere oppure creare un piano di backup basato sull'agente Arcserve Unified Data Protection. In alternativa, utilizzare Agente Arcserve Unified Data Protection per Windows per eseguire il backup dei dati di Microsoft SQL Server ed Exchange Server.
Avviso	VMware non supporta la disattivazione a livello di applicazione se il sistema operativo guest contiene dischi dinamici.	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'Agente Arcserve Unified Data Protection per Windows per eseguire il backup dei dati di Microsoft SQL Server e di Exchange Server. **Nota**: VMware non supporta la disattivazione a livello di applicazione su computer virtuali Windows Server 2008 con dischi di base o dinamici.
Avviso	Not verified because the application failed to access the virtual machine. Verify that the user credentials are correct and	Fornire le credenziali predefinite dell'amministratore locale o dell'amministratore di dominio per acce-

	have administrative privileges.	dere al sistema operativo guest del computer virtuale. Inoltre, verificare che gli strumenti VMware all'interno del computer virtuale siano aggiornati e in esecuzione. A causa di una limitazione di VMware, il backup è supportato soltanto sui computer virtuali eseguiti in un server ESX con licenza a pagamento. Il backup non viene supportato sui server ESXi con licenza gratuita. **Nota:** la verifica della coerenza dei dati è supportata su Windows Server 2008 e versioni successive.
Avviso	Se il computer virtuale non è attivato, non si può verificare la possibilità di eseguire il backup dei dati.	Fare riferimento alla colonna Stato alimentazione
Avviso	VMware non supporta la disattivazione a livello di applicazione se il sistema operativo guest contiene aree di archiviazione abilitate. Il recupero a livello di file è supportato soltanto per i volumi con spazi di archiviazione non sono abilitati. (Il recupero completo del computer virtuale è supportato tramite Recupera computer virtuale).	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'Agente Arcserve Unified Data Protection per Windows per eseguire il backup dei dati di Microsoft SQL Server e Microsoft Exchange Server.

Creazione di snapshot coerenti con l'applicazione per VMware

In alcuni casi, il writer VMware VSS non crea snapshot coerenti con l'applicazione su alcuni computer virtuali. Di conseguenza, i dati oggetto del backup potrebbero non trovarsi in uno stato coerente.

Verificare i prerequisiti:

Completare i prerequisiti seguenti per creare snapshot coerenti con l'applicazione:

- Gli strumenti VMware più recenti devono essere installati e in esecuzione nel sistema operativo guest del computer virtuale. Inoltre, assicurarsi che il servizio del fornitore della snapshot VMware sia installato (non è necessario che sia in esecuzione).
- È necessario eseguire il computer virtuale su ESXi 4.1 o versione successiva.
- Il computer virtuale deve utilizzare solo dischi SCSI. Il computer virtuale deve disporre di un numero di slot SCSI liberi pari al numero dei dischi.
- La disattivazione coerente con l'applicazione non è supportata per il computer virtuale con dischi IDE o SATA.
- Tutti i volumi nel computer virtuale sono dischi di base e non è presente alcun disco dinamico.
- Il sistema operativo guest non dispone di aree di archiviazione abilitate.
- È necessario configurare il parametro disk.EnableUUID del computer virtuale. I computer virtuali creati con le versioni 4.1 (o versioni successive) dispongono del parametro abilitato per impostazione predefinita. Le seguenti configurazioni vengono eseguite automaticamente dal processo di backup per evitare incoerenze di dati e per eseguire backup conformi alle applicazioni. Se il processo di backup non può abilitare disk.EnableUUID, configurare il parametro manualmente attenendosi alla seguente procedura:
  - Se disk.EnableUUID esiste ed è impostato su FALSE, impostarlo su TRUE.
  - Se disk.EnableUUID non esiste, crearlo e impostarlo su TRUE.
  - Se disk.EnableUUID esiste ed è impostato su TRUE, non modificare le impostazioni.

  Nota: Per ulteriori informazioni sulla creazione di backup coerenti, fare riferimento all'articolo VMware della Knowledge Base.

Funzionalità interessate:

Se i requisiti non vengono rispettati, i dati della sessione saranno coerenti con l'arresto anomalo. Di conseguenza, ciò interesserà le funzionalità seguenti:

- I dati sottoposti a backup che includono dati di applicazione dei computer virtuali, come ad esempio SQL, Exchange e SharePoint possono rimanere in stato di arresto anomalo.
- Il processo di catalogo potrebbe non riuscire.

Soluzioni per gli elementi di verifica preliminare dei computer virtuali Hyper-V

Altri riferimenti:

- Soluzioni per gli elementi di verifica preliminare dei computer virtuali VMware
- Soluzioni per gli elementi di verifica preliminare dei computer virtuali Nutanix AHV

Le tabelle seguenti descrivono le soluzioni per gli errori e avvisi contenuti nei risultati della verifica preliminare per i computer virtuali Hyper-V:

Credenziali Hyper-V

Stato	Messaggio	Soluzione
Errore	Impossibile accedere alla condivisione ADMIN$per il server Hyper-V oppure l'utente non dispone delle credenziali corrette.	■ Verificare che il server Hyper-V sia in esecuzione ■ Verificare se la connessione della rete del server Hyper-V è possibile. ■ Verificare se la condivisione ADMIN$ del server Hyper-V è abilitata. ■ Fornire i diritti di amministratore di Hyper-V quando si importa il computer virtuale da esso.

Servizi integrazione

Stato	Messaggio	Soluzione
Avviso	Non installato, in esecuzione, operativo.	Installare/aggiornare/abilitare i servizi di integrazione. **Note:** ■ Se i servizi di integrazione sono installati per il computer virtuale di Windows, verificare che i due seguenti servizi obbligatori siano in esecuzione sul computer virtuale: Servizio Scambio di dati Hyper-V e Richiedente Copia Shadow del volume Hyper-V. Verificare inoltre la presenza di errori dei servizi Hyper-V nel registro eventi del computer virtuale. ■ Per i computer virtuali Linux, verificare l'installazione

		dei servizi di integrazione più recenti e che le funzionalità di *coppia chiave-valore* e del *backup in tempo reale del computer virtuale* siano disponibili per il computer virtuale Linux. Per ulteriori informazioni sui servizi integrati di Linux nei computer virtuali Hyper-V, fare riferimento all'articolo della Knowledge Base di Microsoft.
Avviso	Non risponde	Riavviare i servizi di integrazione sul sistema operativo guest del computer virtuale.
Avviso	Il servizio di integrazione all'interno del computer virtuale non è compatibile con il servizio di integrazione nel server Hyper-V.	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'agente Arcserve Unified Data Protection per eseguire il backup del computer virtuale.
Avviso	Non aggiornato.	Eseguire l'aggiornamento dei servizi di integrazione.

Stato di alimentazione

Stato	Messaggio	Soluzione
Avviso	Disattivato.	Avviare il computer virtuale.
Avviso	Sospeso.	Avviare il computer virtuale.

Disco

Stato	Messaggio	Soluzione
Avviso	Non viene eseguito il backup del disco rigido fisico connesso al computer virtuale.	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'agente Arcserve Unified Data Protection per eseguire il backup del computer virtuale.
Avviso	Impossibile ottenere le informazioni sul computer virtuale dall'istanza UUID.	Verificare se il computer virtuale esiste sul server Hyper-V.

Coerenza dei dati

Stato	Messaggio	Soluzione
Avviso	Una snapshot coerente con l'applicazione non è supportata. Il computer virtuale ha un disco dinamico.	Creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'agente Arcserve Unified Data Protection per eseguire il backup del computer virtuale.
Avviso	Una snapshot coerente con l'applicazione non è supportata in quanto il computer virtuale contiene spazi di archiviazione.	Creare un piano di backup basato su agente in Arcserve UDP o utilizzare l'agente di Arcserve UDP per eseguire il backup del computer virtuale.

Avviso	Una snapshot coerente con l'applicazione non è supportata poiché il computer virtuale dispone di un volume la cui area di archiviazione della copia shadow si trova su un altro volume.	Modificare l'area di archiviazione della copia shadow del volume impostandola sul volume stesso. **Nota:** Per un computer virtuale Hyper-V 2012 R2, se sull'host Hyper-V viene applicato l'aggiornamento più recente di Microsoft, la snapshot coerente con l'applicazione è ancora supportata in tali casi.
Avviso	Una snapshot coerente con l'applicazione non è supportata. Il computer virtuale ha file system diversi da NTFS/ReFS.	Se si desidera eseguire il backup del computer virtuale ma ignorare i file system non NTFS/ReFS, creare un piano di backup basato su agente in Arcserve Unified Data Protection o utilizzare l'agente Arcserve Unified Data Protection per eseguire il backup del computer virtuale. **Nota:** Per un computer virtuale Hyper-V 2012 R2, se sull'host Hyper-V viene applicato l'aggiornamento più recente di Microsoft, la snapshot coerente con l'applicazione è ancora supportata in tali casi.
Avviso	Una snapshot coerente con l'applicazione non è supportata. La funzionalità ScopeSnapshot viene abilitata nel computer virtuale.	Disattivare la funzionalità ScopeSnapshot nel computer virtuale aggiungendo una chiave di registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\ScopeSnapshots con valore 0.
Avviso	Una snapshot coerente con l'applicazione non è supportata. Il servizio di integrazione non è operativo (stato Non riuscito).	Fare riferimento alla colonna Servizi integrazione.
Avviso	Non verificato perché l'applicazione non è riuscita a ottenere il computer virtuale in base all'istanza UUID.	Verificare se il computer virtuale esiste sul server Hyper-V.
Avviso	Non verificato perché il computer virtuale non è acceso.	Fare riferimento alla colonna Stato alimentazione.
Avviso	Una snapshot coerente con l'applicazione non è supportata. Impossibile accedere al computer virtuale per verificare il motivo.	Fornire le credenziali predefinite dell'amministratore locale o dell'amministratore di dominio per accedere al sistema operativo guest del computer virtuale. Verificare inoltre che il computer virtuale disponga della connettività di rete.
Avviso	Una snapshot coerente con l'applicazione non è supportata per una ragione sconosciuta.	Per identificare il motivo per cui è impossibile acquisire una snapshot coerente con l'applicazione, controllare i registri eventi. Il registro eventi si trova nella posizione seguente:

		Computer virtuale: Visualizzatore eventi > Registri di Windows > Eventi di applicazione e sistema. Nel registro, cercare gli errori che provengono da Disco, VSS e VolSnap. Server Hyper-V: Visualizzatore eventi > Registri di Windows > Registri applicazioni e servizi > Microsoft > Windows > Hyper-V-*. Nel registro, cercare gli errori per il computer virtuale corrispondente.

Creazione di snapshot coerenti con l'applicazione per Hyper-V

In alcuni casi, il writer Hyper-V VSS non crea snapshot coerenti con l'applicazione su alcuni computer virtuali. Di conseguenza, i dati oggetto del backup potrebbero non trovarsi in uno stato coerente.

Verificare i prerequisiti:

Completare i prerequisiti seguenti per creare snapshot coerenti con l'applicazione:

- Nel computer virtuale figlio, il servizio di integrazione denominato Richiedente copia shadow del volume Hyper-V è installato e in esecuzione.
- Il computer virtuale figlio è in esecuzione.
- La posizione dei file snapshot VM per il computer virtuale è impostata in modo tale che il volume sia lo stesso nel sistema operativo host e nei file VHD per il computer virtuale.
- Tutti i volumi nel computer virtuale figlio sono dischi di base e non è presente alcun disco dinamico.
- Tutti i dischi nel computer virtuale figlio devono utilizzare un file system che supporta le snapshot (ad esempio, NTFS).

Verificare le considerazioni:

Completare le considerazioni seguenti per creare snapshot coerenti con l'applicazione:

- Il servizio di integrazione installato nel computer virtuale figlio deve essere compatibile con l'host Hyper-V.
  - Esempio: Il servizio di integrazione Windows 8.1/2012R2 all'interno del computer virtuale non è compatibile con l'host Hyper-V di Windows 2008R2.
- Per Windows 8, 2012 e versioni successive e per il computer virtuale in esecuzione sull'host Hyper-V di Windows 2008R2, è necessario disattivare la funzionalità ScopeSnapshot nel computer virtuale. Per disattivare la funzionalità ScopeSnapshot, seguire questi passaggi:
  1. Accedere alla macchina virtuale.
  2. Accedere alla posizione seguente:

     HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
  3. Aprire la chiave SystemRestore.

Nota: Creare la chiave se non esiste.

4. Aggiungere un valore del Registro di sistema DWORD a 32 bit denominata "ScopeSnapshots" e impostare il valore su 0.

Funzionalità interessate:

Se i requisiti non vengono soddisfatti, i dati della sessione saranno coerenti con l'arresto anomalo. Di conseguenza, ciò interesserà le funzionalità seguenti:

- I dati sottoposti a backup che includono dati di applicazione dei computer virtuali, come ad esempio SQL, Exchange e SharePoint possono rimanere in stato di arresto anomalo.
- Il processo di catalogo potrebbe non riuscire.

Soluzioni per gli elementi di verifica preliminare dei computer virtuali Nutanix AHV

Altri riferimenti:

- Soluzioni per gli elementi di verifica preliminare dei computer virtuali VMware
- Soluzioni per gli elementi di verifica preliminare dei computer virtuali Hyper-V

Le tabelle seguenti descrivono le soluzioni per gli errori e gli avvisi contenuti nei risultati della verifica preliminare per i computer virtuali Nutanix AHV:

Nutanix Guest Tools (NGT)

Stato	Messaggio	Soluzione
Avviso	Non in esecuzione	Abilitare Nutanix Guest Tools per il computer virtuale.
Avviso	Strumenti abilitati	Guest Tools è abilitato ma non in esecuzione. Installare Guest Tools nel computer virtuale.

Stato di alimentazione

Stato	Messaggio	Soluzione
Avviso	Disattivato	Avviare il computer virtuale.
Avviso	Sospeso	Continuare con il computer virtuale.

Coerenza dei dati

Stato	Messaggio	Soluzione
Avviso	Nutanix AHV non supporta la disattivazione a livello di applicazione per un computer virtuale con dischi IDE.	Creare un piano di backup basato sull'agente in Arcserve UDP o utilizzare l'agente Arcserve UDP (Windows) per eseguire il backup dei dati di Microsoft SQL Server ed Exchange Server.
Avviso	Nutanix AHV non supporta la disattivazione a livello di applicazione per un computer virtuale con dischi SATA.	Creare un piano di backup basato sull'agente in Arcserve UDP o utilizzare l'agente Arcserve UDP per eseguire il backup dei dati di Microsoft SQL Server ed Exchange Server.
Avviso	Nutanix AHV non supporta la disattivazione a livello di applicazione perché gli slot SCSI non sono sufficienti.	Creare un piano di backup basato sull'agente in Arcserve UDP o utilizzare l'agente Arcserve UDP (Windows) per eseguire il backup dei dati di Microsoft SQL Server ed Exchange Server.
Avviso	Not verified because the application failed to access the virtual machine. Verify that the user credentials are correct and have administrative privileges.	Fornire le credenziali predefinite dell'amministratore locale o dell'amministratore di dominio per accedere al sistema operativo guest del computer virtuale.

Avviso	Se il computer virtuale non è attivato, non si può verificare la possibilità di eseguire il backup dei dati.	Fare riferimento alla colonna Stato alimentazione.

Aggiunta e gestione del percorso UNC/NFS

Il percorso UNC/NFS è stato introdotto come tipo di nodo in Arcserve UDP. A differenza di altri nodi, non è possibile aggiungere il nodo del percorso UNC/NFS dalla sezione Tutti i nodi. Come i nodi di Exchange Online, è possibile aggiungere il nodo di percorso UNC/NFS solo durante la creazione di un piano. Una volta aggiunto, è possibile gestire il nodo di percorso UNC/NFS dalla sezione Tutti i nodi per aggiornarlo o eliminarlo.

Come procedere?

- Aggiunta di un percorso UNC/NFS
- Aggiornamento del percorso UNC/NFS
- Eliminazione di un percorso UNC/NFS

Aggiunta di un percorso UNC/NFS

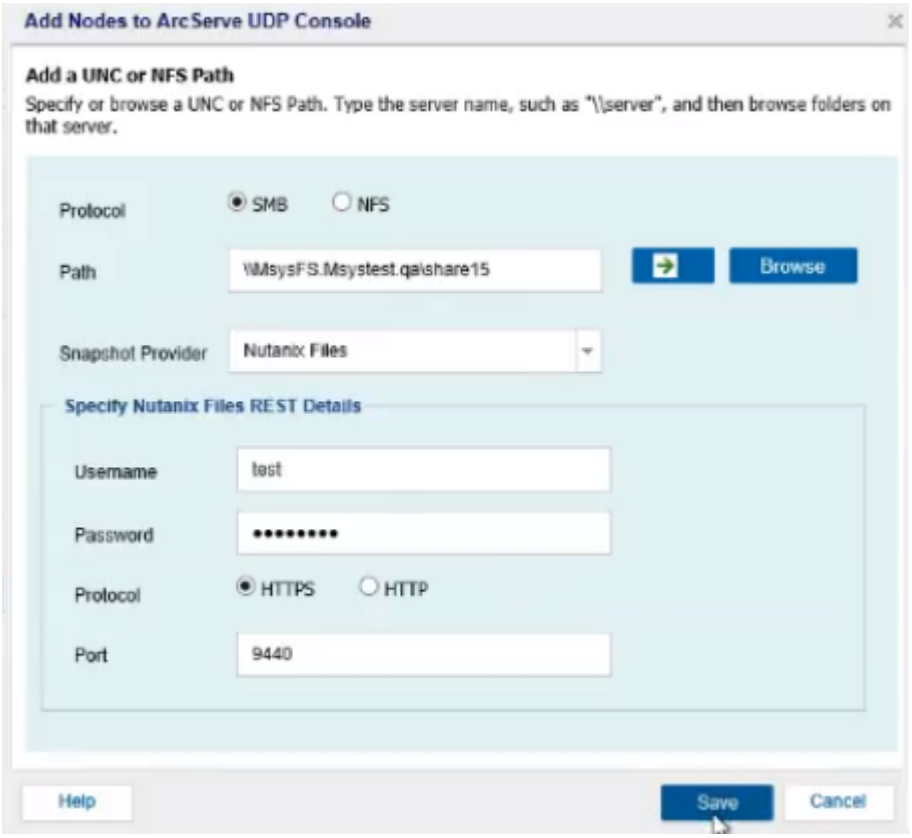
È possibile aggiungere un percorso UNC/NFS solo durante la creazione di un piano di backup del percorso UNC/NFS. Durante la creazione del piano, dalla scheda **Origine** è possibile aggiungere un nodo del percorso UNC/NFS .

Effettuare le operazioni seguenti:

1. Dalla scheda **Origine** del piano di backup del percorso UNC, fare clic sull'opzione **Aggiungi percorso UNC o NFS.**

   Viene visualizzata la finestra di dialogo Aggiungi nodi alla Console di Arcserve UDP.

2. Nella pagina Aggiungi un percorso UNC o NFS, procedere come segue:



   a. Selezionare **SMB** o **NFS** come protocollo.

      - Se si seleziona **SMB**, procedere come segue:

        1. Immettere il percorso UNC nel formato seguente:

           *Hostname**share*

           Note:

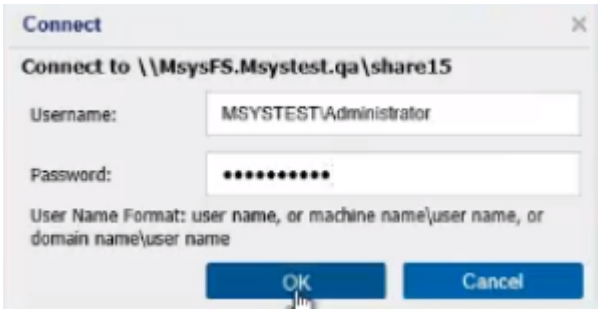
- Pur fornendo la condivisione Nutanix Files come origine per il backup con Nutanix Files come provider di snapshot, i backup possono essere eseguiti solo a livello di condivisione ma non a livello di sottocartella.
- Per ottenere il percorso UNC, procedere come segue:
  a. Selezionare la condivisione appena creata nel riquadro centrale.
  b. Nella colonna Condividi/Esporta dettagli, dal riquadro Riepilogo, accedere a **Percorso di montaggio**, quindi copiare il percorso di montaggio.

     Se il percorso UNC è valido, vengono visualizzate una freccia rivolta verso destra e l'opzione Sfoglia.

2. Fare clic sulla freccia destra (>) per convalidare il percorso UNC.

   Viene visualizzata la finestra di dialogo Connetti.

3. Immettere il nome utente e la password, quindi fare clic su **OK**.



   Nella finestra di dialogo Aggiungi nodi alla console Arcserve UDP viene riportato il percorso UNC verificato.

- Se si seleziona NFS, procedere come segue:

  1. Immettere il percorso UNC nel formato seguente:

     *Hostname**share*

  2. Selezionare codifica dalle opzioni disponibili - ANSI, GB2312-80, KSC5601, BIG5, SHIFT JIS, EUC-KR, EUC-TW, EUC-JP.

     Il valore predefinito è ANSI.

     Nota: durante il backup di una cartella NFS condivisa, tutti i file e le cartelle il cui nome è associato a una codifica di lingua non supportata vengono ignorati oppure il loro nome non viene visualizzato correttamente.

b. Dall'elenco a discesa Provider snapshot, selezionare **Nutanix Files**.

c. Per la casella Specificare i dettagli REST di Nutanix Files, fornire le seguenti credenziali:

Nome utente

Fa riferimento al nome utente creato dall'utente dell'API REST utilizzando Nutanix Prism.

Nota: Per una comunicazione più sicura, selezionare il protocollo HTTPS.

Password

Fa riferimento alla password per il nome utente.

Protocollo

Specificare il protocollo che si desidera utilizzare per la comunicazione con il server di destinazione. Le opzioni disponibili sono HTTP e HTTPS.

Porta

Si riferisce al numero di porta. Il valore predefinito della porta è 9440, il quale consente di accedere alle chiamate API REST e a Prism.

3. Fare clic su **Salva**.

È possibile aggiornare o eliminare il nodo del percorso UNC/NFS.

Aggiornamento del percorso UNC/NFS

È possibile aggiornare le informazioni relative ai nodi esistenti. Quando si modificano le credenziali del percorso UNC/NFS, è necessario aggiornare il percorso UNC/NFS nella Console.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

2. Dal riquadro sinistro, accedere a **Nodi** e selezionare **Percorsi UNC/NFS**.

   I nodi di percorso UNC/NFS esistenti vengono mostrati nel riquadro centrale.

3. Nel riquadro centrale, selezionare un percorso UNC/NFS e fare clic su **Azioni**.

   Viene visualizzato l'elenco delle opzioni disponibili.

4. Dall'elenco, fare clic su **Aggiorna**.

   Viene visualizzata la finestra di dialogo **Aggiorna nodo**.

5. Aggiornare i dettagli e fare clic su **OK**.

   Le informazioni sul nodo sono state aggiornate.

Eliminazione di un percorso UNC/NFS

È possibile eliminare un nodo di percorso UNC/NFS esistente dalla scheda **Risorse**:

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

2. Dal riquadro sinistro, accedere a **Nodi** e selezionare **Percorsi UNC/NFS**.

   I nodi di percorso UNC/NFS esistenti vengono mostrati nel riquadro centrale.

3. Selezionare il nodo di percorso UNC/NFS e fare clic su **Azioni**.

   Viene visualizzato l'elenco delle opzioni disponibili.

4. Fare clic su **Elimina**.

   Viene visualizzata una finestra di dialogo di conferma.

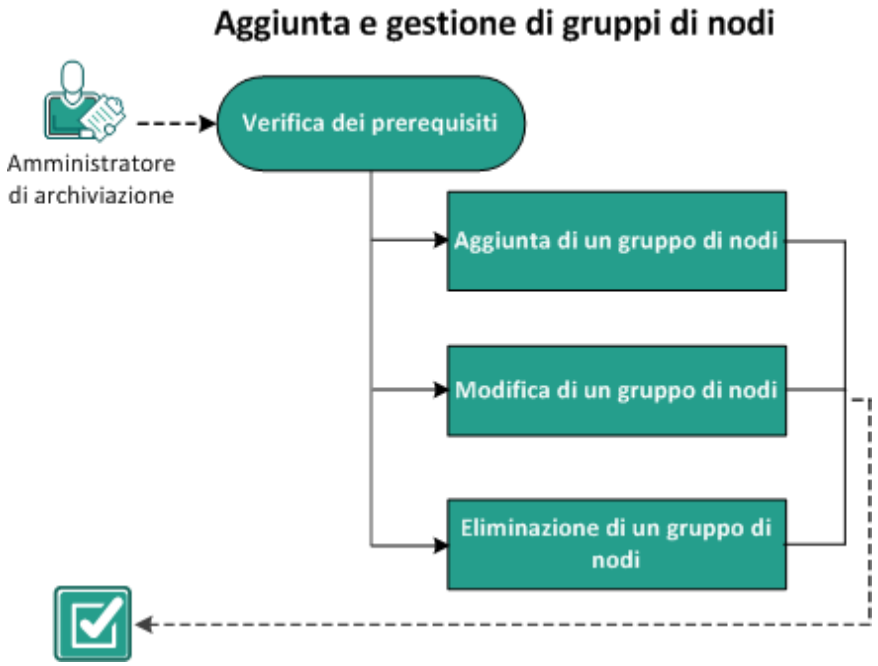
5. Fare clic su **OK**.

   Il percorso UNC/NFS viene eliminato.

Aggiunta e gestione di gruppi di nodi

Arcserve Unified Data Protection consente di aggiungere più nodi a un gruppo. È possibile aggiungere i gruppi di nodi per gestire l'ambiente fisico e del computer virtuale.

Nel diagramma seguente viene illustrato come aggiungere e gestire i gruppi di nodi:



La soluzione Arcserve Unified Data Protection contiene i gruppi di nodi seguenti:

- Gruppi predefiniti:
  - **Tutti i nodi**: vengono visualizzati tutti i nodi aggiunti alla Console.
  - **Nodi senza un piano**: vengono visualizzati i nodi che non hanno nessun piano assegnato.

  Nota: i gruppi di nodi predefiniti non possono essere modificati o eliminati.
- Gruppi visualizzati quando si aggiungono gruppi figli:
  - **Gruppi di piani**: viene visualizzato l'elenco di piani creati dall'utente. Selezionare ciascun piano sotto il gruppo per visualizzare tutti i nodi associati con quel piano.
  - **Gruppi personalizzati**: viene visualizzato l'elenco di gruppi di nodi personalizzati creati dall'utente. Ad esempio, il gruppo di nodi creato facendo clic su **Azioni**, **Gruppo nodi**, **Aggiungi** dal riquadro centrale.

- **Gruppi vCenter/ESX:** vengono visualizzati i nodi aggiunti mediante l'opzione **Importazione da vCenter/ESX**.
- **Gruppo server di backup di Linux:** vengono visualizzati i nodi del server di backup di Linux.
- **Nodi Exchange Online**: consente di visualizzare i nodi Exchange Online.
- **Percorsi UNC**: consente di visualizzar i nodi UNC.
- **Gruppi di profili SLA**: consente di visualizzare i nodi relativi al Service Level Agreement (SLA).
- **Gruppi Hyper-V:** vengono visualizzati i nodi aggiunti mediante l'opzione **Importazione da Hyper-V**.
- **Gruppi Global Dashboard:** viene visualizzato tutto il server primario filiale di Arcserve Backup nel server GDB. Il gruppo Global Dashboard viene aggiunto quando si aggiunge un server Global Dashboard di Arcserve Backup nella Console e si esegue una sincronizzazione completa di Arcserve Backup per il server GDB aggiunto.
- **Gruppo database Oracle**: visualizza i nodi del database Oracle.

Come procedere?

- Verifica dei prerequisiti
- Aggiunta di gruppi di nodi
- Modifica di gruppi di nodi
- Eliminazione di gruppi di nodi

Verifica dei prerequisiti

Prima di utilizzare i gruppi di nodo, completare i seguenti passaggi preliminari:

- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.
- Accedere alla Console.
- Aggiungere un nodo.

Aggiunta di gruppi di nodi

Per gestire l'elenco dei nodi, è possibile creare un gruppo per i nodi selezionati. Ad esempio, è possibile raggrupparli per funzione di business o per applicazioni installate. È inoltre possibile aggiungere i nodi a qualsiasi gruppo personalizzato dopo l'aggiunta di un gruppo vuoto.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.
3. Dal riquadro centrale, fare clic sul menu a discesa **Azioni**.
4. Fare clic su **Crea gruppo nodi**.

   Viene aperta la finestra di dialogo **Aggiungi gruppo** contenente tutti i nodi disponibili.
5. Completare le azioni seguenti per aggiungere nodi al gruppo e fare clic su **OK**.
   - Selezionare i nodi che si desidera aggiungere a un gruppo.
   - Fornire un nome al gruppo.

     Nel riquadro a destra viene visualizzata la finestra di dialogo **Informazioni** che notifica la creazione del gruppo di nodi.

Il gruppo aggiunto viene collocato sotto **Gruppi personalizzati** nel riquadro sinistro.

Nota: Le opzioni **Modifica** ed **Elimina** vengono abilitate solo quando è stato aggiunto un gruppo.

Modifica di gruppi di nodi

La soluzione Arcserve Unified Data Protection consente di modificare i gruppi di nodi creati. È possibile aggiungere o rimuovere i nodi dai gruppi di nodi e modificare il nome dei gruppi di nodi.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.
3. Da **Gruppi personalizzati** nel riquadro sinistro, selezionare un gruppo.

   I dettagli del gruppo selezionato vengono visualizzati sul riquadro centrale.
4. Fare clic sull'elenco a discesa **Azioni**, quindi fare clic su **Modifica gruppo nodi**.

   Viene visualizzata la finestra di dialogo **Modifica gruppo**.
5. Aggiornare i dettagli e fare clic su **OK**.

   Il gruppo di nodi è stato aggiornato.

Eliminazione di gruppi di nodi

È possibile eliminare un gruppo, se necessario. Quando si elimina un gruppo aggiunto manualmente, i computer virtuali o fisici non vengono rimossi da Arcserve Unified Data Protection. Tuttavia, se un gruppo creato automaticamente dal rilevamento di un server ESX o vCenter viene eliminato, il gruppo e tutti i computer virtuali verranno eliminati dalla Console.

Importante. Non è possibile eliminare i gruppi di nodi predefiniti.

Nota: Il processo di eliminazione dei gruppi di nodi non comporta l'eliminazione dei singoli nodi dalla console.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.
3. Da **Gruppi personalizzati** nel riquadro sinistro, selezionare un nome gruppo.

   I dettagli del gruppo selezionato vengono visualizzati sul riquadro centrale.
4. Fare clic sull'elenco a discesa **Azioni**, quindi fare clic su **Elimina gruppo nodi**.

   Viene visualizzata la finestra di dialogo **Conferma**.
5. Fare clic su **Sì**.

   Nel riquadro a destra viene visualizzata la finestra di dialogo **Informazioni** che notifica l'eliminazione del gruppo di nodi.

Gestione dei nodi per il cloud

Arcserve UDP consente di eseguire più azioni per la gestione di un nodo per il cloud.

Come procedere?

- Download del punto di ripristino dal cloud
- Caricamento del punto di ripristino su cloud
- Copia del punto di ripristino su disco locale o condivisione di rete

Download del punto di ripristino dal cloud

Questa funzione consente di scaricare i punti di ripristino dal cloud in una condivisione locale o di rete.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

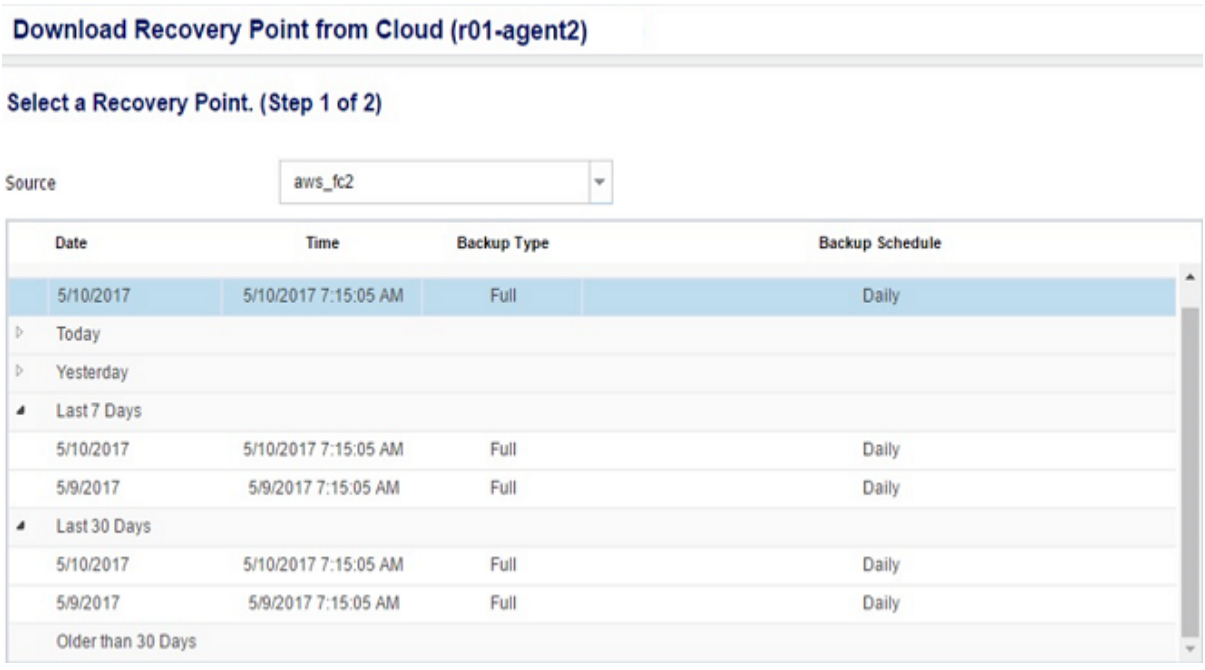
   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

2. Eseguire una delle seguenti operazioni:
   - Fare clic con il tasto destro del mouse sul nome del nodo.
   - Selezionare il nome del nodo e dal riquadro centrale fare clic sull'elenco a discesa **Azioni**.

3. Fare clic su **Scarica punto di ripristino da cloud**.

   Viene visualizzata la pagina **Scarica punto di ripristino da cloud**.

   È possibile scaricare il punto di ripristino dal cloud in due passaggi.

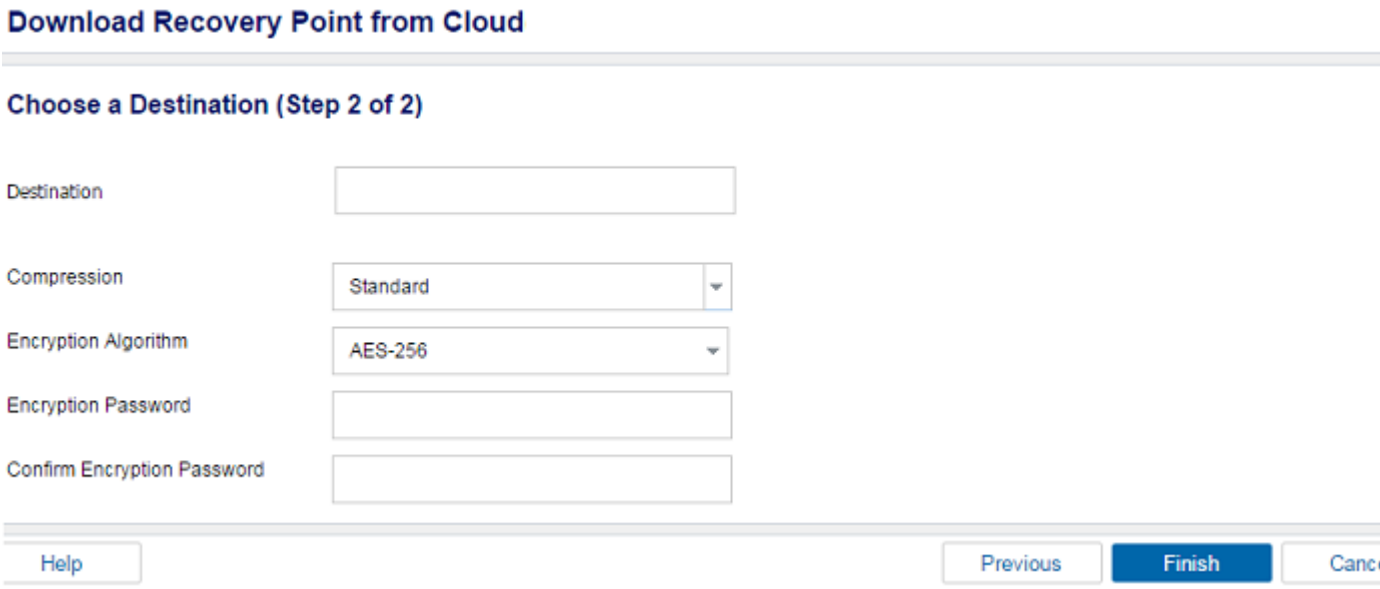


4. Nel passaggio 1, per selezionare un punto di ripristino, procedere come segue, quindi fare clic su **Avanti**.
   a. Dall'elenco a discesa Servizio cloud, selezionare un servizio cloud.
   b. Dal menu a discesa Archiviazione cloud, selezionare un'archiviazione cloud.

c. Dall'elenco a discesa Nome bucket, selezionare un nome bucket contenente un punto di ripristino.

I dettagli del punto di ripristino vengono visualizzati solo quando si configura un'attività CRP nel piano.

Viene visualizzata la schermata Scegliere una destinazione.



5. Nel Passaggio 2, immettere i seguenti dettagli e fare clic su **Fine**.
   a. Indicare una **destinazione**.

      Nota: Se è stata specificata una destinazione remota che richiede la convalida, dopo aver fatto clic su **Fine**, viene visualizzata la finestra di dialogo **Connetti**. Immettere i dettagli per convalidare la destinazione.

   b. Selezionare un tipo di **compressione**.
   c. Selezionare il tipo di **algoritmo di crittografia**.
   d. Immettere la **password di crittografia** due volte.

Il punto di ripristino viene scaricato dal cloud.

Caricamento del punto di ripristino su cloud

Questa funzionalità consente di caricare i punti di ripristino da destinazioni di backup come una condivisione di server RPS, locale o remota su cloud.

Importante! Sono necessari un nodo che disponga di un piano di backup e una sessione di backup completo per la copia sul cloud.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

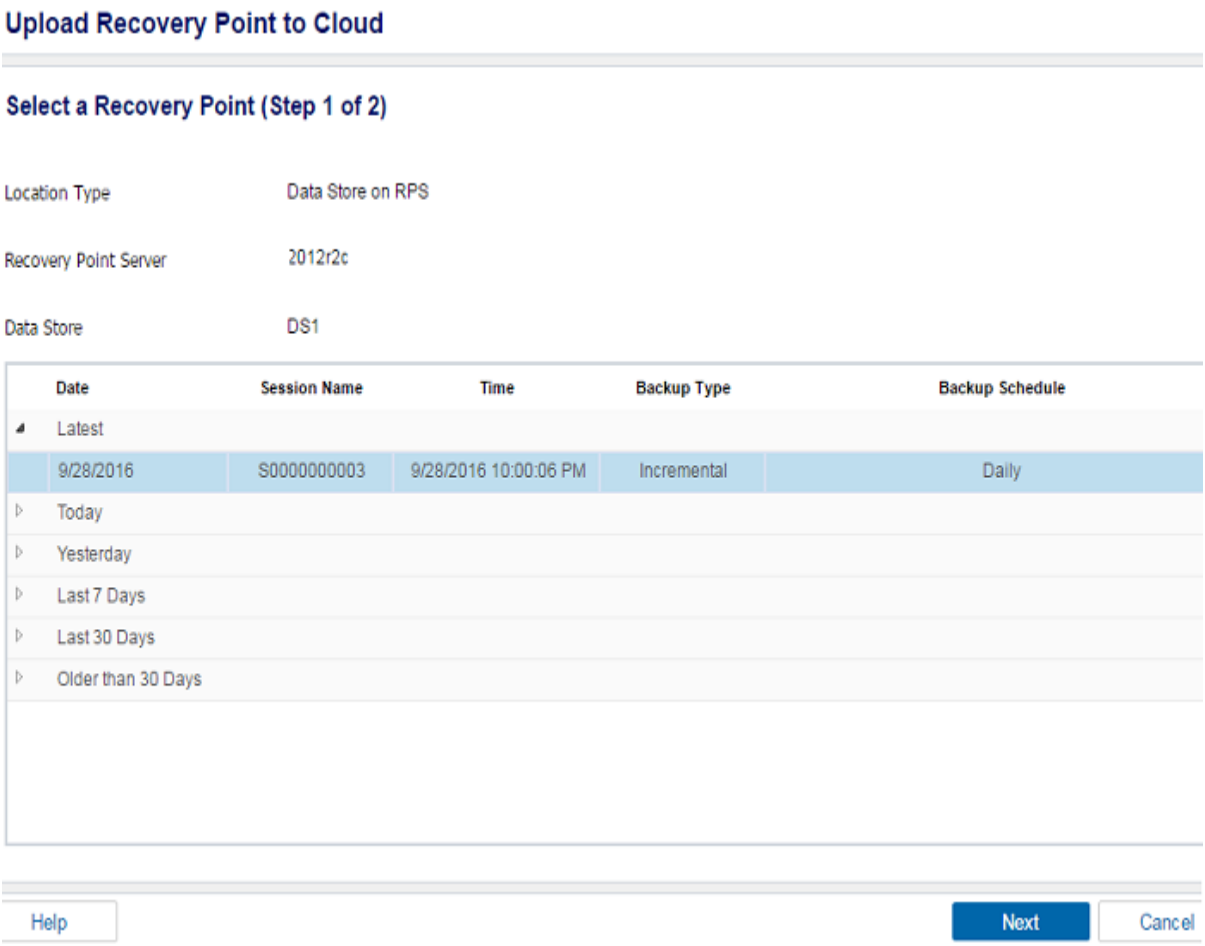
2. Eseguire una delle seguenti operazioni:

   - Fare clic con il tasto destro del mouse sul nome del nodo.
   - Selezionare il nome del nodo e dal riquadro centrale fare clic sull'elenco a discesa **Azioni**.

3. Fare clic su **Carica punto di ripristino su cloud**.

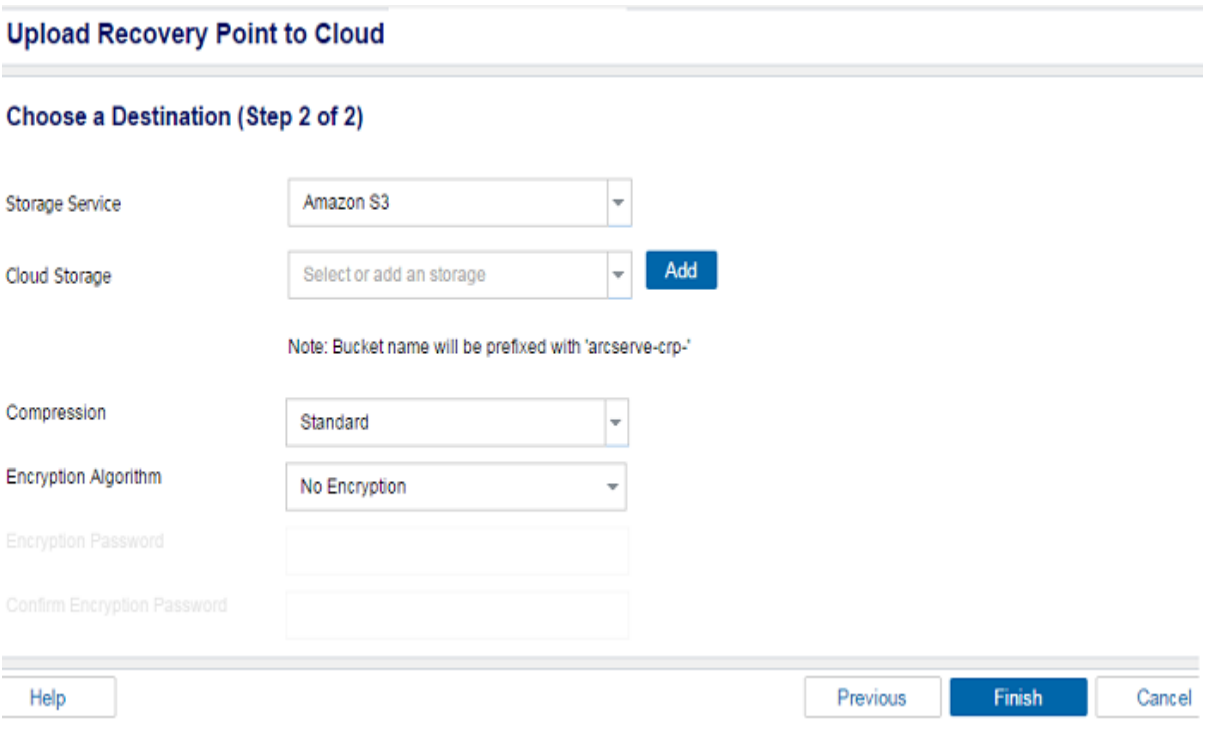
   Viene visualizzata la finestra di dialogo **Carica punto di ripristino su cloud**.

   È possibile caricare il punto di ripristino sul cloud in due passaggi.



4. Nel Passaggio 1, selezionare un **punto di ripristino** e fare clic su **Avanti**.

   Viene visualizzata la schermata successiva di caricamento.



5. Nel Passaggio 2, immettere i seguenti dettagli e fare clic su **Fine**.
   a. Selezionare il **servizio di archiviazione** dall'elenco a discesa.
   b. Selezionare l'**archiviazione cloud** dall'elenco a discesa.

      Nota: Se precedentemente non è stato aggiunto un account cloud, fare clic su **Aggiungi** per aggiungerne uno.
   c. Selezionare il tipo di compressione dall'elenco a discesa.
   d. Selezionare il tipo di **algoritmo di crittografia**.
   e. Immettere la **password di crittografia** due volte.

   Nota: un bucket/contenitore viene creato con la convenzione di denominazione *arcserve-{random-generate-id}-<BucketName>*. Tuttavia, ogni processo di *caricamento del punto di ripristino su cloud* crea un nuovo bucket/contenitore con un ID *{random-generato-id}* univoco. Per il nome esatto del bucket/contenitore, fare riferimento al registro attività del processo.

   Il punto di ripristino viene caricato nel Cloud.

Copia del punto di ripristino su disco locale o condivisione di rete

Questa funzionalità consente di copiare i punti di ripristino da destinazioni di backup come una condivisione di server RPS, locale o remota in locale o in remoto.

Importante! Sono necessari un nodo che disponga di un piano di backup configurato e una sessione di backup completo per la copia in una condivisione locale o remota.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina **Nodi: Tutti i nodi**.

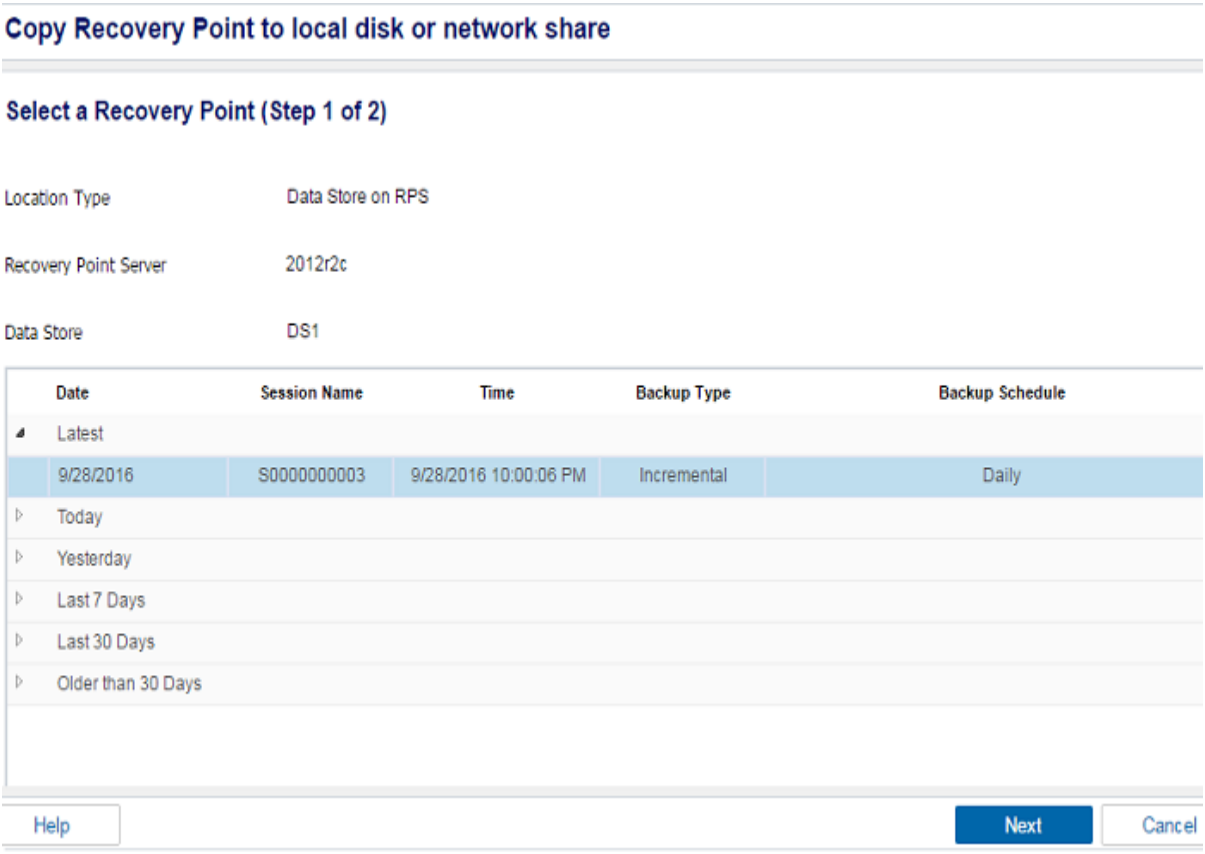
2. Eseguire una delle seguenti operazioni:

   - Fare clic con il tasto destro del mouse sul nome del nodo.
   - Selezionare il nome del nodo e dal riquadro centrale fare clic sull'elenco a discesa **Azioni**.

3. Fare clic su **Copia punto di ripristino su disco locale o condivisione di rete**.

   Viene visualizzata la finestra di dialogo **Copia punto di ripristino su disco locale o condivisione di rete**.

   È possibile copiare il punto di ripristino su disco locale o condivisione di rete in due passaggi.



4. Nel Passaggio 1, selezionare un **punto di ripristino** e fare clic su **Avanti**.

   Viene visualizzata la schermata successiva di copia del punto di ripristino.



5. Nel Passaggio 2, immettere i seguenti dettagli e fare clic su **Fine**.

a. Indicare una **destinazione**.

   Nota: Se è stata specificata una destinazione remota che richiede la convalida, dopo aver fatto clic su **Fine**, viene visualizzata la finestra di dialogo **Connetti**. Immettere i dettagli per convalidare la destinazione.

b. Selezionare un tipo di **compressione**.

c. Selezionare il tipo di **algoritmo di crittografia**.

d. Immettere la **password di crittografia** due volte.

Il punto di ripristino viene copiato dal cloud.

Aggiunta di un array di archiviazione

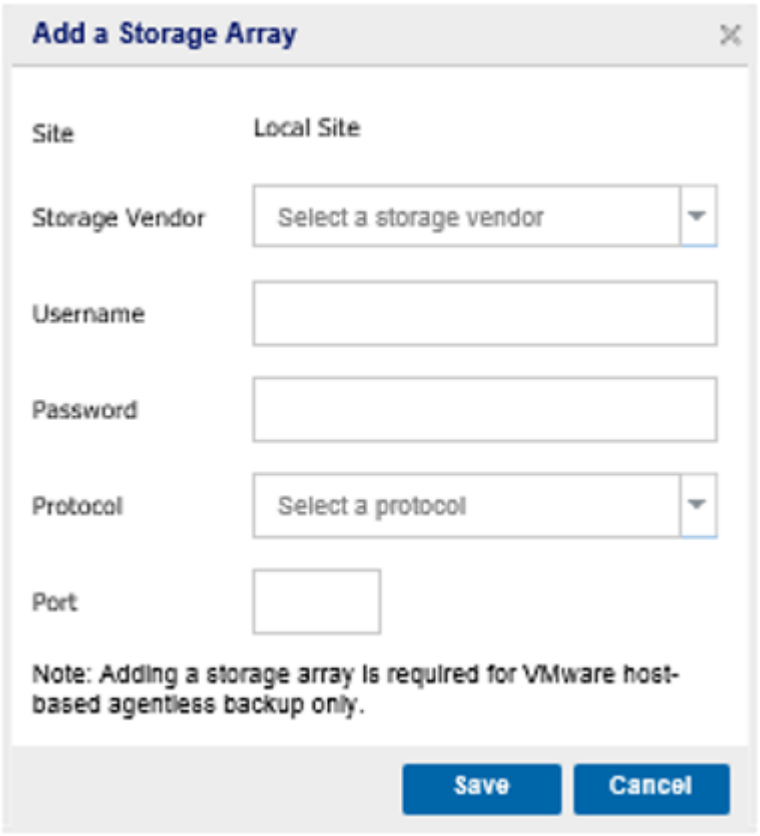
Se si utilizzano le snapshot hardware, è necessario aggiungere alla console i dettagli relativi all'array di archiviazione. Se non si aggiunge l'array di archiviazione e si invia un processo di backup utilizzando la snapshot hardware, il processo di backup cercherà innanzitutto i dettagli dell'array di archiviazione nella console. Se il processo di backup non è in grado di individuare i dettagli dell'array di archiviazione, utilizzerà una snapshot software per creare le sessioni di backup.

L'aggiunta di un array di archiviazione è necessaria soltanto per i backup senza agente basati su host VMware.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic su **Risorse**.
2. Accedere a **Infrastruttura** nel riquadro sinistro e fare clic su **Array di archiviazione**.

   Viene visualizzata la finestra di dialogo **Aggiungi un array di archiviazione**.



È possibile aggiungere un array di archiviazione per le seguenti opzioni:

- NetApp

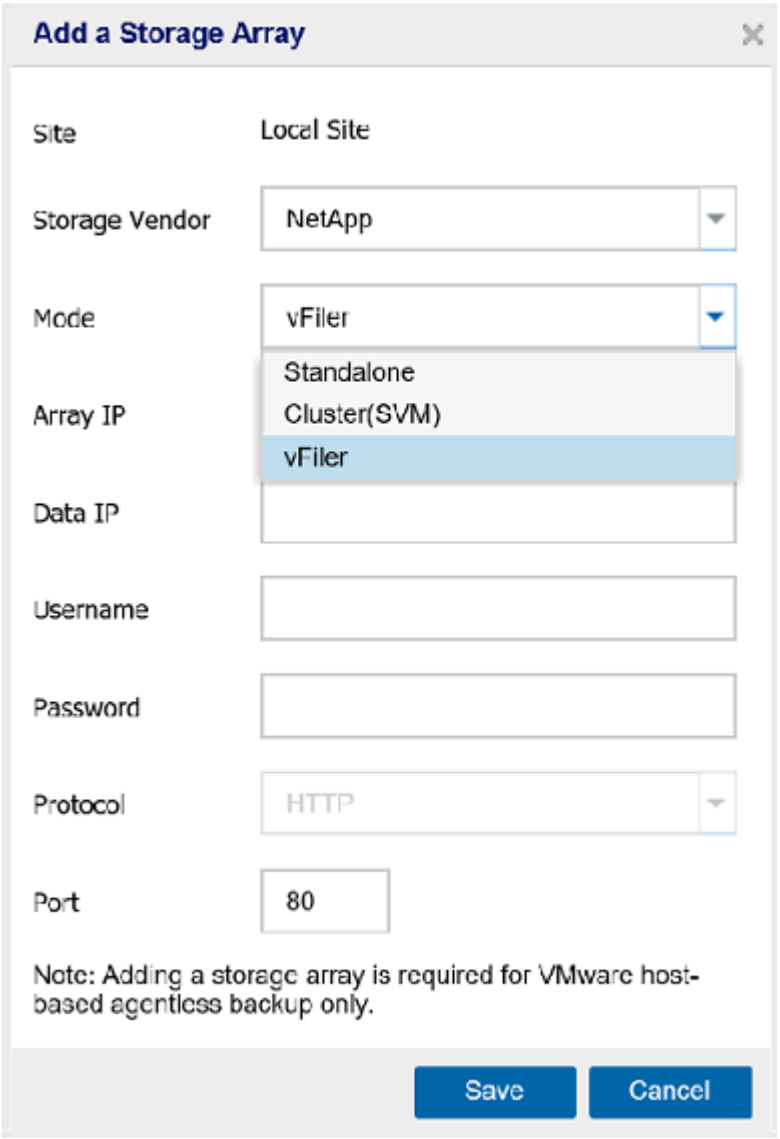
- HPE 3PAR
- Nimble

Aggiunta di un array di archiviazione per NetApp

Per aggiungere un array di archiviazione NetApp, è possibile utilizzare tre opzioni.

Effettuare le operazioni seguenti:

1. Dalla finestra di dialogo **Aggiungi array di archiviazione**, selezionare NetApp dall'elenco a discesa **Fornitore archiviazione**.



2. Da Modalità, selezionare una delle opzioni seguenti per il tipo di array:

Standalone

Specifica che l'array di archiviazione è un dispositivo standalone.

Cluster (SVM)

Specifica che l'array di archiviazione appartiene a un cluster di array.

vFiler

Specifica che l'array di archiviazione è un vFiler.

3. Immettere i dettagli seguenti per il tipo specifico di array:

Sito

Specifica il nome del sito.

IP array

Specifica l'indirizzo IP dell'array. Per 7-mode, specificare l'indirizzo IP che può accedere alla interfaccia iSCSI e NFS. VMware(ESXi) utilizza l'indirizzo IP per accedere all'array di archiviazione per le operazioni di lettura e scrittura. Per gli array cluster e vFiler, specificare l'indirizzo IP di gestione dell'array di archiviazione o del computer virtuale di archiviazione (SVM, Storage Virtual Machine).

Per individuare l'indirizzo IP dell'array, consultare l'argomento Individuazione dell'indirizzo IP dell'array e dei dati dall'array di archiviazione SVM della console Arcserve UDP.

IP dati

Specificare l'IP di accesso ai dati (interfaccia logica) del computer virtuale di archiviazione (SVM), da cui i computer di destinazione (ESXi) possono accedere a questo array di archiviazione per operazioni di lettura e scrittura. Questa opzione è applicabile solo per cluster e vFiler. Se il computer virtuale di archiviazione supporta solo il protocollo FC, immettere NA.

Per individuare l'indirizzo IP dei dati, consultare l'argomento Individuazione dell'indirizzo IP dell'array e dei dati dall'array di archiviazione SVM della console Arcserve UDP.

Nome utente

Specifica il nome utente per la connessione all'array di archiviazione.

Password

Specifica la password per il nome utente.

Protocollo

Specifica il protocollo per la connessione all'array.

Porta

Specifica il numero di porta dell'array.

Impostazione predefinita: 443 (HTTPS), 80 (HTTP)

4. Fare clic su **Salva**.

L'array di archiviazione è stato aggiunto alla console.

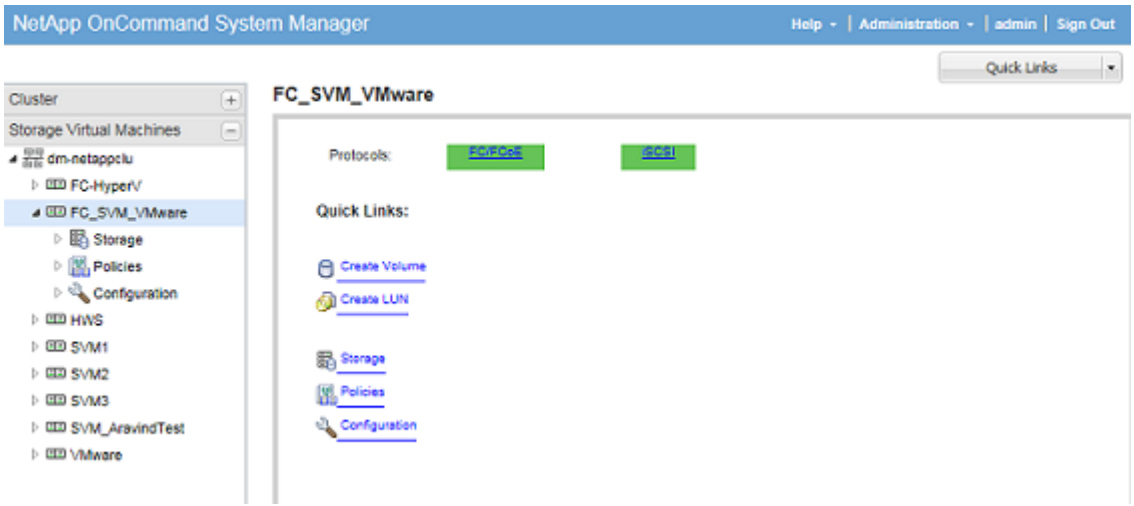
Individuazione dell'indirizzo IP dell'array e dei dati dall'array di archiviazione SVM della console Arcserve UDP

In questa sezione viene descritta la procedura per individuare l'indirizzo IP dell'array e dei dati quando l'array di archiviazione NetApp è in esecuzione in modalità cDOT(cluster).

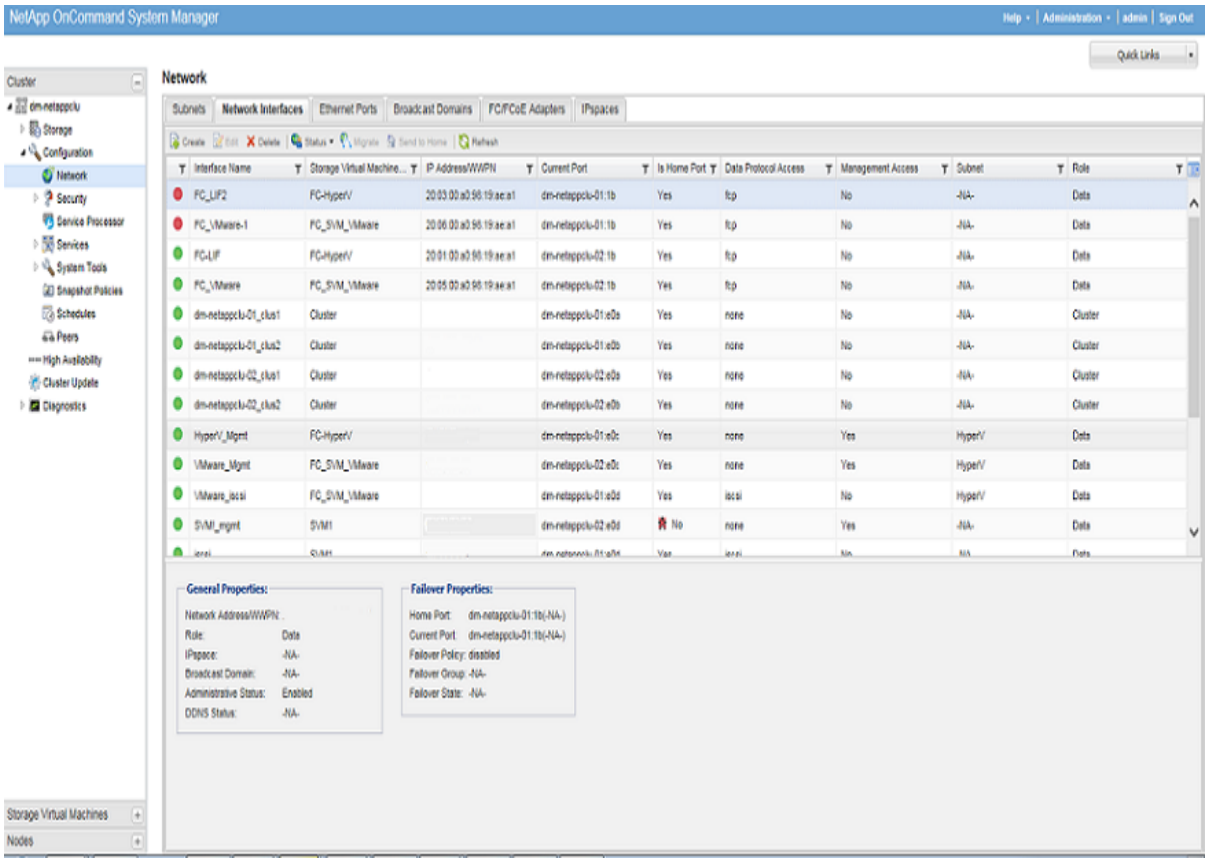
Nota: Applicabile solo al cluster (SVM).

Effettuare le operazioni seguenti:

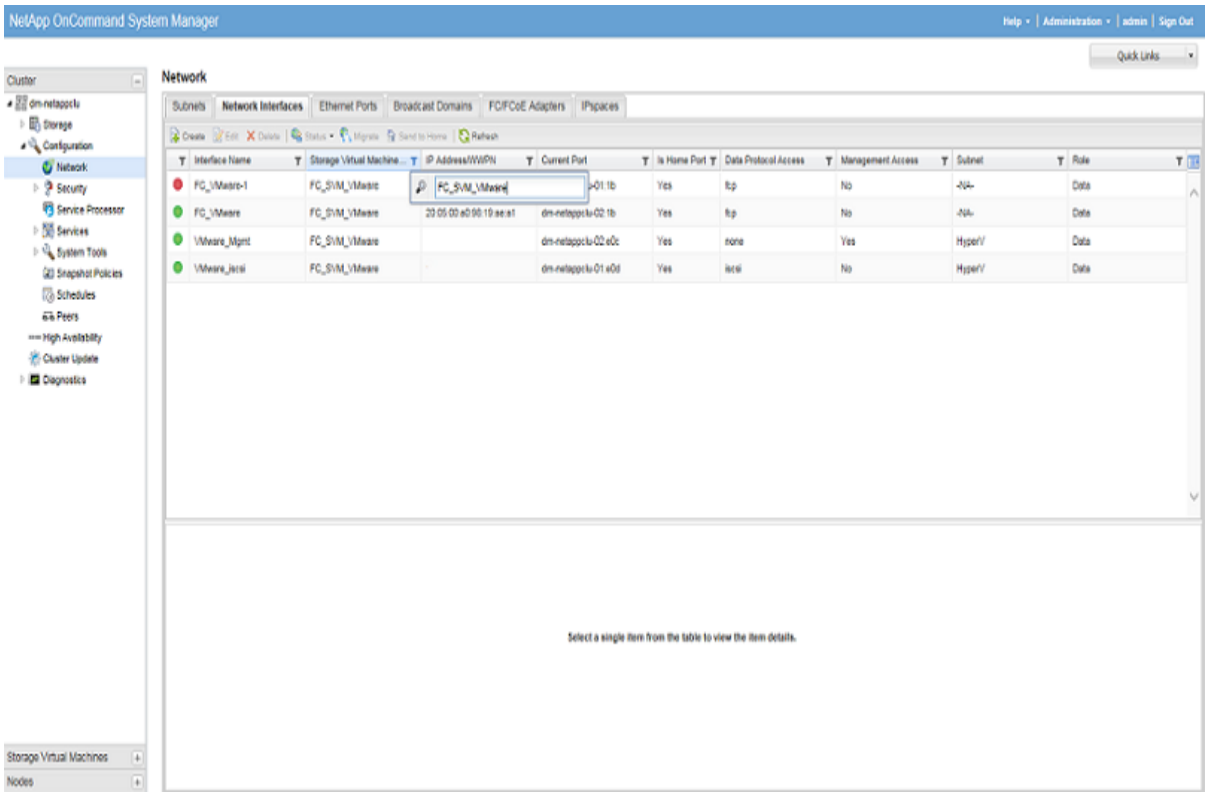
1. Accedere all'utilità di gestione del sistema NetApp e connettersi al cluster utilizzando credenziali utente valide.
2. Identificare il computer SVM da aggiungere alla console Arcserve UDP.



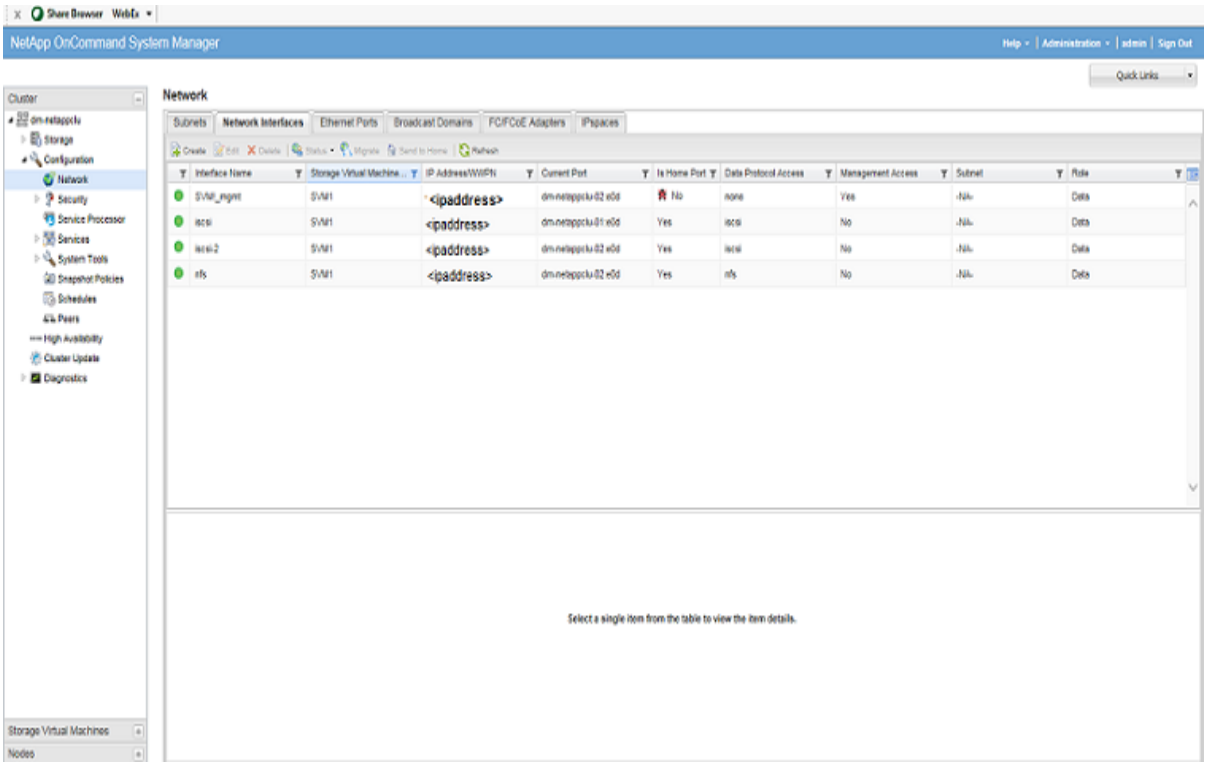
3. Modificare la visualizzazione in Cluster.
4. Da Cluster>Configurazione, fare clic su Rete, quindi aprire le interfacce di rete.

5. 

6. Filtrare il computer virtuale di archiviazione in base al computer SVM identificato.

7. 

8. Ottenere gli indirizzi IP di accesso alla gestione e al protocollo dati, quindi inserirli nella finestra Aggiungi un array di archiviazione della console UDP.
   - Ottenere l'indirizzo IP di accesso alla gestione:
     - Individuare l'interfaccia utente con l'opzione **Sì** sotto la colonna **di accesso alla gestione**.
     - Dall'interfaccia, selezionare l'indirizzo IP disponibile in **Indirizzo IP/WWPN**.
   - Ottenere l'indirizzo IP di accesso al protocollo dei dati:
     - Individuare l'interfaccia contenente l'opzione **iSCSI** o **NFS** nella colonna **Protocollo dati**.
     - Per l'interfaccia ISCSI o NFS, selezionare l'indirizzo IP corrispondente disponibile in **Indirizzo IP/WWPN.**



Nota: Il server ESXi deve utilizzare lo stesso indirizzo IP di accesso al protocollo dati in lettura e scrittura per l'array di archiviazione NetApp iSCSI o NFS.

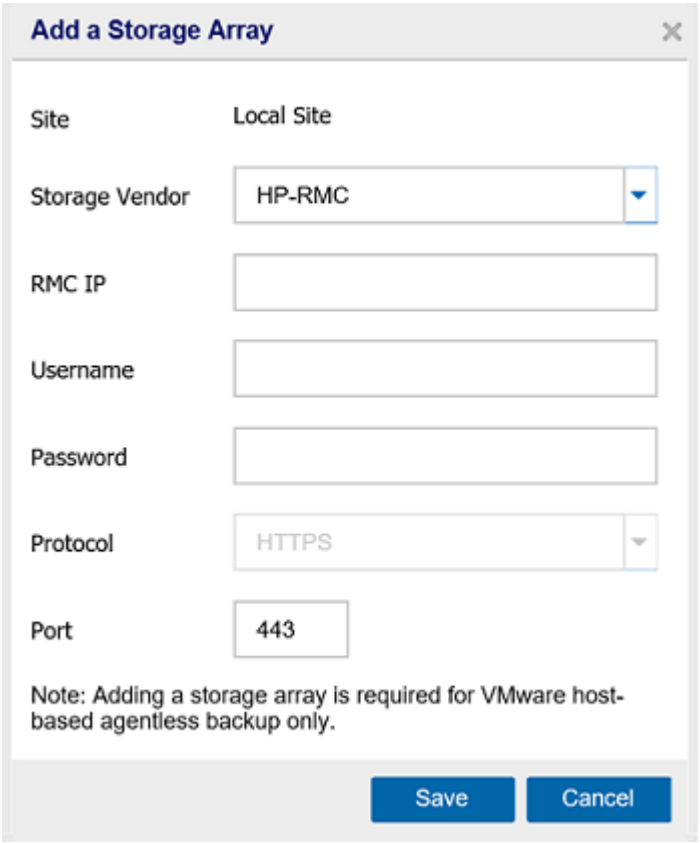
Aggiunta dei dettagli di HPE RMC che gestisce l'array di archiviazione HPE 3PAR StoreServ

È possibile aggiungere i dettagli di HPE RMC che gestisce un array HPE 3PAR StoreServ.

Importante! Il server di archiviazione HPE 3PAR deve essere gestito da HP RMC..

Effettuare le operazioni seguenti:

1. Dalla finestra di dialogo **Aggiungi un array di archiviazione**, selezionare HP-RMC nel menu a discesa **Fornitore archiviazione**.



2. Fornire i dettagli seguenti:

IP RMC

Specifica l'indirizzo IP di gestione HPE RMC.

Nome utente

Specifica il nome utente per la connessione all'array di archiviazione.

Password

Specifica la password per il nome utente.

Protocollo

Specifica il protocollo per la connessione all'array.

Nota: È supportato solo il protocollo HTTPS.

Porta

Specifica il numero di porta dell'array.

Valore predefinito: 443

3. Fare clic su **Salva**.

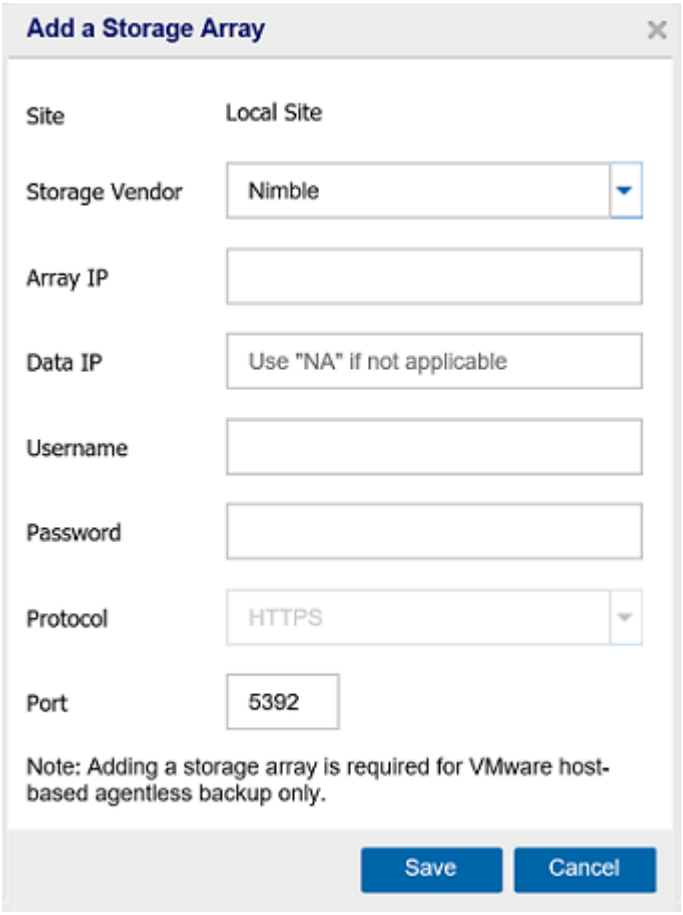
L'array di archiviazione è stato aggiunto alla console.

Aggiunta di un array di archiviazione Nimble

È possibile aggiungere un array di archiviazione Nimble.

Effettuare le operazioni seguenti:

1. Dalla finestra di dialogo **Aggiungi array di archiviazione**, selezionare Nimble dall'elenco a discesa **Fornitore archiviazione**.



2. Immettere i dettagli seguenti per il tipo specifico di array:

IP array

Specifica l'indirizzo IP dell'array. Immettere l'indirizzo IP di gestione dell'array di archiviazione.

IP dati

Specificare l'IP di accesso ai dati (interfaccia logica) dell'array di archiviazione Nimble da cui i computer di destinazione (ESXi) possono accedere a questo array di archiviazione per operazioni di lettura e scrittura. Se l'array di archiviazione Nimble supporta solo il protocollo FC, immettere ND.

Nome utente

Specifica il nome utente per la connessione all'array di archiviazione.

Password

Specifica la password per il nome utente.

Protocollo

Specifica il protocollo per la connessione all'array.

Nota: È supportato solo il protocollo HTTPS.

Porta

Specifica il numero di porta dell'array.

Valore predefinito: 5392

3. Fare clic su **Salva**.

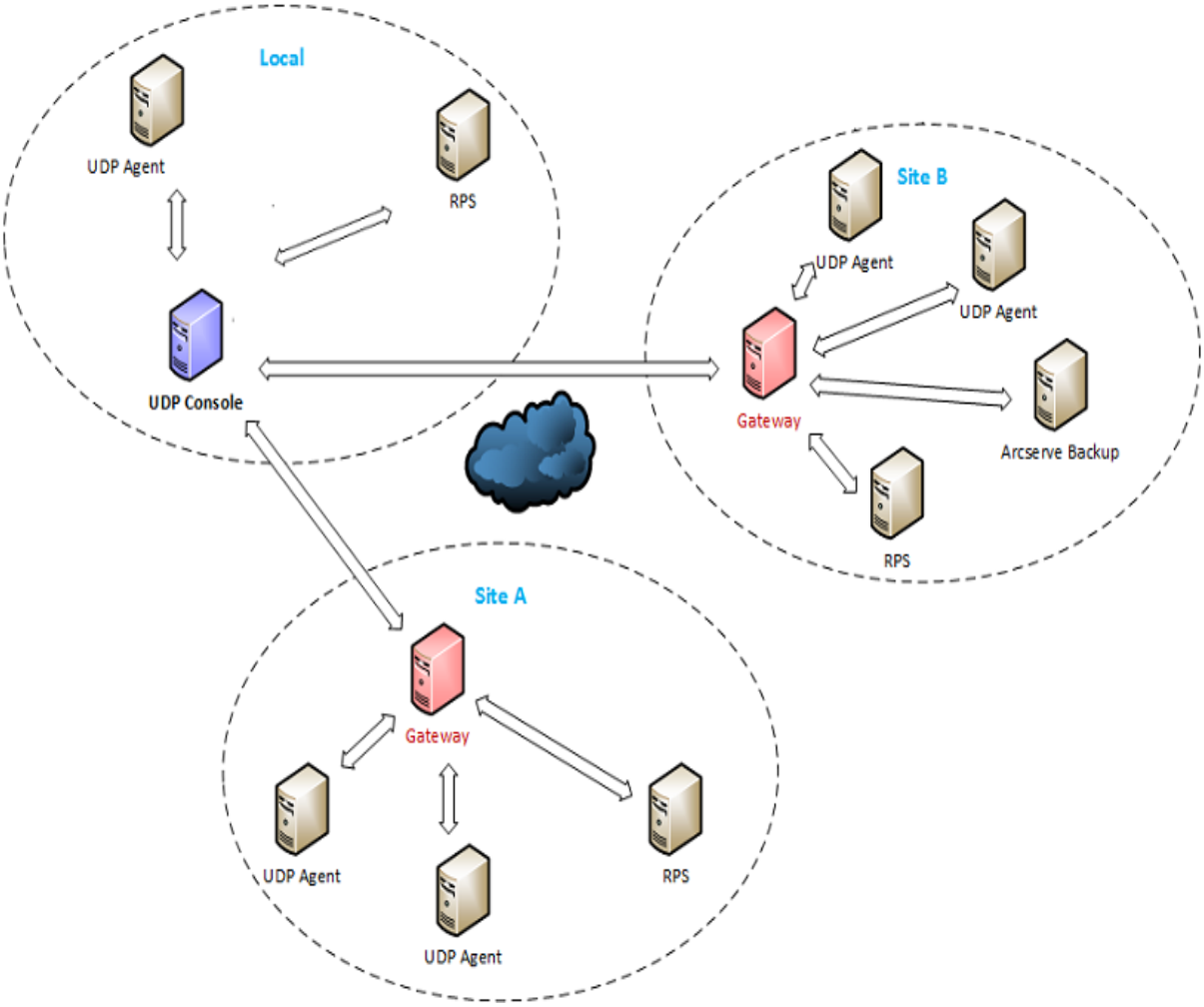
L'array di archiviazione è stato aggiunto alla console.

Aggiunta e gestione di un sito

La console Arcserve UDP consente di gestire i nodi remoti e i Recovery Point Server da un altro subnet su una rete WAN. I nodi e il server remoti in un sito interagiscono con la console mediante un gateway. Il gateway viene installato in Siti. Sebbene la console non possa connettersi direttamente ai nodi remoti, Arcserve UDP utilizza il gateway per stabilire la connessione tra i nodi e la console.

Importante! Se i punti di ripristino si trovano in un sito remoto, per poter ripristinare i dati è necessario che la console si connetta al sito remoto tramite la connessione VPN.

Il diagramma seguente illustra la connessione tra il sito locale e gli altri siti.



Dopo aver aggiunto un sito, è possibile modificare, aggiornare o eliminare i siti dalla console. È inoltre possibile gestire i nodi remoti dalla console.

Definizione del nome del sito

La pagina Nome del sito consente di specificare un nome per il sito e selezionare un intervallo di heartbeat. Il nome del sito viene visualizzato nella console.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della console.
2. Dal riquadro sinistro, accedere a **Infrastrutture**, quindi fare clic su **Siti**.

   Nel riquadro centrale viene visualizzata la pagina Infrastruttura: Siti remoti.
3. Fare clic su **Aggiungi sito**.

   Viene visualizzata la procedura guidata **Aggiungi sito**.
4. Fornire i seguenti dettagli nella pagina Sito:

   Nome sito

   Fornire un nome per il sito.

   Intervallo di heartbeat

   Selezionare un intervallo di heartbeat dall'elenco a discesa. L'heartbeat verifica la connessione tra la console e il sito negli intervalli di tempo specificati.

   URL di connessione alla console UDP

   Specifica l'URL della console UDP. Il server gateway stabilisce la connessione all'URL.

   Ricorda URL di connessione alla console UDP

   Selezionare questa casella di controllo per memorizzare l'URL della console.
5. Fare clic su **Avanti**.

   Viene visualizzata la pagina delle istruzioni di installazione del gateway di gestione remoto Arcserve.

   Il nome per il sito remoto è stato specificato.

Condivisione delle istruzioni di registrazione

L'opzione di condivisione delle istruzioni di registrazione include le informazioni per scaricare e installare il gateway. Le istruzioni di download vengono inviate all'amministratore remoto. L'amministratore remoto dovrà utilizzare le informazioni di download per scaricare e installare il gateway.

Effettuare le operazioni seguenti:

1. Copiare le istruzioni e salvarle per poterle consultare in un secondo momento.

   Se non è stata configurata la posta elettronica di Arcserve UDP, inviare le istruzioni copiate all'amministratore remoto da un altro server di posta elettronica.

2. Selezionare **Invia istruzioni con messaggio di posta elettronica di Arcserve UDP** e fornire l'indirizzo di posta elettronica dell'amministratore remoto.

3. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Conferma**.

   Le istruzioni di registrazione sono state condivise correttamente.

Verifica e aggiunta del sito

Prima di aggiungere il sito, verificare i dettagli. È possibile fare clic su **Precedente** per visitare le pagine precedenti.

Effettuare le operazioni seguenti:

1. Verificare i seguenti dettagli nella pagina di conferma.

   È possibile modificare qualsiasi informazione nelle pagine precedenti, se necessario.

2. Fare clic su **Fine**.

   La procedura guidata viene chiusa.

   Il sito remoto viene creato nella pagina **Infrastruttura: siti**.

   Se l'amministratore remoto installa il gateway di gestione remota Arcserve e fornisce al gateway il codice di autorizzazione, verrà visualizzato un segno di spunta verde accanto al nome del sito nella Console.

   Il sito è stato aggiunto correttamente.

Modifica dell'URL della console

Quando si modifica l'URL della console, è necessario registrare nuovamente il gateway per gestire il sito dalla console. La registrazione del gateway viene eseguita dall'amministratore remoto. Quando si aggiorna l'URL della console, Arcserve UDP invia messaggi di posta elettronica all'amministratore remoto contenenti informazioni dettagliate su come registrare il gateway nella console.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic su **Risorse**.
2. Accedere a **Infrastruttura** nel riquadro sinistro e fare clic su **Siti**.

   La pagina **Infrastruttura: siti** viene visualizzata nel riquadro centrale.
3. Selezionare il sito e fare clic su **Azioni**, **Aggiorna URL console**.

   Viene visualizzata la finestra di dialogo **Aggiorna URL console**.
4. Specificare il nuovo URL della console.
5. Fare clic su **Invia**.

   Viene inviato un messaggio di posta elettronica all'amministratore remoto. Quando l'amministratore aggiorna il nuovo URL sul server gateway, la console mostra un segno di spunta di colore verde accanto al sito aggiornato.

   L'URL della console è stato aggiornato correttamente.

Modifica del sito

È possibile modificare il sito per modificare i parametri del sito aggiunto. Ad esempio, è possibile rinominare il sito o cambiare l'intervallo di heartbeat.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Accedere a **Infrastruttura** nel riquadro sinistro e fare clic su **Siti**.

   La pagina **Infrastruttura: Sito** viene visualizzata nel riquadro centrale.
3. Selezionare il sito e fare clic su **Azioni**, **Modifica**.

   Viene visualizzata la procedura guidata **Modifica sito**.
4. Utilizzare **Indietro** e **Avanti** per visitare le pagine e modificare i parametri.
5. Fare clic su **Fine**.

   La procedura guidata **Modifica sito** viene chiusa.

   Il sito è stato modificato correttamente.

Eliminazione di un sito

È possibile eliminare un sito che non si desidera gestire. Prima di eliminare un sito, tutti i nodi e i filtri di rilevamento dei nodi relativi a questo sito devono essere eliminati.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Accedere a **Infrastruttura** nel riquadro sinistro e fare clic su **Siti**.

   La pagina **Infrastruttura: Sito** viene visualizzata nel riquadro centrale.
3. Selezionare il sito e fare clic su **Azioni**, Elimina.

   Viene visualizzata la finestra di dialogo **Conferma**.
4. Fare clic su **Sì**.

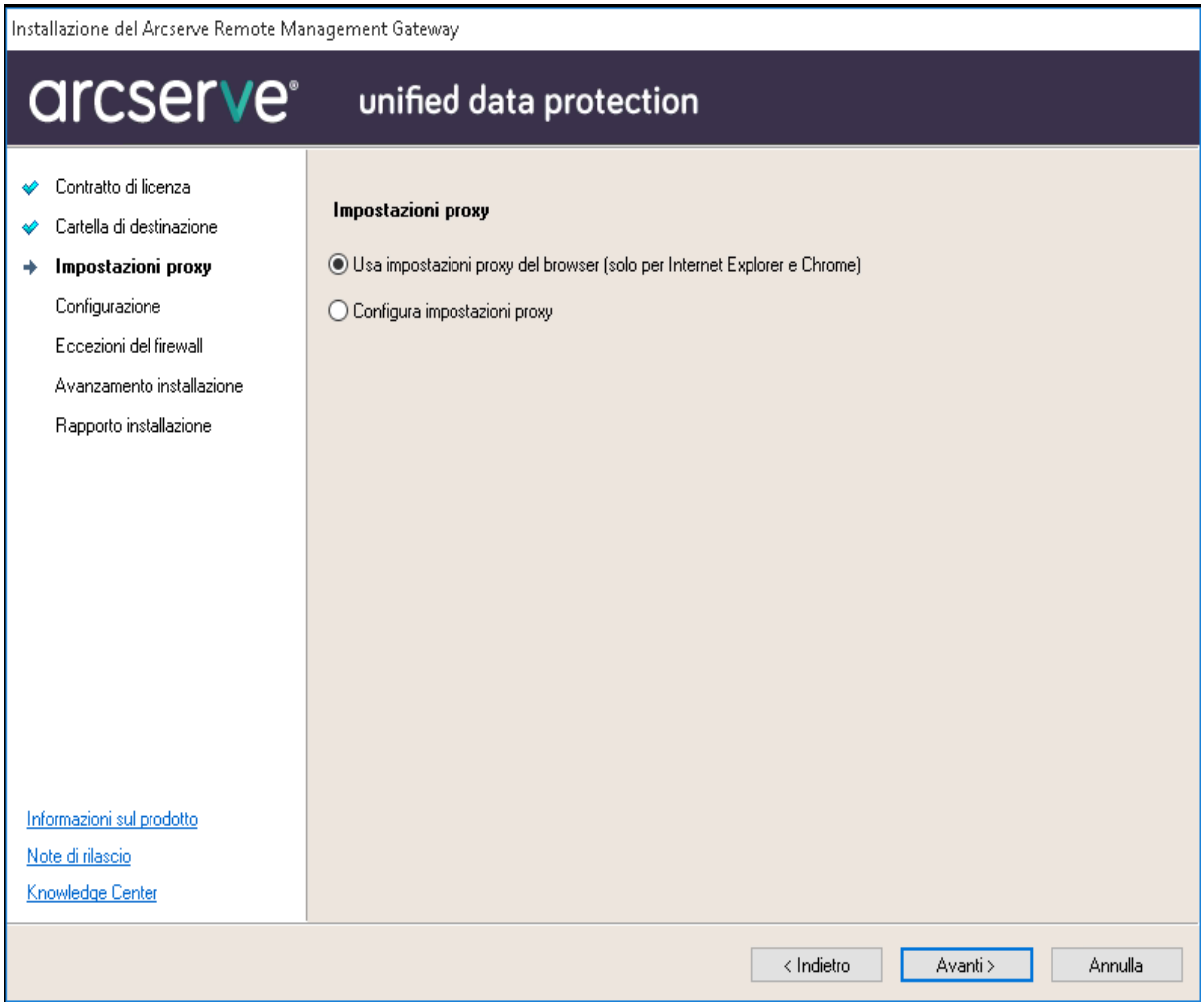
   Il sito viene eliminato.

Impostazione di un server proxy per il gateway

Arcserve UDP supporta l'installazione di un server proxy sul computer gateway. Il gateway utilizza questa impostazione proxy per comunicare con la relativa console registrata.

Effettuare le operazioni seguenti:

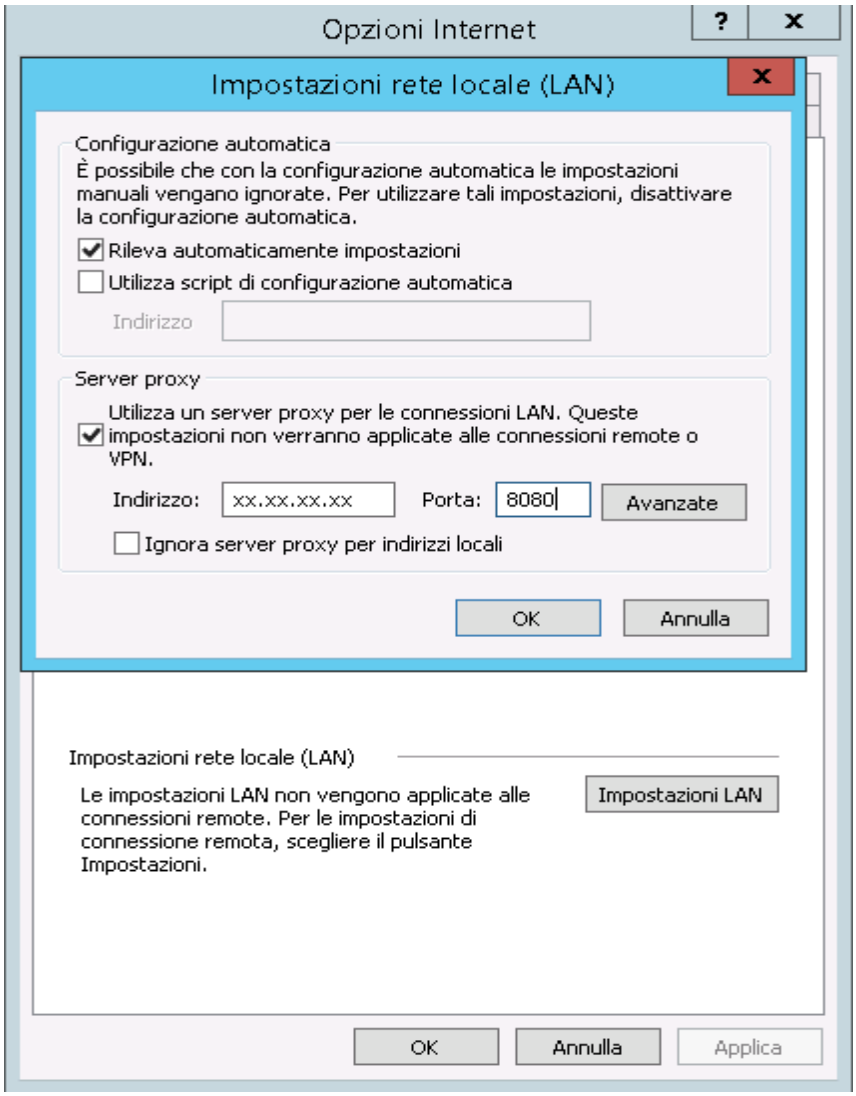
1. Aprire la procedura guidata di installazione del gateway di gestione remota Arcserve.



2. Nella finestra di dialogo Impostazioni proxy, scegliere una delle seguenti opzioni:

   Usa impostazioni proxy del browser (solo per Internet Explorer e Chrome)

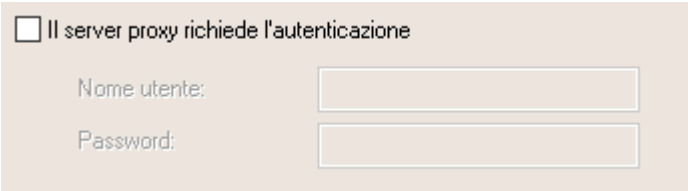
Specifica se utilizzare le impostazioni proxy del browser. È necessario aggiornare le impostazioni proxy del browser. Aprire il browser e fare clic su **Opzioni**, **Connessione**, **Configurazione LAN**.



Configurazione delle impostazioni proxy

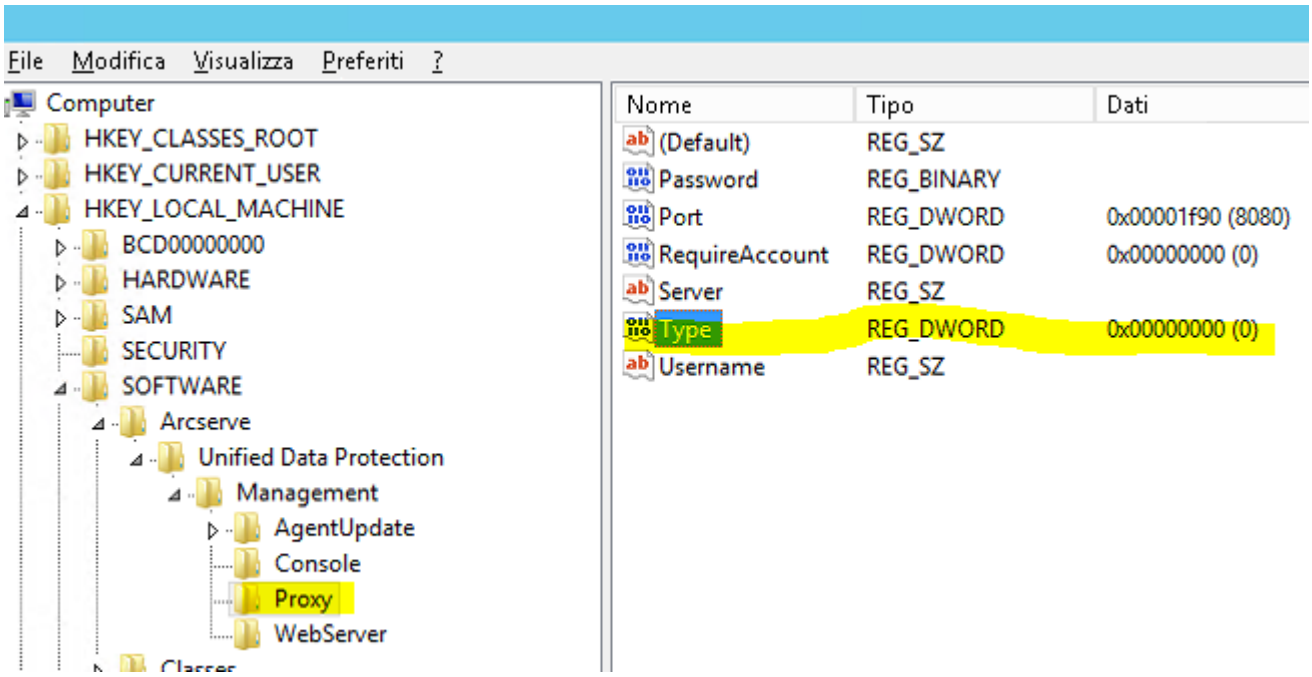
Specifica se è necessario fornire i dettagli del server proxy nella pagina della procedura guidata.

3. Se il proxy non supporta le credenziali, deselezionare la casella di controllo di autenticazione.



Il server proxy viene impostato per il gateway.

4. Per verificare le impostazioni del proxy, aprire regedit e accedere al proxy.



Nel campo Tipo, 0 indica le impostazioni del browser e 1 indica le altre impostazioni.

Nota: Utilizzare regedit per modificare le impostazioni proxy come il tipo di porta o l'indirizzo IP del server.

Gestione dei nodi di Exchange Online

Non è possibile aggiungere i nodi di Exchange Online direttamente alla visualizzazione di tutti i nodi. Una volta aggiunto il piano di backup, il nodo di Exchange Online viene aggiunto direttamente alla visualizzazione di tutti i nodi.

È possibile eseguire le seguenti attività:

1. Aggiunta di un nodo Exchange Online
2. Aggiornamento di un nodo di Exchange Online
3. Eliminazione di un nodo di Exchange Online
4. Supporto delle caselle di posta delle cartelle pubbliche per la protezione di Exchange Online

Aggiunta di un nodo Exchange Online

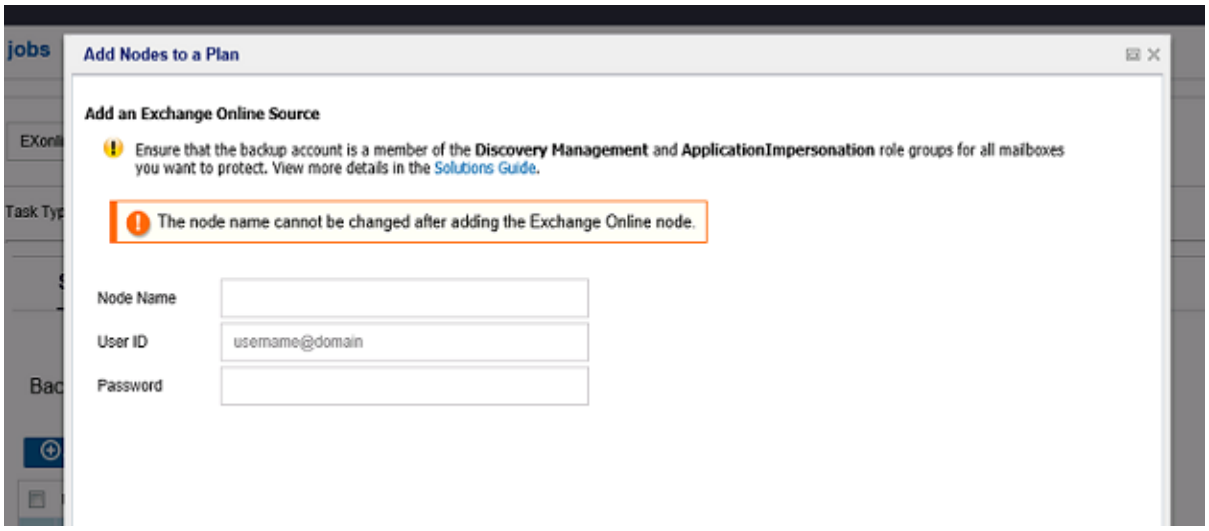
Nota: A differenza di altri nodi, non è possibile aggiungere il nodo Exchange Online dalla pagina Tutti i nodi. Un nodo Exchange Online viene aggiunto solo in un piano o durante la modifica di un piano.

Per informazioni sulla creazione di un piano, consultare la sezione Creazione di un piano Exchange Online.

Effettuare le operazioni seguenti:

1. Immettere il nome utente dell'account di backup di Exchange Online che soddisfa i prerequisiti nel campo Nome utente o nell'account utente per il nodo Exchange Online.

   Più nodi Exchange Online possono utilizzare lo stesso account utente (account servizio) di Exchange Online. Per aggiungere il nodo Exchange dal piano, specificare il nome del nodo, il nome utente e la password. Una volta creato, non è possibile modificare il nome del nodo Exchange Online.



   Nota: Aggiornando o modificando l'account utente, il numero di caselle di posta protette potrebbe essere modificato. Verificare che l'account del servizio nuovo/aggiornato disponga dei diritti di impersonificazione per la protezione delle caselle di posta elettronica.

2. Immettere la password e fare clic su **Connetti**.
3. Selezionare gli account Exchange Online da proteggere, quindi fare clic sulla freccia verso destra (>) per spostarli nell'elenco protetto.

   Nota: Selezionare la casella di controllo per proteggere tutte le origini Exchange Office 365 per proteggere tutti gli account di Exchange Online in tutte le pagine.

Per aggiungere tutti gli account Exchange Online elencati nella pagina all'elenco protetto, fare clic sulla freccia verso destra (>).

4. Fare clic su **Salva**.

   È possibile selezionare le cartelle di cui non si desidera eseguire il backup utilizzando l'opzione Cartelle da escludere dal backup della scheda Origine.

   Gli account Exchange Online selezionati vengono aggiunti.

Aggiornamento di un nodo di Exchange Online

Quando si modificano le credenziali del nodo di Exchange Online, aggiornare il nodo di Exchange Online nella Console.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Nodi di Exchange Online**.

   I nodi di Exchange Online creati vengono mostrati nel riquadro centrale.
3. Selezionare il nodo Exchange Online e fare clic su **Azioni**.
4. Fare clic su **Aggiorna**.

   Viene visualizzata la finestra di dialogo **Aggiorna nodo**.
5. Modificare i dettagli come desiderato e fare clic su **OK**.

   Il nodo di Exchange Online è stato aggiornato.

Eliminazione di un nodo di Exchange Online

Eliminare qualsiasi nodo Exchange Online non più necessario.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Passare a **Nodi**, quindi fare clic su **Nodi Exchange Online**.

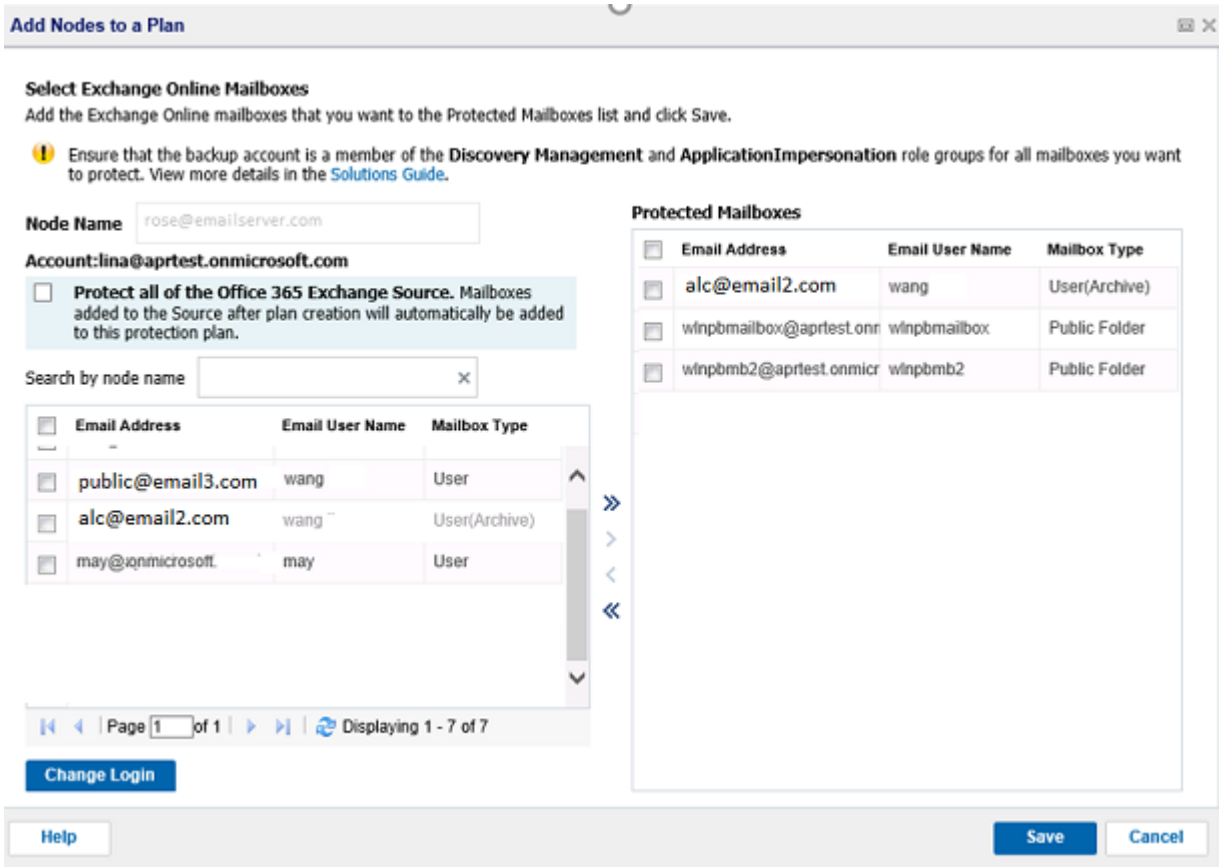
   I nodi di Exchange Online creati vengono mostrati nel riquadro centrale.
3. Selezionare il nodo Exchange Online e fare clic su **Azioni**.
4. Fare clic su **Elimina**.

   Viene visualizzata una finestra di dialogo di conferma.
5. Fare clic su **OK**.

   Il nodo Exchange Online è stato eliminato correttamente.

Supporto delle caselle di posta delle cartelle pubbliche per la protezione di Exchange Online.

Quando si aggiunge il nodo Exchange Online, è possibile visualizzare la colonna Tipo della casella di posta nella finestra **Aggiungi nodi a piano**. La casella di posta delle cartelle pubbliche viene visualizzata in questa finestra e nella colonna viene visualizzata come **cartella pubblica**. Per proteggere una cartella pubblica, aggiungere la casella di posta pubblica corrispondente in **Caselle di posta protette**, quindi salvare il piano.



Nota: Per ulteriori informazioni sulla casella di posta delle cartelle pubbliche di Exchange Online e l'autorizzazione, fare riferimento al collegamento 1 e al collegamento 2.

Gestione dei nodi SharePoint Online

Non è possibile aggiungere i nodi di SharePoint Online direttamente alla visualizzazione di tutti i nodi. Una volta aggiunto il piano di backup, il nodo di SharePoint Online viene aggiunto direttamente alla visualizzazione di tutti i nodi.

È possibile eseguire le seguenti attività:

1. Aggiunta di un nodo SharePoint Online
2. Aggiornamento di un nodo SharePoint Online
3. Eliminazione di un nodo SharePoint Online

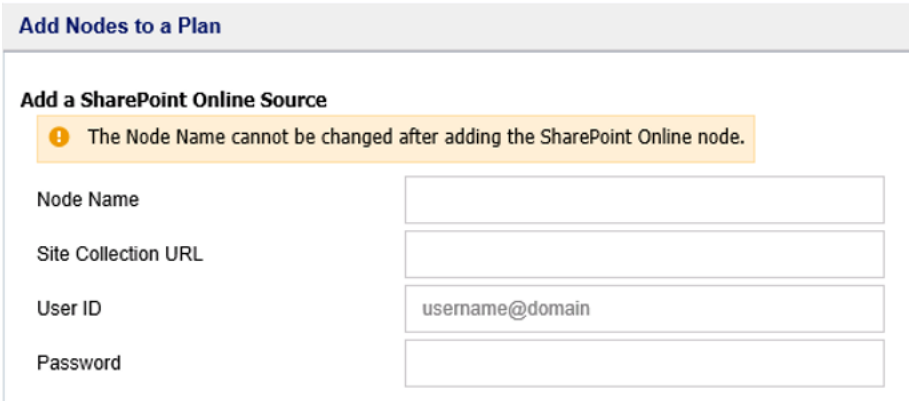
Aggiunta di un nodo di SharePoint Online

Nota: A differenza di altri nodi, non è possibile aggiungere il nodo di SharePoint Online dalla pagina Tutti i nodi. È possibile aggiungere un nodo di SharePoint Online in un piano soltanto durante la creazione o la modifica di un piano.

Per informazioni sulla creazione di un piano, consultare la sezione Creazione di un piano SharePoint Online.

Effettuare le operazioni seguenti:

1. Immettere il nome utente del nodo SharePoint e immettere l'URL della raccolta siti, il nome utente del proprietario del sito e la password.



2. Immettere la password e fare clic su **Connetti**.
3. Selezionare l'elenco SharePoint/Libreria o gli elementi dell'elenco da proteggere.
4. Fare clic su **Salva**.

   Gli account SharePoint Online selezionati vengono aggiunti.

Aggiornamento di un nodo di SharePoint Online

Quando si modificano le credenziali del nodo di SharePoint Online, aggiornare il nodo di SharePoint Online nella Console.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Nodi di SharePoint Online**.

   I nodi di SharePoint Online creati vengono mostrati nel riquadro centrale.
3. Selezionare il nodo SharePoint Online e fare clic su **Azioni**.
4. Fare clic su **Aggiorna**.

   Viene visualizzata la finestra di dialogo **Aggiorna nodo**.
5. Modificare i dettagli come desiderato e fare clic su **OK**.

   Il nodo di SharePoint Online è stato aggiornato.

Eliminazione di un nodo di SharePoint Online

Eliminare qualsiasi nodo SharePoint Online non più necessario.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Passare a **Nodi**, quindi fare clic su **Nodi SharePoint Online**.

   I nodi di SharePoint Online creati vengono mostrati nel riquadro centrale.
3. Selezionare il nodo SharePoint Online e fare clic su **Azioni**.
4. Fare clic su **Elimina**.

   Viene visualizzata una finestra di dialogo di conferma.
5. Fare clic su **OK**.

   Il nodo SharePoint Online è stato eliminato correttamente.

Come gestire i nodi OneDrive

Non è possibile aggiungere i nodi di OneDrive direttamente alla visualizzazione di tutti i nodi. Dopo avere aggiunto il piano di backup, il nodo di OneDrive viene aggiunto direttamente alla visualizzazione di tutti i nodi.

È possibile eseguire le seguenti attività:

1. Aggiunta di un nodo di OneDrive
2. **Eliminazione del nodo:** dal menu Azioni del nodo di OneDrive, fare clic su **Elimina** quindi confermare nel pop-up l'eliminazione del nodo dalla console.
3. **Esportazione del nodo:** dal menu Azioni del nodo di OneDrive, fare clic su **Esporta** e per ricevere i nodi sotto forma di file ZIP.
4. **Modifica del piano:** dal menu Azioni del nodo di OneDrive, fare clic su **Modifica piano** per aprire il piano correlato e aggiornarlo come necessario.
5. **Accesso all'agente:** dal menu Azioni del nodo di OneDrive, fare clic su **Accedi all'agente** per eseguire le operazioni specifiche dell'agente, come il ripristino mediante l'opzione di montaggio del volume.
6. **Esecuzione del backup:** dal menu Azioni del nodo di OneDrive, fare clic su **Esegui backup** per eseguire il backup manuale.
7. **Ripristino:** dal menu Azioni del nodo di OneDrive, fare clic su **Ripristina** per accedere all'agente ed eseguire il ripristino.
8. Download del punto di ripristino dal cloud

9. Aggiornamento del punto di ripristino su cloud
10. Copia del punto di ripristino su disco locale o condivisione di rete

Aggiunta di un nodo di OneDrive

Nota: diversamente dagli altri nodi, il nodo di OneDrive non può essere aggiunto dalla pagina Tutti i nodi. Un nodo di OneDrive può essere aggiunto a un piano solamente durante la creazione o la modifica del piano.

Per informazioni sulle modalità di aggiunta del nodo, è possibile visualizzare la "Definizione dell'origine" a pagina 1044 durante la creazione del piano di backup di OneDrive.

Eliminazione di un nodo di OneDrive Online

Eliminare tutti i nodi di OneDrive Online che non sono più necessari.

Effettuare le operazioni seguenti:

1. Fare clic su **Elimina** nel menu **Azioni** del nodo di OneDrive.
2. Nel pop-up confermare l'eliminazione del nodo dalla console.

   Il nodo di OneDrive Online viene eliminato correttamente.

Gestione dei nodi del gruppo di database Oracle

Arcserve UDP consente di eseguire più azioni per gestire i nodi del database Oracle, ad esempio aggiornare il nodo, esportare il nodo, eseguire un processo di backup, annullare un processo di backup ed eliminare un nodo.

La presente sezione descrive i seguenti argomenti:

Aggiornamento del nodo del database Oracle

È possibile aggiornare le informazioni relative ai nodi esistenti. Quando si modificano le credenziali dei nodi del database Oracle, è necessario aggiornare i nodi del database Oracle sulla console.

Effettuare le operazioni seguenti:

1. Accedere alla console Arcserve UDP.
2. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina Nodi: Tutti i nodi.
3. Eseguire una delle seguenti operazioni:

- Nel riquadro sinistro, accedere a **Nodi**, **Gruppo database Oracle**, fare clic con il pulsante destro del mouse sul nodo che si desidera aggiornare, quindi selezionare **Aggiorna**.
- Nel riquadro centrale, selezionare il nodo che si desidera aggiornare, fare clic sull'elenco a discesa **Azioni**, quindi selezionare **Aggiorna**.

Viene visualizzata la finestra di dialogo Aggiorna nodo.

5. Nella finestra di dialogo Aggiorna nodo, modificare i dettagli in base alle esigenze, quindi fare clic su **OK**.

   Il nodo del database Oracle viene aggiornato.

Esportazione del nodo

È possibile esportare dei nodi come file ZIP (.zip). Se necessario, è possibile importare il file ZIP per memorizzare i nodi. Ad esempio, esportare i nodi prima degli aggiornamenti o dei riavvii consente di importare lo stesso insieme di nodi.

È possibile esportare soltanto i nodi con credenziali validi e in esecuzione su sistemi operativi Windows.

Effettuare le operazioni seguenti:

1. Accedere alla console Arcserve UDP.
2. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina Nodi: Tutti i nodi.
3. Eseguire una delle seguenti operazioni:
   - Nel riquadro sinistro, accedere a **Nodi**, **Gruppo database Oracle**, fare clic con il pulsante destro del mouse sul nodo che si desidera esportare, quindi selezionare **Esporta**.
   - Nel riquadro centrale, selezionare il nodo che si desidera esportare, fare clic sull'elenco a discesa **Azioni**, quindi selezionare **Esporta**.

   Viene visualizzata una finestra di dialogo che richiede l'intervento dell'utente nel file list.zip.
4. Fare clic su **Apri** o **Salva**.

   L'elenco di nodi viene esportato.

Backup del nodo del database Oracle

In genere, i backup vengono eseguiti automaticamente e vengono controllati attraverso le impostazioni di pianificazione. In aggiunta al backup pianificato, un backup

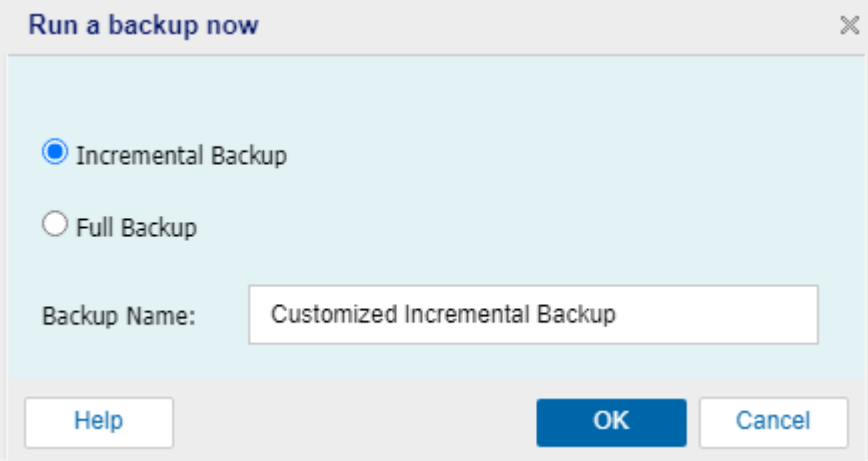
manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze.

Effettuare le operazioni seguenti:

1. Accedere alla console Arcserve UDP.
2. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina Nodi: Tutti i nodi.
3. Eseguire una delle seguenti operazioni:
   - Nel riquadro sinistro, accedere a **Nodi**, **Gruppo database Oracle**, fare clic con il pulsante destro del mouse sul nodo di cui si desidera eseguire il backup, quindi selezionare **Esegui backup ora**.
   - Nel riquadro centrale, selezionare il nodo di cui si desidera eseguire il backup, fare clic sull'elenco a discesa **Azioni**, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
4. Nella finestra di dialogo *Esegui un backup immediato*, selezionare il tipo di backup che si desidera eseguire, quindi specificare il nome del backup, se necessario.



Le opzioni disponibili sono:

Backup incrementale

Avvia un backup incrementale del computer. Un backup incrementale esegue il backup solo dei blocchi modificati dopo l'ultimo backup.

Nota: se si esegue un backup per la prima volta, il backup completo viene avviato automaticamente anche se è stata selezionata l'opzione Backup incrementale.

I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup con dimensioni molto ridotte. Questa modalità di esecuzione backup è ottimale.

Backup completo

Avvia un backup completo dell'intero computer o dei volumi selezionati.

Nota: se non viene specificato alcun nome di backup, per impostazione predefinita viene automaticamente denominato Backup completo personalizzato o Backup incrementale.

5. Fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.

6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.

   Il processo di backup è stato eseguito correttamente.

Annullamento del processo di backup dei nodi del database Oracle

Dopo aver avviato il processo di backup dei nodi del database Oracle, è possibile annullare il processo in qualsiasi momento. Quando si annulla il processo di backup, il backup viene interrotto immediatamente.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina Nodi: Tutti i nodi.

3. Eseguire una delle seguenti operazioni:

   - Nel riquadro sinistro, accedere a **Nodi**, **Gruppo database Oracle**, fare clic con il pulsante destro del mouse sul nodo per il quale si desidera annullare il backup, quindi selezionare **Annulla**.
   - Nel riquadro centrale, selezionare il nodo per il quale si desidera annullare il backup, fare clic sull'elenco a discesa **Azioni** e selezionare **Annulla**.

   Verrà visualizzato un messaggio di conferma.

5. Fare clic su **Sì** per confermare.

   Il processo di backup viene annullato correttamente.

Eliminazione dei nodi del database Oracle

È possibile eliminare i nodi del database Oracle non più necessari. Se i nodi vengono eliminati, le cronologie dei registri e dei processi associati verranno eliminati di conseguenza. Se necessario, sarà possibile aggiungere il nodo eliminato in un secondo momento.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.

   Viene visualizzata la pagina Nodi: Tutti i nodi.

3. Eseguire una delle seguenti operazioni:

   - Nel riquadro sinistro, accedere a **Nodi**, **Gruppo database Oracle**, fare clic con il pulsante destro del mouse sul nodo che si desidera eliminare, quindi selezionare **Elimina**.
   - Nel riquadro centrale, selezionare il nodo che si desidera eliminare, fare clic sull'elenco a discesa **Azioni**, quindi selezionare **Elimina**.

   Verrà visualizzato un messaggio di conferma.

5. Fare clic su **Sì** per confermare.

   Il nodo viene eliminato della Console.

Chapter 9: Aggiunta e gestione delle destinazioni

La presente sezione descrive i seguenti argomenti:

Aggiunta di una destinazione

Una destinazione è una posizione in cui vengono archiviati i dati di backup. Arcserve UDP consente di aggiungere più tipi di destinazioni.

Come procedere:

1. Aggiunta di una destinazione tramite RPS
2. Aggiunta dei server Arcserve Backup
3. Aggiunta di una console remota
4. Aggiunta di un account cloud
5. Aggiunta di un account Arcserve Cloud

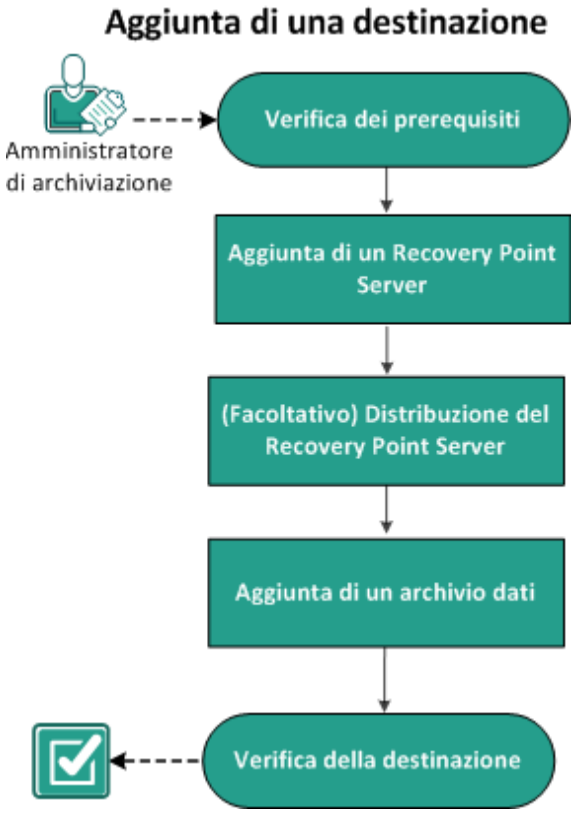
Aggiunta di una destinazione

Per Arcserve UDP, è possibile assegnare un Recovery Point Server (RPS) come destinazione centrale. È possibile archiviare dati da più nodi in un server Recovery Point Server e recuperare i dati quando è necessario. L'aggiunta di una destinazione presenta essenzialmente due fasi:

a. Aggiunta di un Recovery Point Server alla Console.

b. Aggiunta di un archivio dati al Recovery Point Server.

Nel diagramma seguente viene illustrato come aggiungere una destinazione:



Come procedere?

1. Revisione dei prerequisiti
2. Aggiunta di un Recovery Point Server
3. (Facoltativo) Distribuzione del Recovery Point Server
4. Aggiunta di un archivio dati
5. Verifica della destinazione

Verifica dei prerequisiti

Prima di impostare un Recovery Point Server, completare i seguenti prerequisiti:

- Consultare le Note di rilascio per conoscere i requisiti di sistema, i sistemi operativi supportati e l'elenco dei problemi noti per questa release di Arcserve Unified Data Protection.
- Assicurarsi di disporre di privilegi di amministratore prima di installare Arcserve Unified Data Protection.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Aggiunta di un Recovery Point Server

L'aggiunta di una destinazione inizia con l'aggiunta di un Recovery Point Server alla Console. In seguito sarà possibile aggiungere gli archivi dati al RPS.

Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: Recovery Point Server**.
3. Fare clic su **Aggiungi un Recovery Point Server**.

   Viene visualizzata la pagina **Aggiungi un Recovery Point Server**.
4. Immettere le seguenti informazioni:

   Nome nodo/Indirizzo IP

   Definisce il nome del nodo del Recovery Point Server che si desidera aggiungere alla Console.

   Nome utente e Password

   Definisce il nome utente e la password per l'accesso al nodo.

   Nota: Utilizzare uno dei seguenti formati per il nome utente: nome computer, nome dominio/nome utente o nome utente.

   Descrizione

   (Facoltativo) Definisce eventuali informazioni supplementari sul nodo.
5. Immettere i campi seguenti per le **Impostazioni di installazione**:

   Nota: se sul nodo è già stato installato un Recovery Point Server, è possibile ignorare queste impostazioni.

   Posizione installazione

   Specificare la posizione in cui si desidera installare il Recovery Point Server. È possibile accettare il percorso predefinito o specificare un percorso alternativo.

   Porta

   Specifica il numero di porta che si connette all'interfaccia utente basata sul Web.

   Valore predefinito: 8014

   Protocollo

Specificare il protocollo che si desidera utilizzare per la comunicazione con il server di destinazione. Le opzioni disponibili sono HTTP e HTTPS.

Nota: Per una comunicazione più sicura, selezionare il protocollo HTTPS.

Driver di rilevamento modifiche

Specificare se si desidera **installare il driver di rilevamento modifiche dell'agente**.

6. Pianificare o aggiornare l'installazione selezionando una delle opzioni disponibili in **Ora di inizio installazione o aggiornamento**.

   Nota: se sul server è già stato installato un Recovery Point Server, è possibile ignorare queste impostazioni.

7. Fare clic su **Salva**.

   Il progresso della distribuzione viene visualizzato nel riquadro destro. Il Recovery Point Server è stato aggiunto.

   Viene ora eseguita la distribuzione del Recovery Point Server. È possibile aggiungere archivi dati dopo l'aggiunta del Recovery Point Server.

(Facoltativo) Distribuzione del Recovery Point Server

Arcserve Unified Data Protection consente di rilevare e distribuire l'ultima versione del componente RPS sui Recovery Point Server. Dopo avere effettuato la distribuzione del componente RPS, il nodo è pronto per archiviare le sessioni di backup e fungere da Recovery Point Server.

Nota: I componenti RPS vengono installati con l'installazione di Arcserve Unified Data Protection.

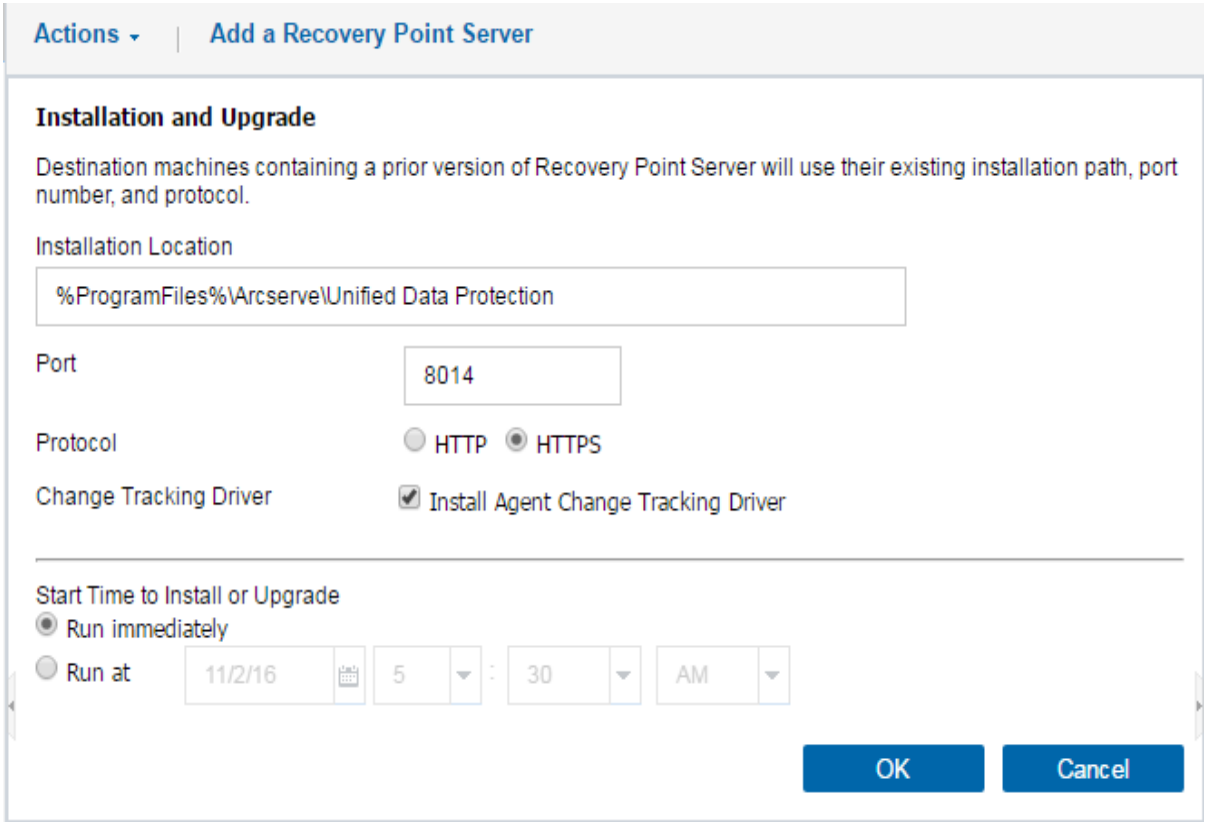
Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Viene visualizzata la pagina **Destinazione: Recovery Point Server**.
3. Eseguire una delle seguenti operazioni:
   - Fare clic con il pulsante destro del mouse su un Recovery Point Server.
   - Selezionare un Recovery Point Server e dal riquadro centrale fare clic sul menu a discesa **Azioni**.

   Viene visualizzato un elenco di opzioni.
4. Fare clic su **Installazione o aggiornamento del Recovery Point Server**.

   Viene visualizzata la pagina **Installazione e aggiornamento**.



5. Modificare le impostazioni di distribuzione, quindi fare clic su **OK** per distribuire il Recovery Point Server sul nodo selezionato.

   La distribuzione del Recovery Point Server viene avviata. È possibile visualizzare l'avanzamento della distribuzione nel riquadro destro.

Aggiunta di un archivio dati

Per creare la destinazione, il Recovery Point Server deve disporre degli archivi dati. L'archivio dati specifica la posizione in cui sono archiviati i dati di backup. È possibile aggiungere più archivi dati a un Recovery Point Server.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Viene visualizzata la pagina **Destinazioni: Recovery Point Server**.
3. Eseguire una delle seguenti operazioni:
   - Fare clic con il pulsante destro del mouse su un Recovery Point Server.
   - Selezionare un Recovery Point Server e dal riquadro centrale fare clic sul menu a discesa **Azioni**.

   Viene visualizzato un elenco di opzioni.
4. Fare clic su **Aggiungi archivio dati**.

   Viene visualizzata la pagina **Crea archivio dati** con il nome del server del Recovery Point Server.
5. Completare i seguenti campi, quindi fare clic su **Salva**.

   Recovery Point Server

   Definisce il Recovery Point Server in cui viene creato l'archivio dati. Il Recovery Point Server è già aggiunto per impostazione predefinita.

   Nome archivio dati

   Definisce il nome dell'archivio dati.

   Cartella archivio dati

   Definisce la posizione del percorso della cartella in cui viene creato l'archivio dati. Fare clic su Sfoglia per selezionare la cartella di destinazione.

   Note:

   - È ora possibile attivare e visualizzare i volumi nascosti. Per ulteriori informazioni, consultare la sezione Attivazione e visualizzazione dei volumi nascosti durante la creazione di un archivio dati.
   - Per l'archivio dati di deduplicazione e non di deduplicazione, il percorso di destinazione deve essere una cartella vuota.

   Limite nodi attivi simultaneamente

Specifica il numero massimo di processi simultanei dell'archivio dati.

Valore predefinito: 4

Corrisponde a un valore compreso tra 1 e 9999. Il valore indica il numero di processi che possono essere eseguiti contemporaneamente. Se i processi in esecuzione corrispondono al numero indicato, un processo viene inserito nella coda e potrà essere avviato soltanto al completamento del processo in esecuzione. Un processo completato può essere un processo terminato, annullato o non riuscito.

Questo numero viene applicato ai tipi di processo ma non ai nodi del server. Ad esempio, il numero 5 indica che cinque processi di backup sono in esecuzione. Qualsiasi processo pianificato dopo cinque processi di backup dovrà attendere nella coda. Tuttavia, è possibile inoltrare un processo diverso, come ad esempio un processo di catalogo di file system.

Se il valore è maggiore di 16 o 32, vengono visualizzati dei messaggi indicanti l'aumento della domanda sulla periferica hardware.

Nota: Il limite influisce solamente sui processi di replica in uscita, ma non sui processi di replica in entrata. Il limite non influisce sui processi di ripristino o processi di ripristino bare metal. Tali processi non vengono inseriti nella coda.

Enable Deduplication (Abilita deduplicazione)

Specifica che per l'archivio dati è abilitata la deduplicazione. Arcserve UDP supporta entrambi i tipi di deduplicazione: Deduplicazione all'origine e Deduplicazione globale. La deduplicazione dal lato origine impedisce che i blocchi di dati duplicati vengano spostati nella rete da parte di un determinato agente. La deduplicazione globale elimina i dati duplicati su tutti i computer client basati sul livello cluster del computer.

Dimensione di blocco della deduplicazione

Definisce la dimensione del blocco della deduplicazione. Le opzioni sono 4 KB, 8 KB, 16 KB, 32 KB e 64 KB. La dimensione del blocco di deduplicazione influisce inoltre sulla stima della capacità di deduplicazione. Se, ad esempio, il valore predefinito 16 KB viene modificato in 32 KB, la capacità di deduplicazione prevista risulterà raddoppiata. L'aumento delle dimensioni di blocco della deduplicazione comporta una diminuzione della percentuale di deduplicazione.

Allocazione memoria hash

Specifica il valore di memoria fisica allocata per conservare gli hash. Questo campo viene precompilato con un valore predefinito, che si basa sul calcolo seguente:

Se la memoria fisica del server RPS è inferiore o pari a 4 GB, il valore predefinito dell'**allocazione di memoria hash** corrisponde alla memoria fisica del server RPS.

Se la memoria fisica del server RPS è superiore a 4 GB, Arcserve UDP calcola la memoria libera disponibile al momento del calcolo. Si supponga che la memoria libera disponibile attuale sia di X GB. Arcserve UDP verifica anche le seguenti condizioni:

- Se (X * 80%) > = 4 GB, il valore predefinito dell'**allocazione di memoria hash** è (X * 80%).
- Se (X * 80%) < 4 GB, il valore predefinito dell'**allocazione di memoria hash** è 4 GB.

Esempio: Tenere presente che il server RPS dispone di 32 GB di memoria fisica. Si supponga che il sistema operativo e altre applicazioni utilizzano 4 GB di memoria durante la creazione dell'archivio dati. Di conseguenza, la memoria libera disponibile attuale è pari a 28 GB. Quindi, il valore predefinito dell'**allocazione di memoria hash** è 22.4 GB (22.4 GB = 28 GB * 80%).

La destinazione hash si trova sull'unità SSD (Solid State Drive)

Specifica se la cartella hash si trova su un'unità SSD.

Nota: Configurare la destinazione hash sull'unità SSD locale se è abilitata l'opzione La destinazione hash si trova sull'unità SSD (Solid State Drive).

Destinazione dati

Definisce la cartella di destinazione dei dati per salvare i blocchi di dati univoci effettivi. Utilizzare un disco di maggiori dimensioni per l'archiviazione dei dati contenenti i blocchi di dati originali dell'origine.

Nota: il percorso **Destinazione dati** deve corrispondere a una cartella vuota.

Destinazione indice

Definisce la cartella di destinazione indice per archiviare i file di indice. Selezionare un disco diverso per migliorare il processo di deduplicazione.

Nota: il percorso **Destinazione indice** deve corrispondere a una cartella vuota.

Destinazione hash

Definisce il percorso per archiviare il database hash. Arcserve UDP utilizza l'algoritmo SHA1 per generare l'hash dei dati di origine. I valori hash sono gestiti dal database hash. La selezione di un'unità SSD (Solid State Drive) ad alta velocità può aumentare la capacità di deduplicazione richiedendo

un'allocazione di memoria ridotta. Per ottenere prestazioni hash migliori, si consiglia di formattare il volume SSD come file system NTFS con dimensioni cluster del volume di 4 KB.

Nota: Il percorso **Destinazione hash** deve corrispondere a una cartella vuota.

Nota: Non è possibile specificare lo stesso percorso per le quattro cartelle seguenti: **Cartella archivio dati, Destinazione dati, Destinazione indice** e **Destinazione hash**.

Enable Compression (Abilita compressione)

Consente di specificare che le impostazioni di compressione dei dati siano abilitate.

Tipo di compressione

Specifica se utilizzare il tipo di compressione standard o massimo.

La compressione consente solitamente di ridurre l'utilizzo dello spazio su disco. Tuttavia, comporta una riduzione della velocità di backup a causa dell'aumento di utilizzo della CPU. In base alle necessità, è possibile selezionare una delle tre opzioni disponibili.

Nota: Per ulteriori informazioni, consultare la sezione Tipo di compressione.

Enable Encryption (Abilita crittografia)

Consente di specificare che le impostazioni di crittografia siano abilitate. Quando si seleziona questa opzione, è necessario specificare e confermare la password di crittografia.

La crittografia dei dati corrisponde alla conversione di dati in un modulo incomprensibile senza un meccanismo di decifratura. La soluzione Arcserve Unified Data Protection utilizza algoritmi protetti di crittografia AES (Advanced Encryption Standard) per ottenere la massima protezione e riservatezza dei dati. Per gli archivi dati, sono supportate le opzioni Crittografia o Nessuna crittografia. Per Crittografia, è disponibile solo AES-256.

Se il ripristino viene eseguito sullo stesso computer su cui è stato eseguito il backup, non è necessario immettere la password. La password viene richiesta in caso di ripristino su un computer diverso. Per impostazione predefinita, la password viene richiesta soltanto per il primo accesso. Per immettere la password anche in seguito al primo accesso, l'amministratore dovrà arrestare manualmente il servizio di estensione Explorer dell'agente Arcserve UDP.

Invia un avviso di posta elettronica quando una destinazione sta per raggiungere la capacità massima

Questa opzione consente di configurare l'archivio dati per l'invio di avvisi di posta elettronica. Il server RPS invia avvisi di posta elettronica ai destinatari quando la cartella di destinazione dell'archivio dati è quasi piena.

Configurazione della posta elettronica

Questo pulsante viene visualizzato solo quando si attiva l'opzione di *Invia un avviso di posta elettronica quando una destinazione sta per raggiungere la capacità massima*. Il pulsante consente di fornire un ID di posta elettronica per ricevere gli avvisi. Scegliere il pulsante **Configurazione del messaggio di posta elettronica** per caricare le impostazioni degli avvisi di posta elettronica globali da Console>Impostazioni>Configurazione posta elettronica e avvisi. Se le impostazioni di posta elettronica globali non sono disponibili, facendo clic sul pulsante **Configurazione del messaggio di posta elettronica** si apre la finestra di dialogo **Impostazioni di posta elettronica** per impostare i dettagli di posta elettronica.

L'archivio dati viene creato e visualizzato nel riquadro centrale. Fare clic sull'archivio dati per visualizzare i dettagli nel riquadro destro.

Diversi stati dell'archivio dati

Per l'archivio dati vengono visualizzati diversi stati a seconda dell'attività eseguita. Quando si seleziona un archivio dati dalla scheda delle **risorse**, lo stato dell'archivio dati viene visualizzato nel riquadro sulla destra

- **Interrotto:** l'archivio dati non è attivo. In questo stato, non è possibile inviare alcun processo.
- **Avvio in corso:** l'archivio dati è in corso di avvio. Durante l'avvio dell'archivio dati, lo stato di avanzamento viene visualizzato nella console.
- **Running** (In esecuzione): l'archivio dati è attivo. In questo stato, è possibile inoltrare dei processi.
- **Arresto in corso:** l'archivio dati è in corso di arresto. Durante l'interruzione dell'archivio dati, lo stato di avanzamento viene visualizzato nella Console.
- **Modifica in corso:** è in corso l'aggiornamento dell'archivio dati con i nuovi dati. Durante la modifica dell'archivio dati, lo stato di avanzamento viene visualizzato nella Console.
- **Eliminazione in corso:** è in corso l'eliminazione dell'archivio dati. Durante l'eliminazione dell'archivio dati, lo stato di avanzamento viene visualizzato nella Console.
- **Fuori servizio:** l'archivio dati non funziona correttamente. In questo stato, non è possibile inviare alcun processo. Arrestare l'archivio dati e verificare il motivo di questo comportamento. Lo stato Out of Service (Fuori servizio) di un archivio dati può essere causato dalle situazioni seguenti:
  - Non è possibile accedere alla destinazione di backup dell'archivio dati.
  - Le configurazioni nel registro o nel file sono danneggiate.
  - Sono presenti degli errori interni nell'indice GDD o nel ruolo di dati.
  - Il processo dell'indice GDD o del ruolo di dati è stato arrestato manualmente.
- **Ripristina solo:** nella fase di solo ripristino, tutti i processi che richiedono la scrittura dei dati nell'archivio dati non vengono eseguiti. Si tratta ad esempio dei processi di backup, replica (in entrata), JumpStart (in entrata) e di migrazione dei dati. Tutti gli altri processi che richiedono la lettura dei dati dall'archivio dati vengono invece eseguiti. Lo stato dell'archivio dati viene modificato su Restore Only (Solo ripristino) nelle condizioni seguenti:

- Se il processo del ruolo di hash è stato arrestato manualmente.
- Quando destinazione di backup/dati/indice/capacità del volume del percorso hash/memoria hash assegnata raggiunge il suo limite massimo.

Importante! Quando lo stato dell'archivio dati è impostato su Restore only (Degraded State) (Solo ripristino (Stato danneggiato)) o su Out of service (Bad State) (Fuori servizio (Stato non valido)), l'archivio dati non funziona correttamente. È necessario interrompere l'archivio dati e verificare la causa principale dello stato. Ad esempio, il problema potrebbe essere dovuto al fatto che il volume di deduplicazione dei dati ha raggiunto il limite massimo. Dopo aver risolto la causa principale, avviare l'archivio dati e inviare nuovamente il processo di backup.

Verifica della destinazione

Dopo aver completato tutte le procedure per l'aggiunta del RPS, verificare che sia stato aggiunto correttamente.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: Recovery Point Server**.
3. Verificare i dettagli seguenti:
   - L'RPS creato viene visualizzato.
   - Gli archivi dati vengono visualizzati al di sotto del RPS.

Aggiunta dei server Arcserve Backup

Aggiungere un server Arcserve Backup per archiviare i dati su un nastro. Quando si crea un piano per archiviare i dati su una periferica nastro, è possibile utilizzare questa destinazione.

Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection e fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Server Arcserve Backup**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni:** Nel riquadro centrale viene visualizzata la pagina **Server Arcserve Backup**.
3. Fare clic su **Aggiungi server Arcserve Backup**.

   Viene visualizzata la pagina **Aggiungi server Arcserve Backup**.
4. Immettere le seguenti informazioni:

   Nome nodo/Indirizzo IP

   Specifica il nome nodo o l'indirizzo IP del server Arcserve Backup.

   Tipo di autenticazione

   Specifica il tipo di autenticazione utilizzato per accedere al server Arcserve Backup. Sono disponibili le due opzioni seguenti:

   Autenticazione Windows

   Specifica che per l'accesso al server Arcserve Backup viene utilizzata l'autenticazione di Windows.

   Nota: L'utente di Windows deve essere registrato in Arcserve Backup in precedenza tramite Gestione profili utente di Arcserve Backup.

   Autenticazione Arcserve Backup

   Specifica che per l'accesso al server Arcserve Backup viene utilizzata l'autenticazione di Arcserve Backup.

   Nome utente e Password

   Specifica il nome utente e la password corrispondente per l'accesso al nodo.

   Nota: Utilizzare uno dei seguenti formati per il nome utente: nome computer, nome dominio/nome utente o nome utente.

   Porta

   Specifica il numero porta utilizzato per connettersi al server Arcserve Backup.

Nota: Arcserve UDP utilizza lo stesso numero di porta per connettersi sia al server primario Arcserve Backup che al server membro nel dominio di Arcserve Backup.

5. Fare clic su **Salva**.

   Il server di Arcserve Backup viene aggiunto alla console.

   Dopo aver aggiunto il server di Arcserve Backup nella console, è possibile passare a **Risorse, Destinazione, Server Arcserve Backup** e verificare le informazioni dettagliate relative al supporto nastro.

Aggiunta di una console remota

Aggiungere una console remota per replicare i punti di ripristino in un Recovery Point Server gestito in remoto. È possibile utilizzare la console remota per creare un piano di replica per l'invio di dati alla console di destinazione. È inoltre possibile gestire la console remota aggiunta.

Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Nel riquadro a sinistra, accedere a **Destinazioni**, quindi fare clic su **Console remota**.

   Viene visualizzata la pagina **Destinazioni: Console remota** nel riquadro centrale.
3. Fare clic su **Aggiungi console remota**.

   Viene visualizzata la pagina **Aggiungi console remota**.
4. Immettere le seguenti informazioni:

   Console remota

   Fa riferimento all'URL dell'account della console remota che si desidera aggiungere alla console.

   Nome utente

   Fa riferimento al nome utente utilizzato per l'accesso alla console remota.

   Nota: Utilizzare uno dei seguenti formati per il nome utente: nome computer, nome dominio/nome utente o nome utente.

   Password

   Fa riferimento alla password del nome utente.

   Porta

   Indica il numero di porta che si connette all'interfaccia utente basata sul Web.

   Valore predefinito: 8015

   Protocollo

   Specificare il protocollo che si desidera utilizzare per la comunicazione con il server di destinazione. Le opzioni disponibili sono HTTP e HTTPS.

   Nota: Per una comunicazione più sicura, selezionare il protocollo HTTPS.

   Impostazioni proxy

   Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se

si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

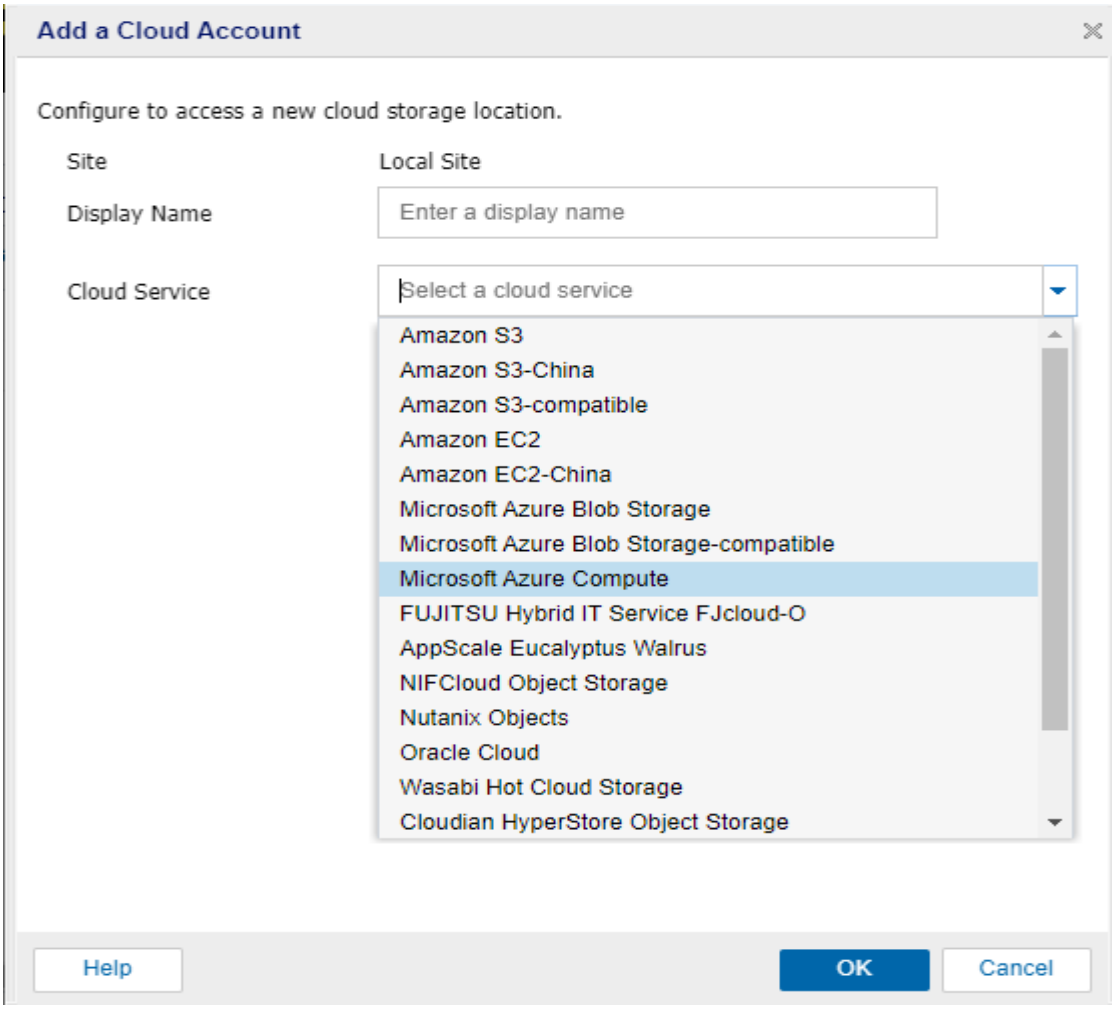
5. Fare clic su **OK**.

   La console remota è stata aggiunta.

Aggiunta di un account cloud

Aggiungere un account cloud per copiare i file o i punti di ripristino in un'archiviazione cloud. È possibile utilizzare gli account corrispondenti durante la creazione delle attività o di uno o più piani per le operazioni Copia punto di ripristino / Copia file /Archivio File /Virtual Standby su cloud / Computer virtuale istantaneo su Amazon EC2. Fornire un nome di archiviazione univoco e selezionare il servizio di archiviazione richiesto dalle opzioni multiple visualizzate nell'elenco a discesa.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.



Le opzioni di configurazione disponibili per ciascun fornitore cloud sono simili (con alcune differenze terminologiche). In caso di differenze viene fornita una descrizione. Aggiungere l'account cloud scelto.

Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Nel campo **Nome visualizzato** specificare un nome univoco.

   Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.
5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

   Vengono visualizzati più campi per la configurazione.
6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   Le opzioni del servizio di archiviazione disponibili sono: Amazon S3, Compatibile con Amazon S3, Microsoft Azure Blob Storage, Compatibile con Microsoft Azure Blob Storage, FUJITSU Hybrid IT Service FJcloud-O, AppScale Eucalyptus Walrus, Amazon EC2, Amazon EC2-China, Microsoft Azure Compute, Nutanix Objects, Wasabi Hot Cloud Storage e Oracle Cloud.

   Nota: fare clic sui nomi corrispondenti ai servizi di archiviazione per visualizzare la modalità di aggiunta di un account cloud per il servizio di archiviazione in questione.

   L'opzione di configurazione dipende dal servizio di archiviazione selezionato.

   L'account cloud del servizio di archiviazione selezionato viene aggiunto alla console Arcserve UDPe visualizzato nella schermata **Destinazioni: Account cloud**. Ad esem-

pio, gli account Amazon S3 vengono visualizzati di seguito.



Come procedere?

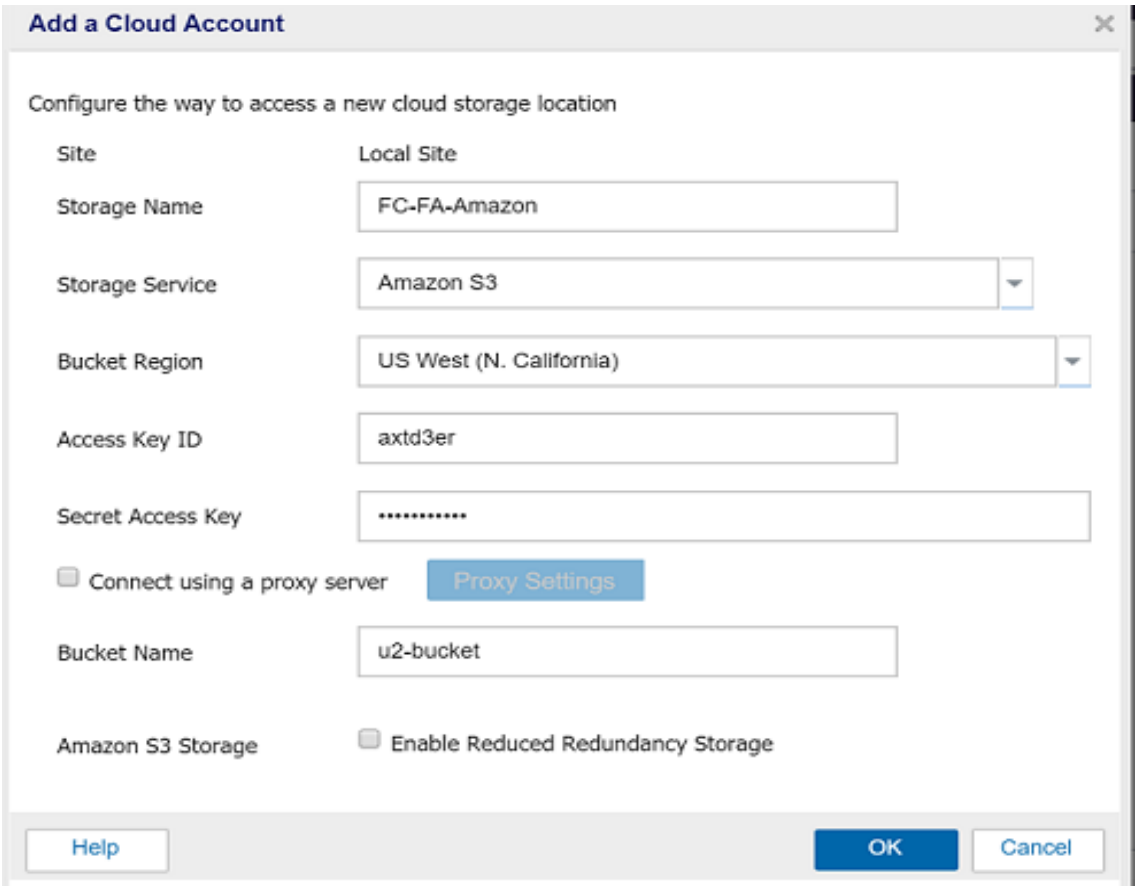
Aggiungere un account cloud per:

- Amazon S3
- Compatibile con Amazon S3
- Microsoft Azure Blob Storage
- Compatibile con Microsoft Azure Blob Storage
- 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

Aggiunta di un account cloud per Amazon S3

Aggiungere un account cloud Amazon S3 per copiare i file o i punti di ripristino nell'archiviazione cloud.

È possibile utilizzare questo account durante la creazione delle attività Copia punto di ripristino / Copia file /Archiviazione file.



Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Nel campo **Nome visualizzato** specificare un nome univoco.

   Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.

5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

   Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   Area di bucket

   Si intende l'area di bucket di Amazon.

   ID del codice di accesso

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Codice di accesso segreto

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché il codice di accesso non è crittografato.

   Importante: Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Impostazioni proxy

   Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

   Nome bucket

   Tutti i file e le cartelle spostati o copiati nel fornitore cloud vengono archiviati e organizzati in bucket. I bucket sono dei contenitori di file utilizzati per raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

   Abilita riduzione di archiviazione dei dati ridondanti

   Con Amazon S3, è possibile selezionare questa opzione per abilitare la riduzione di archiviazione dei dati ridondanti (RRS). L'opzione di archiviazione RSS di Amazon S3 consente di ridurre i costi mediante l'archiviazione dei dati non critici e riproducibili a livelli di ridondanza inferiori rispetto ai livelli di archiviazione standard di Amazon S3. Entrambe le opzioni di archiviazione (con

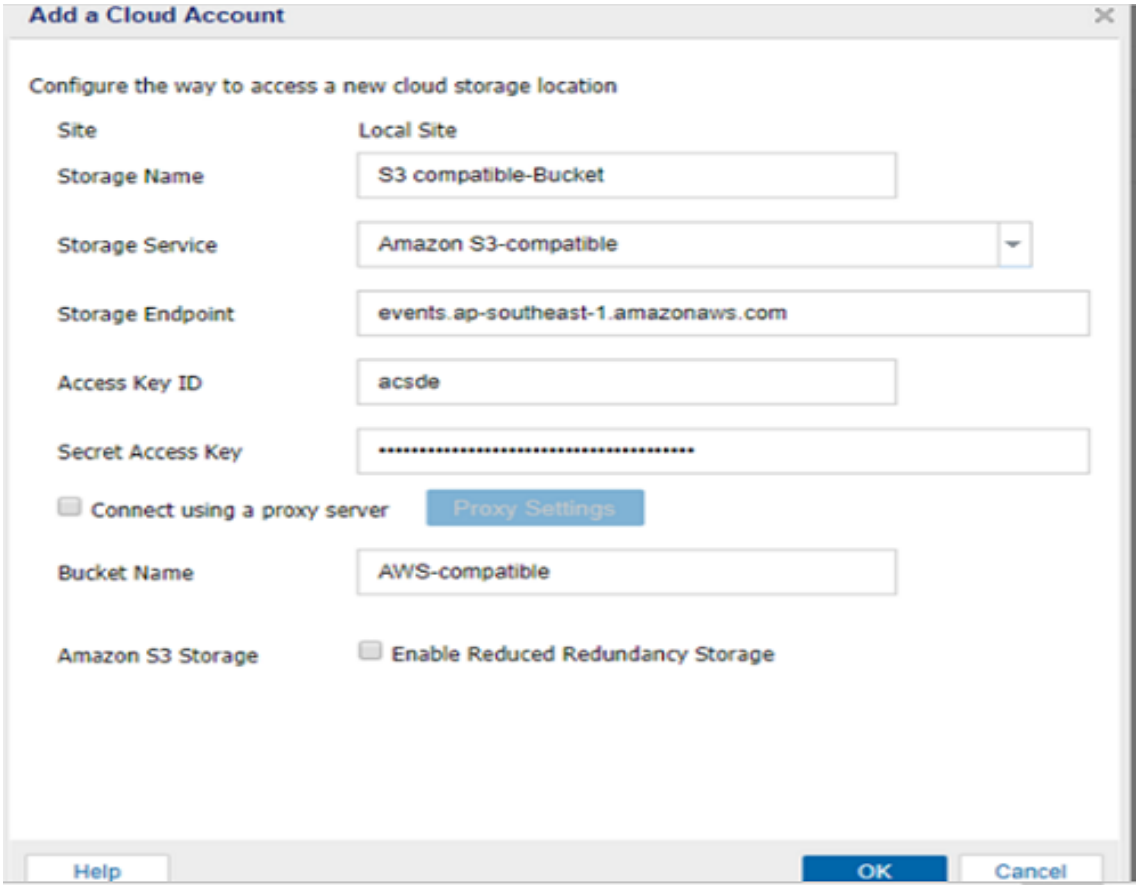
ridondanza standard e ridotta) consentono di archiviare i dati su più dispositivi e periferiche. Tuttavia la riduzione di archiviazione dei dati ridondanti consente di eseguire un numero minore di repliche, riducendo in tal modo i costi. L'archiviazione standard di Amazon S3 e la riduzione di archiviazione dei dati ridondanti presentano gli stessi valori di latenza e velocità. Per impostazione predefinita questa opzione non è selezionata, in quanto Amazon S3 utilizza l'opzione di archiviazione standard.

L'account cloud viene aggiunto alla console.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account cloud compatibile con Amazon S3

Aggiungere un account cloud compatibile con Amazon S3 per copiare i file o i punti di ripristino in un archivio cloud. È possibile utilizzare questo account durante la creazione delle attività Copia punto di ripristino / Copia file /Archiviazione file.



Note:

- Per i fornitori secondari compatibili con S3 che utilizzano il tipo di autenticazione V3/V2 per ottenere la certificazione con Arcserve CCI, il funzionamento sarà corretto in quanto il flag di sostituzione del tipo di firma predefinito è impostato su **True**. Tuttavia, i fornitori secondari che utilizzano l'autenticazione V4 dovranno modificare il flag su **False** nel file AmazonPlugin.properties e riavviare i servizi.

  SIGNER_OVERRIDE=false

- Per il supporto della compatibilità cloud HGST per Amazon S3, è necessario modificare la seguente proprietà di plug-in di Amazon:

  SET_STORAGECLASS_HEADER=false

Questa proprietà consente di ignorare l'intestazione di archiviazione. Pertanto, l'utilizzo di questa proprietà con l'aggiunta dell'attività di copia o archiviazione file come destinazione cloud viene ignorata per impostazione predefinita dall'intestazione di archiviazione.

Il file AmazonPlugin.properties si trova al percorso seguente:

C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN\CCI\Config

Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Nel campo **Nome visualizzato** specificare un nome univoco.

   Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.
5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

   Vengono visualizzati più campi per la configurazione.
6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   Endpoint di archiviazione

   Consente di specificare l'URL del servizio del fornitore. Ad esempio, *http://[server name]:Port No*

   ID del codice di accesso

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Codice di accesso segreto

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché il codice di accesso non è crittografato.

   Importante: Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Impostazioni proxy

Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

Nome bucket

Tutti i file e le cartelle spostati o copiati nel fornitore cloud vengono archiviati e organizzati in bucket. I bucket sono dei contenitori di file utilizzati per raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

Abilita riduzione di archiviazione dei dati ridondanti

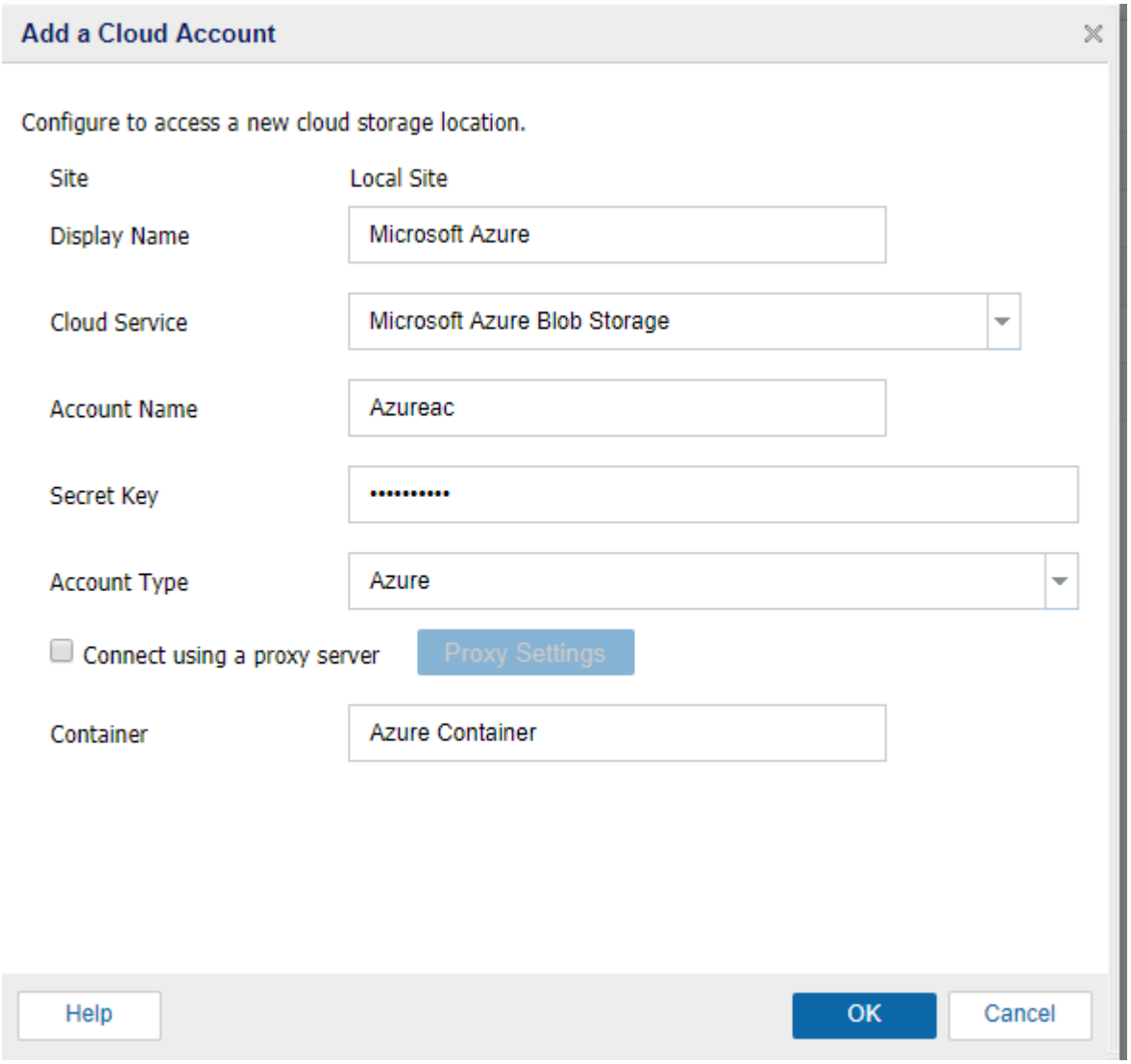
Con Amazon S3, è possibile selezionare questa opzione per abilitare la riduzione di archiviazione dei dati ridondanti (RRS). L'opzione di archiviazione RSS di Amazon S3 consente di ridurre i costi mediante l'archiviazione dei dati non critici e riproducibili a livelli di ridondanza inferiori rispetto ai livelli di archiviazione standard di Amazon S3. Entrambe le opzioni di archiviazione (con ridondanza standard e ridotta) consentono di archiviare i dati su più dispositivi e periferiche. Tuttavia la riduzione di archiviazione dei dati ridondanti consente di eseguire un numero minore di repliche, riducendo in tal modo i costi. L'archiviazione standard di Amazon S3 e la riduzione di archiviazione dei dati ridondanti presentano gli stessi valori di latenza e velocità. Per impostazione predefinita questa opzione non è selezionata, in quanto Amazon S3 utilizza l'opzione di archiviazione standard.

L'account cloud viene aggiunto alla console.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account cloud per Microsoft Azure Blob Storage

Aggiungere un account cloud Microsoft Azure Blob Storage per copiare i file o i punti di ripristino nell'archiviazione cloud. È possibile utilizzare questo account durante la creazione delle attività Copia punto di ripristino / Copia file /Archiviazione file.



Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

Viene visualizzata la pagina **Aggiungi account cloud**.

4. Nel campo **Nome visualizzato** specificare un nome univoco.

   Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.

5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

   Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   Nome account

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Chiave privata

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché il codice di accesso non è crittografato.

   Importante! La chiave privata è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere la chiave privata in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Impostazioni proxy

   Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

   Contenitore

   Tutti i file e le cartelle spostati o copiati nel fornitore cloud vengono archiviati e organizzati nei contenitori. I contenitori consentono di raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

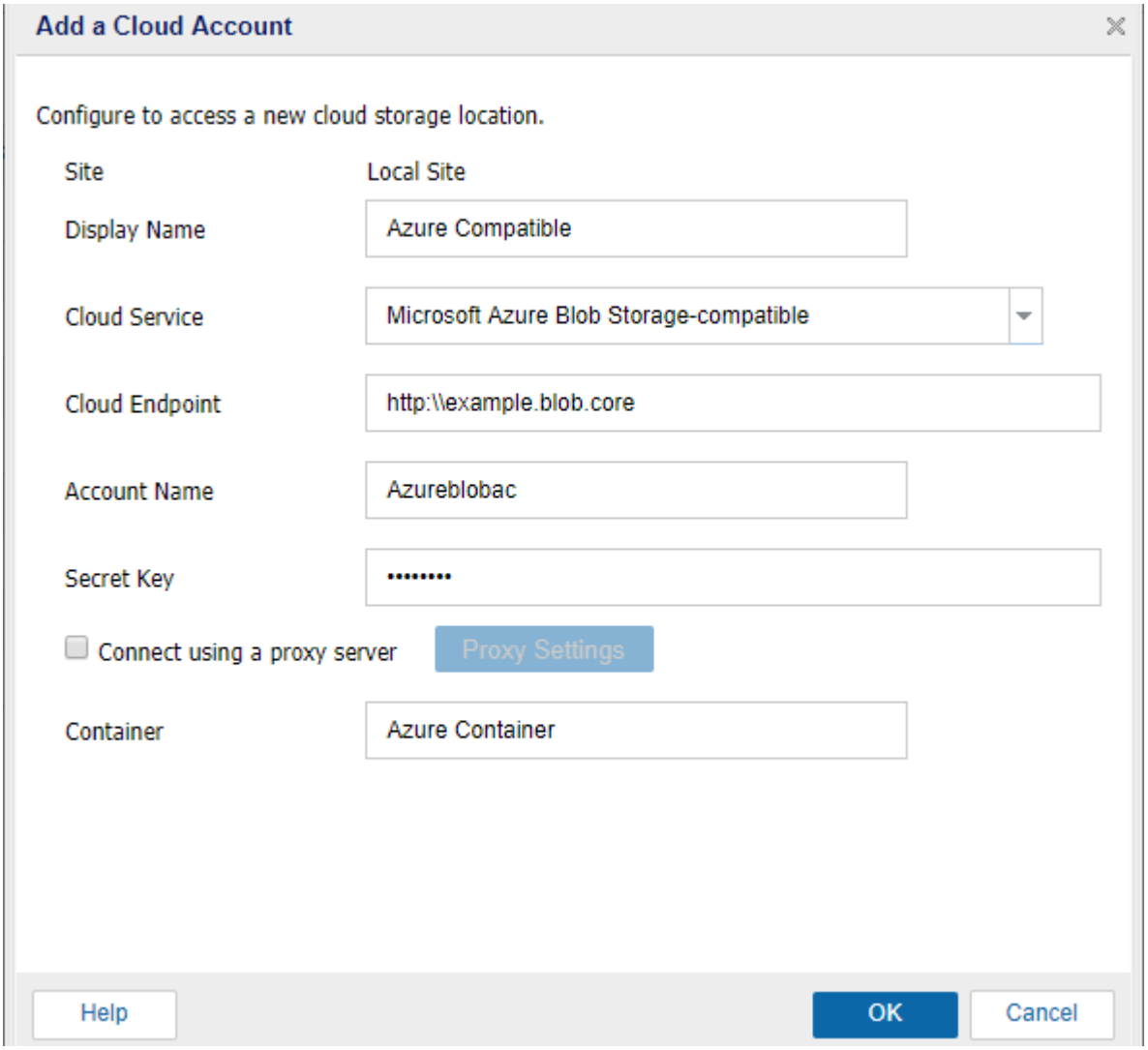
L'account cloud viene aggiunto alla console.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve

UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account cloud compatibile con Microsoft Azure Blob Storage

Aggiungere un account cloud compatibile con Microsoft Azure Blob Storage per copiare i file o i punti di ripristino nell'archiviazione cloud. È possibile utilizzare questo account durante la creazione delle attività Copia punto di ripristino / Copia file /Archiviazione file.



Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.

4. Nel campo **Nome visualizzato** specificare un nome univoco.

   Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.

5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

   Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   Endpoint di archiviazione

   Consente di specificare l'URL del servizio del fornitore. Ad esempio, *http:///[server name]:Port No*

   Nome account

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Chiave privata

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché il codice di accesso non è crittografato.

   Importante! La chiave privata è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere la chiave privata in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Impostazioni proxy

   Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

   Contenitore

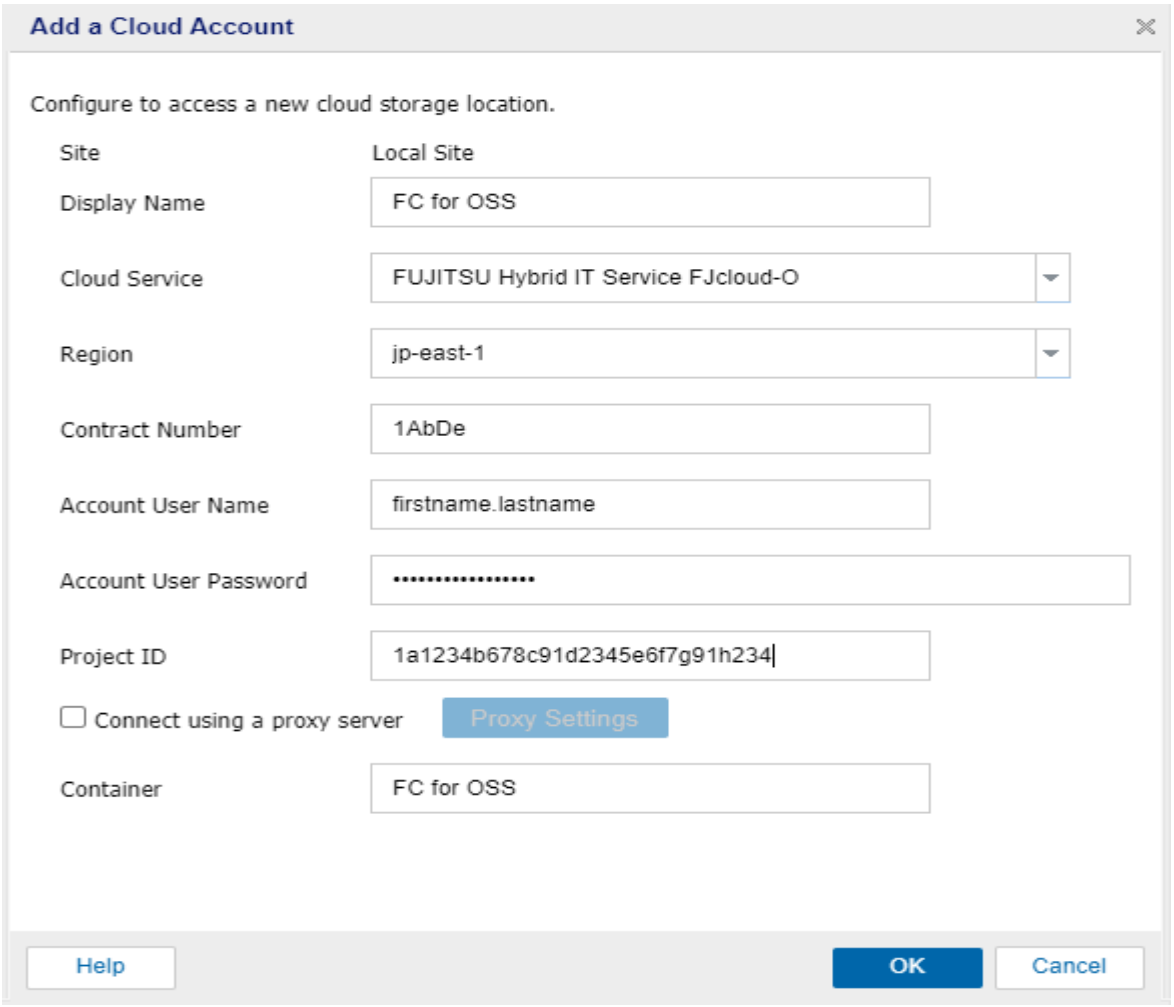
   Tutti i file e le cartelle spostati o copiati nel fornitore cloud vengono archiviati e organizzati nei contenitori. I contenitori consentono di raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

L'account cloud viene aggiunto alla console.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account cloud per FUJITSU Hybrid IT Service FJcloud-O

Aggiungere un account cloud per FUJITSU Hybrid IT Service FJcloud-O per la copia dei file o dei punti di ripristino nell'archiviazione cloud. Durante la creazione di attività di copia file o archiviazione file è possibile utilizzare questo account.



Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Nel campo **Nome visualizzato** specificare un nome univoco.

Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.

5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

   Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   Area di bucket

   Fa riferimento all'area di bucket in FUJITSU Hybrid IT Service FJcloud-O.

   Nome account dell'utente

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Password utente dell'account

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché la password non è crittografata.

   Importante! Questa password è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere la password in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Impostazioni proxy

   Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

   Numero di contratto

   Indica il numero del contratto fornito da FUJITSU Hybrid IT Service FJcloud-O.

   ID progetto

   Indica l'ID del progetto generato da FUJITSU Hybrid IT Service FJcloud-O.

   Contenitore

   Tutti i file e le cartelle spostati o copiati nel fornitore cloud vengono archiviati e organizzati nei contenitori. I contenitori consentono di raggruppare e orga-

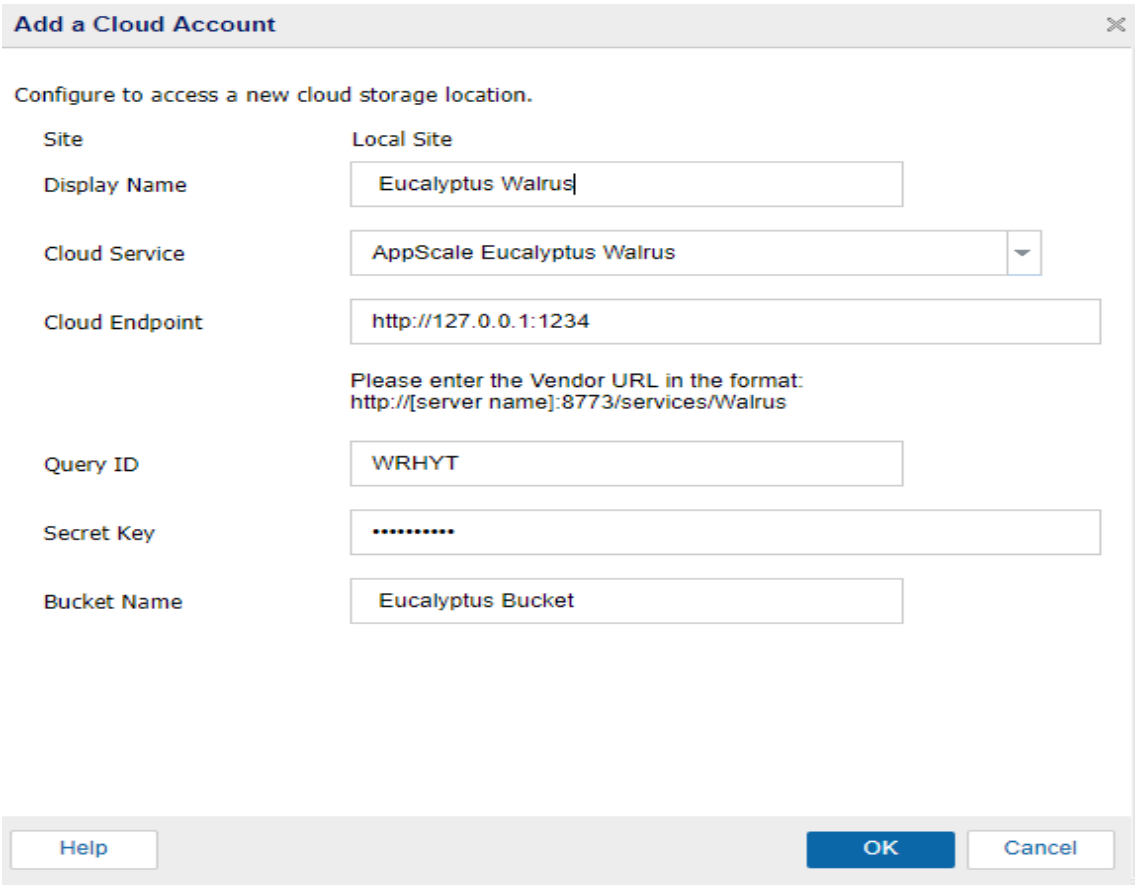
nizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

L'account cloud viene aggiunto alla console.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account cloud per AppScale Eucalyptus Walrus

Aggiungere un account cloud AppScale Eucalyptus Walrus per copiare i file o i punti di ripristino nell'archiviazione cloud. È possibile utilizzare questo account durante la creazione delle attività Copia punto di ripristino / Copia file /Archiviazione file.



Nota: l'utilizzo di AppScale Eucalyptus Walrus come fornitore cloud per la copia file non consente di copiare i file la cui lunghezza di percorso supera i 170 caratteri.

Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Nel campo **Nome visualizzato** specificare un nome univoco.

Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.

5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

   Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   Endpoint di archiviazione

   Consente di specificare l'URL del servizio del fornitore. Ad esempio, *http:///[server name]:Port No*

   ID query

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Chiave privata

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché il codice di accesso non è crittografato.

   Importante! La chiave privata è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere la chiave privata in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Nome bucket

   Tutti i file e le cartelle spostati o copiati nel fornitore cloud vengono archiviati e organizzati in bucket. I bucket sono dei contenitori di file utilizzati per raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

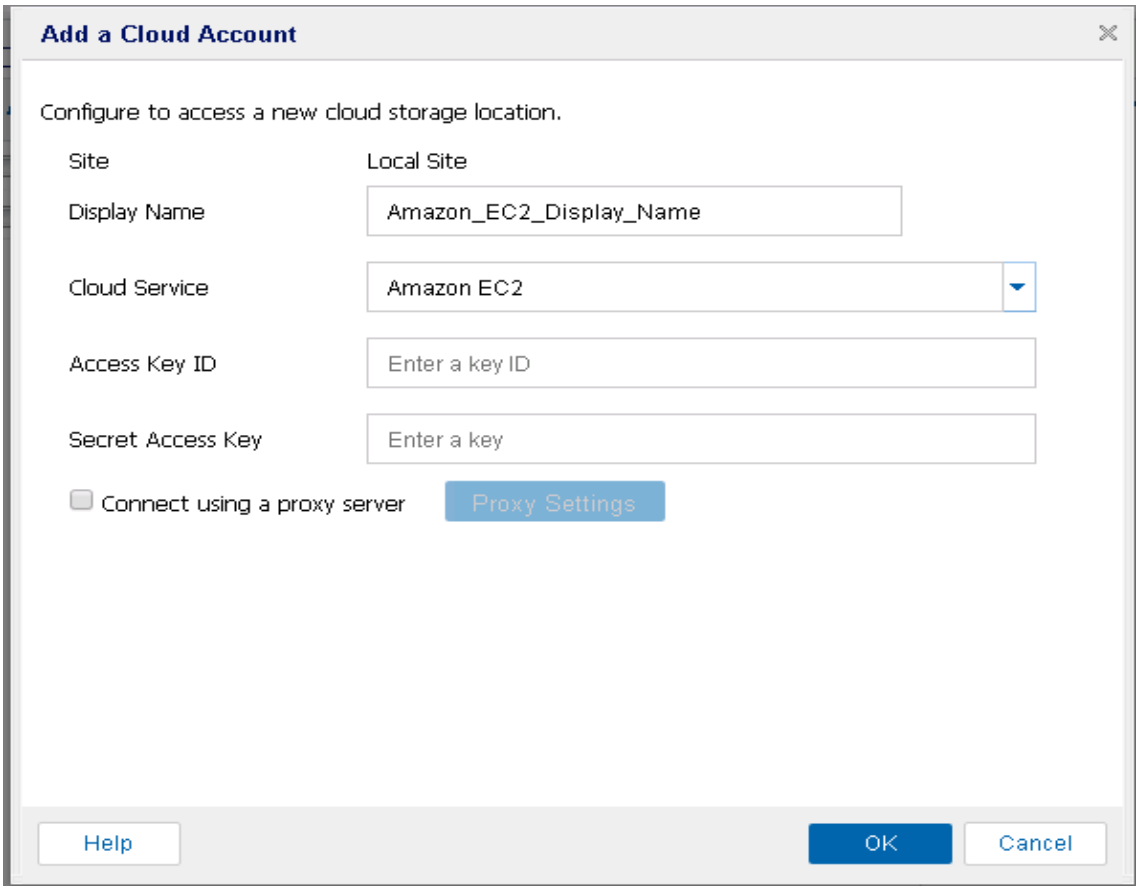
L'account cloud viene aggiunto alla console.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account cloud per Amazon EC2

Aggiungere un account cloud Amazon EC2 per copiare i file o i punti di ripristino nell'archiviazione cloud.

È possibile utilizzare questo account durante la creazione di attività per i piani Virtual Standby su Cloud o Computer virtuale istantaneo su Amazon EC2.



Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Nel campo **Nome visualizzato** specificare un nome univoco.

   Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.

5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

   Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   ID del codice di accesso

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Codice di accesso segreto

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché il codice di accesso non è crittografato.

   Importante: Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Impostazioni proxy

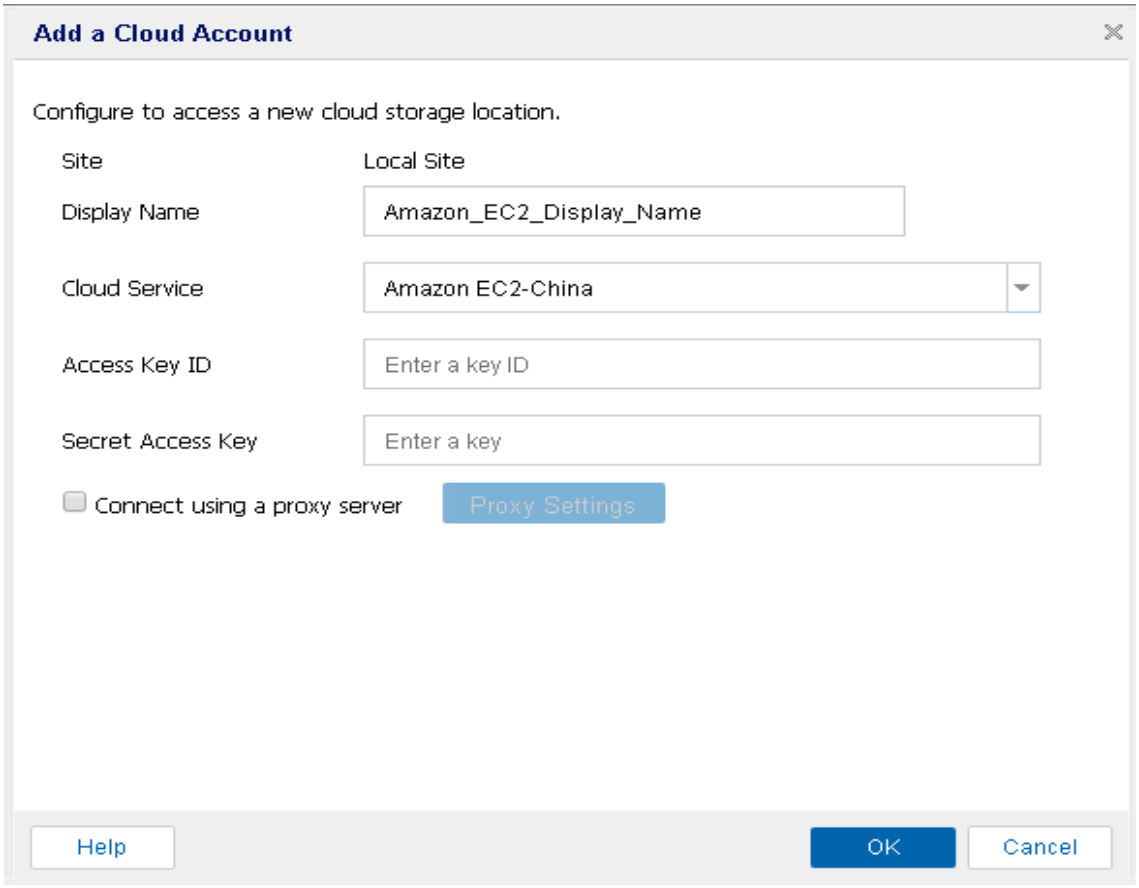
   Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

   L'account cloud viene aggiunto alla console.

   Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account cloud per Amazon EC2-China

Aggiungere un account cloud Amazon EC2-China per copiare i file o i punti di ripristino nell'archiviazione cloud. È possibile utilizzare questo account durante la creazione di attività per i piani Virtual Standby su Cloud o Computer virtuale istantaneo su Amazon EC2.



Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Nel campo **Nome visualizzato** specificare un nome univoco.

   Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.
5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   ID del codice di accesso

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Codice di accesso segreto

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché il codice di accesso non è crittografato.

   Importante: Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Impostazioni proxy

   Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

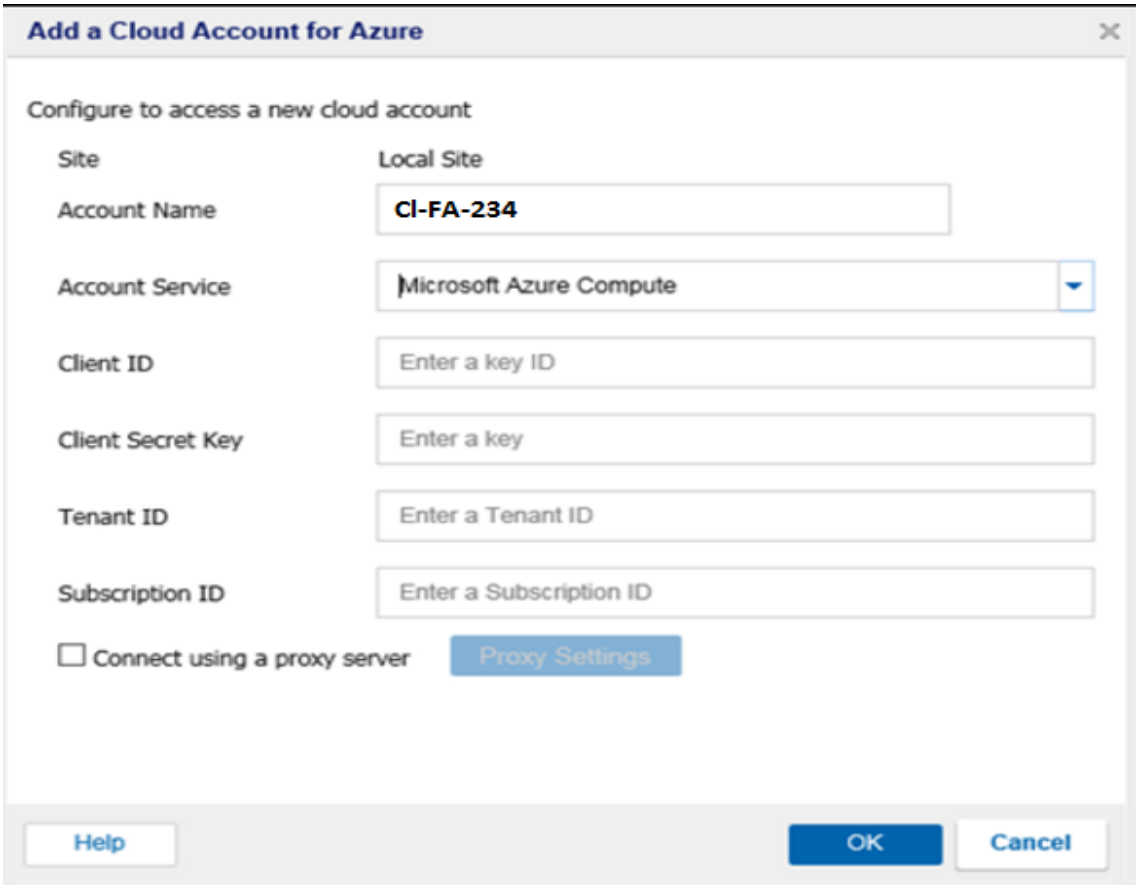
L'account cloud viene aggiunto alla console.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account cloud per Microsoft Azure Compute

Aggiungere un account cloud Microsoft Azure Compute per copiare i file o i punti di ripristino nell'archiviazione cloud. È possibile utilizzare questo account durante la creazione di attività per i piani Virtual Standby su Cloud o Computer virtuale istantaneo su Microsoft Azure.

Nota: per aggiungere un account cloud per Microsoft Azure, è necessario che vengano soddisfatti i prerequisiti. Per ulteriori informazioni, consultare la sezione Prerequisiti.



Effettuare le operazioni seguenti:

1. Accedere ad Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Per il campo **Nome account**, specificare un nome univoco.

Il campo Nome account specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome di archiviazione univoco.

5. Selezionare l'opzione dall'elenco a discesa **Servizio account**.

   Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   ID client

   Fa riferimento all'ID applicazione dell'applicazione Azure Active Directory. Copiare l'ID client preparato nell'editor di testo.

   Chiave segreta client

   Fa riferimento alla chiave di autenticazione generata per l'applicazione Azure Active Directory immessa come ID client. Copiare la chiave segreta client preparata nell'editor di testo.

   Importante! La chiave privata è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere la chiave privata in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   ID tenant

   Fa riferimento all'ID di Azure Active Directory in cui è stata creata l'applicazione Azure Active Directory. Copiare l'ID tenant preparato nell'editor di testo.

   ID sottoscrizione

   Fa riferimento a un ID univoco globale (GUID) che identifica in modo univoco la sottoscrizione per l'utilizzo del servizi Azure. Copiare l'ID di sottoscrizione nell'editor di testo.

   Impostazioni proxy

   Specifica le impostazioni del server proxy fornite. Selezionare **Connetti tramite server proxy** per abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. È quindi necessario fornire le informazioni di autenticazione corrispondenti richieste per l'utilizzo del server proxy.

L'account cloud viene aggiunto alla console.

Prerequisiti per l’aggiunta di un account cloud per Microsoft Azure

Prima di creare un account cloud per Microsoft Azure, è necessario completare le seguenti attività preliminari obbligatorie nel seguente ordine:

1. Preparare i server per effettuare la distribuzione come Console Arcserve UDP e Recovery Point Server. Tali server devono soddisfare i requisiti di sistema per ciascun componente.
2. Verificare di disporre delle autorizzazioni necessarie per creare un'applicazione in Azure Active Directory.

   Per ulteriori informazioni, consultare la sezione Verifica delle autorizzazioni di Azure Active Directory nella documentazione di Microsoft.
3. Creare un'applicazione Azure Active Directory. In un editor di testo (ad esempio Blocco note), copiare l’ID applicazione dell’applicazione e l’etichetta come ID client.

   Per ulteriori informazioni, consultare la sezione Verifica delle autorizzazioni di Azure Active Directory nella documentazione di Microsoft.
4. Ottenere l’ID applicazione e generare una chiave di autenticazione per questa applicazione. Copiare la stringa della chiave di autenticazione nell’editor di testo (ad esempio Blocco note) e contrassegnare la stringa come Chiave segreta client.

   Per ulteriori informazioni, consultare la sezione Acquisizione dell’ID applicazione e della chiave di autenticazione nella documentazione di Microsoft.
5. Ottenere l’ID del tenant, ovvero l’ID di Azure Active Directory in cui è stata creata l’applicazione. In un editor di testo (ad esempio Blocco note), copiare l’ID ed etichettarlo come ID tenant.

   Per ulteriori informazioni, consultare la sezione Acquisizione dell’ID tenant nella documentazione di Microsoft.
6. Eseguire la procedura riportata di seguito per assegnare il ruolo di collaboratore all’applicazione.
   a. Dal riquadro a sinistra del menu del portale Microsoft Azure, selezionare **Sottoscrizioni**.
   b. Selezionare la sottoscrizione.
   c. Selezionare la scheda Access Control (IAM).

d. Aggiungere l'applicazione.

e. Assegnare il ruolo di collaboratore all'applicazione.

Per ulteriori informazioni, consultare la sezione Assegnazione di un'applicazione al ruolo nella documentazione di Microsoft.

7. Ottenere l'ID di sottoscrizione ad Azure.

Nota: l'ID di sottoscrizione è un GUID che identifica in modo univoco la sottoscrizione per l'utilizzo dei servizi Azure.

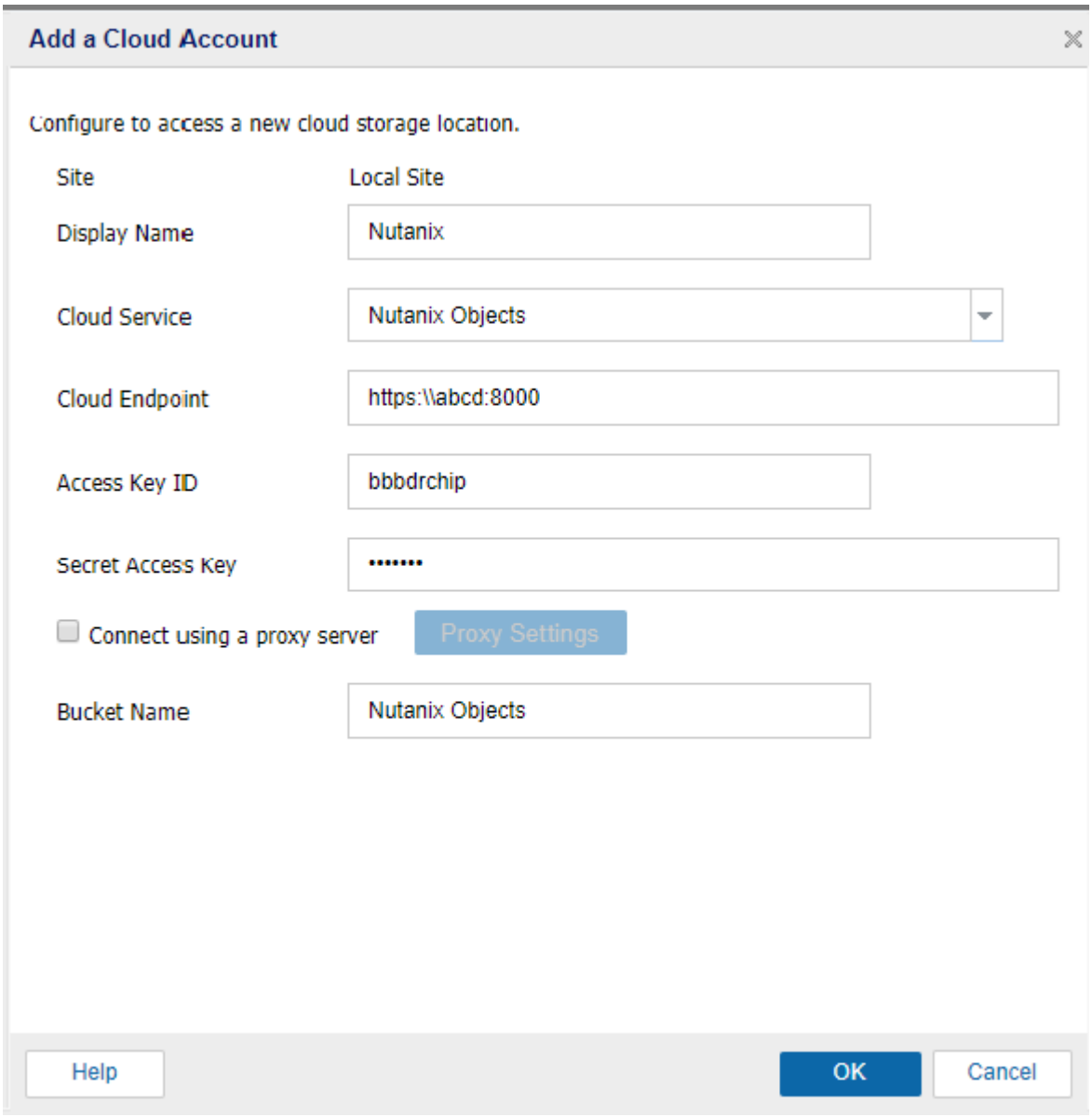
a. Accedere al portale Microsoft Azure.

b. Nel riquadro di navigazione a sinistra, fare clic su Sottoscrizioni.

L'elenco delle sottoscrizioni viene visualizzato con l'ID di sottoscrizione.

Aggiunta di un account cloud per Nutanix Objects

Aggiungere un account cloud Nutanix Objects per copiare i file o i punti di ripristino in un archivio cloud. È possibile utilizzare questo account durante la creazione delle attività Copia punto di ripristino / Copia file /Archiviazione file.



Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Nel campo **Nome visualizzato** specificare un nome univoco.

   Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.
5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   Endpoint di archiviazione

   Consente di specificare l'URL del servizio del fornitore. Ad esempio, *http:///[server name]:Port No*

   ID del codice di accesso

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Codice di accesso segreto

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché il codice di accesso non è crittografato.

   Importante: Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Impostazioni proxy

   Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

   Nome bucket

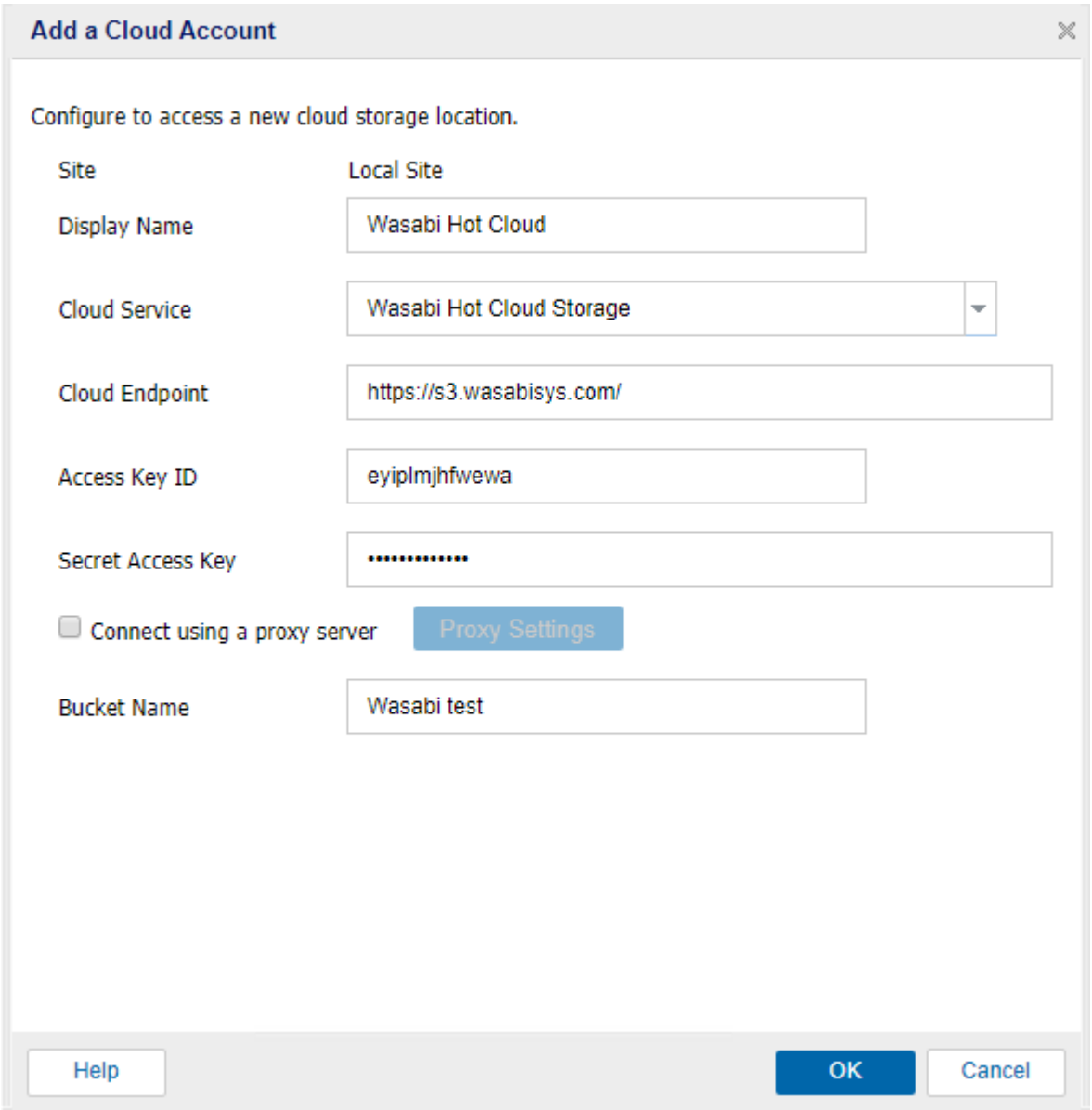
   Tutti i file e le cartelle spostati o copiati nel fornitore cloud vengono archiviati e organizzati in bucket. I bucket sono dei contenitori di file utilizzati per raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

L'account cloud viene aggiunto alla console.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account cloud per Wasabi Hot Cloud Storage

Aggiungere un account cloud Wasabi Hot Cloud Storage per copiare i file o i punti di ripristino nell'archiviazione cloud. È possibile utilizzare questo account durante la creazione delle attività Copia punto di ripristino / Copia file /Archiviazione file.



Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

Viene visualizzata la pagina **Aggiungi account cloud**.

4. Nel campo **Nome visualizzato** specificare un nome univoco.

   Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.

5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

   Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   Endpoint di archiviazione

   Per Wasabi Hot Cloud Storage sono supportate le tre aree seguenti:

   - Per l'area Stati Uniti occidentali l'endpoint è s3.wasabisys.com.
   - Per l'area Stati Uniti orientali l'endpoint è s3.us-west-1.wasabisys.com.
   - Per l'area Stati Uniti centrali l'endpoint è s3.eu-central-1.wasabisys.com.

   ID del codice di accesso

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Codice di accesso segreto

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché il codice di accesso non è crittografato.

   Importante: Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Impostazioni proxy

   Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

   Nome bucket

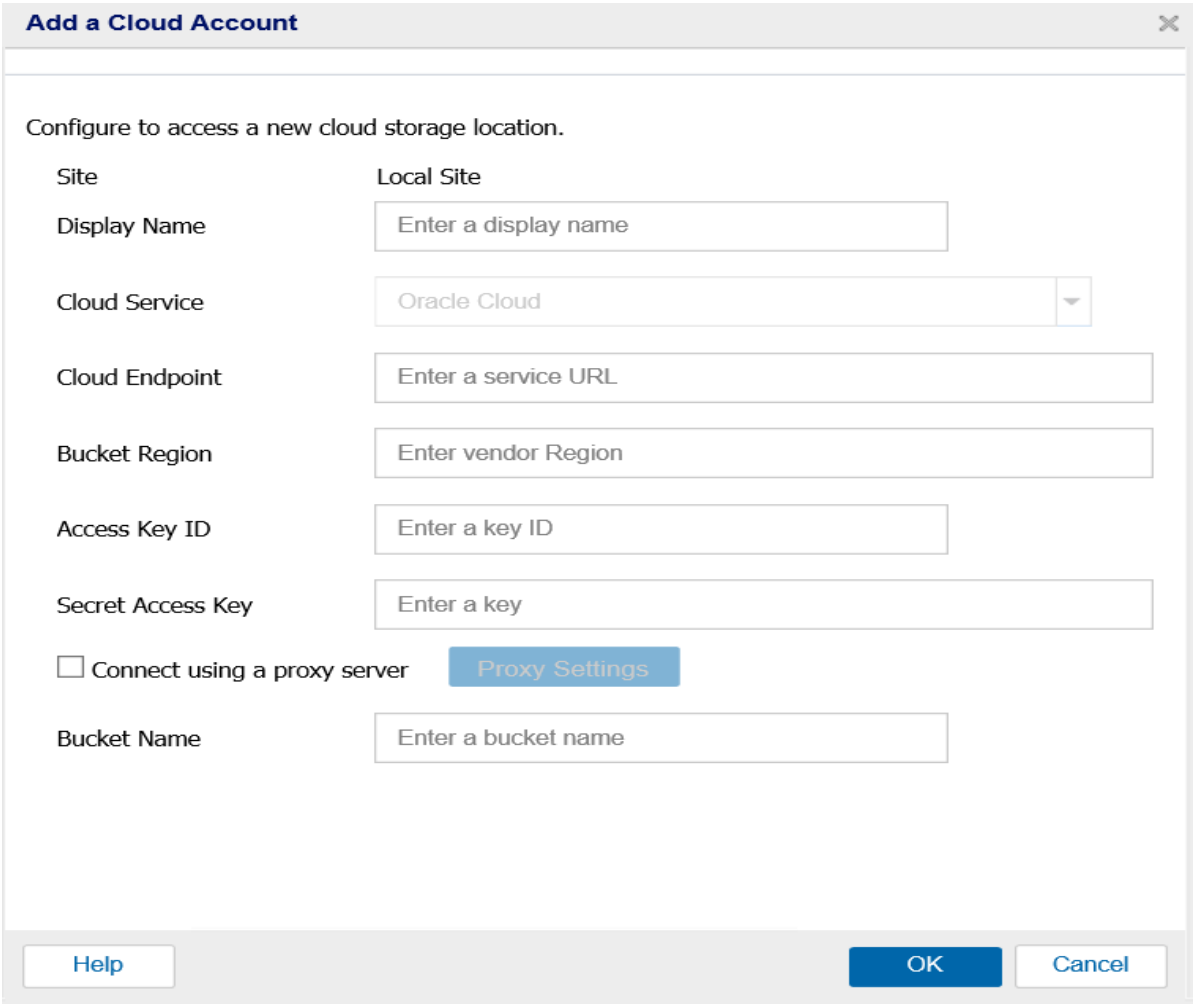
Tutti i file e le cartelle spostati o copiati nel fornitore cloud vengono archiviati e organizzati in bucket. I bucket sono dei contenitori di file utilizzati per raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

L'account cloud viene aggiunto alla console.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account cloud per Oracle Cloud

Aggiungere un account cloud Oracle con per copiare i file o i punti di ripristino in un'archiviazione cloud. È possibile utilizzare questo account durante la creazione delle attività Copia punto di ripristino / Copia file /Archiviazione file.



Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Nel campo **Nome visualizzato** specificare un nome univoco.

Il nome visualizzato specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome visualizzato univoco.

5. Selezionare l'opzione dall'elenco a discesa **Servizio cloud**.

   Vengono visualizzati più campi per la configurazione.

6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   Cloud Endpoint

   Consente di specificare l'URL del servizio del fornitore. Ad esempio, *http-s://namespace.compat.objectstorage.region.oraclecloud.com*

   Area di bucket

   Fa riferimento all'area bucket del fornitore.

   ID del codice di accesso

   Identifica l'utente che sta richiedendo l'accesso a questa posizione.

   Codice di accesso segreto

   Indica la password utilizzata per verificare l'autenticità della richiesta di accesso al percorso perché il codice di accesso non è crittografato.

   Importante: Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   Impostazioni proxy

   Specifica le impostazioni del server proxy fornite. Selezionare la casella di controllo **Connetti tramite server proxy** se si desidera abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

   Nome bucket

   Tutti i file e le cartelle spostati o copiati nel fornitore cloud vengono archiviati e organizzati in bucket. I bucket sono dei contenitori di file utilizzati per rag-

gruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

L'account cloud viene aggiunto alla console.

Nota: se in una versione precedente alla 6.0 di Arcserve UDP sono stati configurati i processi di copia file e archiviazione file e si effettua l'aggiornamento alla versione più recente di Arcserve UDP, per il processo di archiviazione file Arcserve UDP crea un nuovo bucket cloud con il suffisso **-fa**. Il processo di copia file utilizza lo stesso bucket della versione precedente.

Aggiunta di un account Arcserve Cloud

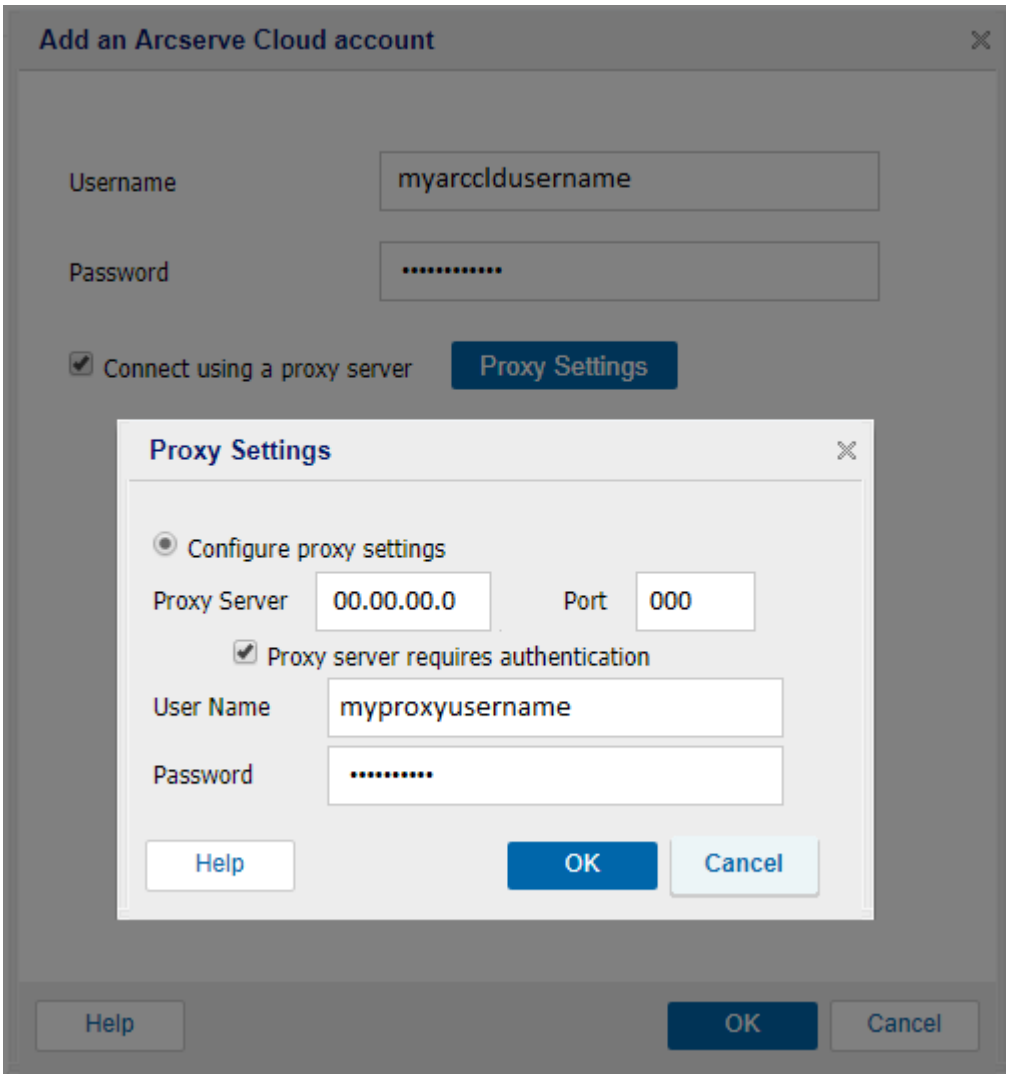
Aggiungere un account Arcserve Cloud per copiare i file o i punti di ripristino nell'archiviazione Arcserve Cloud.

Effettuare le operazioni seguenti:

1. Accedere ad Arcserve UDP e fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni** e fare clic su **Arcserve Cloud**.

   Destinazioni: viene visualizzata la schermata della pagina di Arcserve Cloud.
3. Fare clic su **Aggiungi un account Arcserve Cloud**.

   Viene visualizzata una schermata dell'account Arcserve Cloud.



4. Immettere le seguenti informazioni:

   Nome utente

   Specifica il nome utente dell'account Arcserve Cloud registrato con Arcserve.

   Password

   Specifica la password dell'account utente Arcserve Cloud corrispondente registrato con Arcserve.

   Connetti tramite un server proxy

   Selezionare questa opzione per connettere Arcserve Cloud tramite un server proxy con connessione a Internet.

   Impostazioni proxy

   Fare clic su Impostazioni proxy se è selezionata l'opzione Connetti tramite server proxy.

Viene visualizzata la finestra Impostazioni proxy. Immettere i seguenti dettagli e fare clic su **OK**.

Server proxy

Specifica l'indirizzo IP del server proxy.

Porta

Specifica il numero di porta aperto nel server proxy.

Il server proxy richiede l'autenticazione

Selezionare questa opzione se si desidera che l'accesso al server proxy debba richiede l'autenticazione.

Nome utente

Specifica il nome utente con accesso al server proxy.

Password

Specifica la password dell'account utente corrispondente con accesso al server proxy.

5. Fare clic su **OK**.

   L'account Arcserve Cloud è stato aggiunto correttamente.

Gestione di un archivio dati

In seguito alla creazione di un archivio dati, potrebbe essere necessario eseguire operazioni varie come la modifica, l'eliminazione, l'interruzione e l'avvio di un archivio dati.

È inoltre possibile eseguire processi di unione on demand per più nodi al fine di creare spazio aggiuntivo sul disco.

Come procedere?

- Verifica dei prerequisiti
- Modifica di un archivio dati
- Eliminazione di un archivio dati della Console
- Interruzione di un archivio dati
- Avvio di un archivio dati
- Monitoraggio della capacità di spazio disponibile per l'archivio dati
- Accesso ai punti di ripristino in un archivio dati
- Eliminazione dei dati del nodo dall'archivio dati
- Modifica del limite di nodi attivi simultanei per il backup manuale
- Esecuzione manuale o su richiesta di un processo di unione
- Risoluzione dei problemi: Come utilizzare un archivio dati quando la cartella di destinazione di backup è completa

Verifica dei prerequisiti

Per gestire un archivio dati, completare i seguenti passaggi preliminari:

- Aggiunta di un archivio dati.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Modifica di un archivio dati

È possibile modificare un archivio dati già esistente; tuttavia, esistono alcune restrizioni per le quali non è possibile modificare i seguenti dettagli di un archivio dati:

- Dettagli di compressione
- Archivio dati di non deduplicazione in un archivio dati di deduplicazione o archivio dati di deduplicazione in un archivio dati di non deduplicazione.
- Opzioni di deduplicazione: Deduplicazione dei dati e Dimensione di blocco della deduplicazione.

Considerazioni precedenti alla modifica di un archivio dati:

- Se si modifica il percorso dell'archivio dati o la password di crittografia, tutti i processi in esecuzione in tale archivio dati, inclusi i processi che attendono in coda, vengono annullati. Qualsiasi modifica al nome dell'archivio dati, alla dimensione della memoria hash o al numero di nodi attivi simultaneamente non ha alcun impatto sui processi in esecuzione.
- Per un archivio dati di non deduplicazione: per modificare il percorso dell'archivio dati, mantenere la cartella di destinazione di backup vuota.
- Per un archivio dati di deduplicazione: per modificare il percorso dell'archivio dati, mantenere le cartelle seguenti vuote:
  - Cartella di destinazione del backup
  - Destinazione dati
  - Destinazione indice
  - Destinazione hash
- L'opzione **Password di crittografia** è modificabile soltanto se viene selezionata l'opzione **Crittografa dati** durante la creazione dell'archivio dati.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni:** La pagina **Recovery Point Server** mostra l'elenco di Recovery Point Server disponibili.
3. Espandere un Recovery Point Server.

   È possibile visualizzare l'elenco di archivi dati associati al Recovery Point Server.
4. Eseguire una delle seguenti operazioni:

- Fare clic con il tasto destro del mouse sul nome dell'archivio dati.
- Selezionare l'archivio dati e dal riquadro centrale fare clic sul menu a discesa **Azioni**.

Viene visualizzato un elenco di opzioni.

5. Fare clic su **Modifica**.

   Viene visualizzata la pagina **Modifica archivio dati**.

6. Aggiornare i campi obbligatori, quindi fare clic su **Salva**.

   Recovery Point Server

   Definisce il Recovery Point Server in cui viene creato l'archivio dati. Il Recovery Point Server è già aggiunto per impostazione predefinita.

   Nome archivio dati

   Definisce il nome dell'archivio dati.

   Cartella archivio dati

   Definisce la posizione del percorso della cartella in cui viene creato l'archivio dati. Fare clic su Sfoglia per selezionare la cartella di destinazione.

   Note:

   - È ora possibile attivare e visualizzare i volumi nascosti. Per ulteriori informazioni, consultare la sezione Attivazione e visualizzazione dei volumi nascosti durante la creazione di un archivio dati.
   - Per l'archivio dati di deduplicazione e non di deduplicazione, il percorso di destinazione deve essere una cartella vuota.

   Limite nodi attivi simultaneamente

   Specifica il numero massimo di processi simultanei dell'archivio dati.

   Valore predefinito: 4

   Corrisponde a un valore compreso tra 1 e 9999. Il valore indica il numero di processi che possono essere eseguiti contemporaneamente. Se i processi in esecuzione corrispondono al numero indicato, un processo viene inserito nella coda e potrà essere avviato soltanto al completamento del processo in esecuzione. Un processo completato può essere un processo terminato, annullato o non riuscito.

   Questo numero viene applicato ai tipi di processo ma non ai nodi del server. Ad esempio, il numero 5 indica che cinque processi di backup sono in esecuzione. Qualsiasi processo pianificato dopo cinque processi di backup dovrà attendere

nella coda. Tuttavia, è possibile inoltrare un processo diverso, come ad esempio un processo di catalogo di file system.

Se il valore è maggiore di 16 o 32, vengono visualizzati dei messaggi indicanti l'aumento della domanda sulla periferica hardware.

Nota: Il limite influisce solamente sui processi di replica in uscita, ma non sui processi di replica in entrata. Il limite non influisce sui processi di ripristino o processi di ripristino bare metal. Tali processi non vengono inseriti nella coda.

Enable Deduplication (Abilita deduplicazione)

Specifica che per l'archivio dati è abilitata la deduplicazione. Arcserve UDP supporta entrambi i tipi di deduplicazione: Deduplicazione all'origine e Deduplicazione globale. La deduplicazione dal lato origine impedisce che i blocchi di dati duplicati vengano spostati nella rete da parte di un determinato agente. La deduplicazione globale elimina i dati duplicati su tutti i computer client basati sul livello cluster del computer.

Dimensione di blocco della deduplicazione

Definisce la dimensione del blocco della deduplicazione. Le opzioni sono 4 KB, 8 KB, 16 KB, 32 KB e 64 KB. La dimensione del blocco di deduplicazione influisce inoltre sulla stima della capacità di deduplicazione. Se, ad esempio, il valore predefinito 16 KB viene modificato in 32 KB, la capacità di deduplicazione prevista risulterà raddoppiata. L'aumento delle dimensioni di blocco della deduplicazione comporta una diminuzione della percentuale di deduplicazione.

Allocazione memoria hash

Specifica il valore di memoria fisica allocata per conservare gli hash. Questo campo viene precompilato con un valore predefinito, che si basa sul calcolo seguente:

Se la memoria fisica del server RPS è inferiore o pari a 4 GB, il valore predefinito dell'**allocazione di memoria hash** corrisponde alla memoria fisica del server RPS.

Se la memoria fisica del server RPS è superiore a 4 GB, Arcserve UDP calcola la memoria libera disponibile al momento del calcolo. Si supponga che la memoria libera disponibile attuale sia di X GB. Arcserve UDP verifica anche le seguenti condizioni:

- Se (X * 80%) > = 4 GB, il valore predefinito dell'**allocazione di memoria hash** è (X * 80%).

- Se (X * 80%) < 4 GB, il valore predefinito dell'**allocazione di memoria hash** è 4 GB.

  Esempio: Tenere presente che il server RPS dispone di 32 GB di memoria fisica. Si supponga che il sistema operativo e altre applicazioni utilizzano 4 GB di memoria durante la creazione dell'archivio dati. Di conseguenza, la memoria libera disponibile attuale è pari a 28 GB. Quindi, il valore predefinito dell'**allocazione di memoria hash** è 22.4 GB (22.4 GB = 28 GB * 80%).

La destinazione hash si trova sull'unità SSD (Solid State Drive)

Specifica se la cartella hash si trova su un'unità SSD.

Nota: Configurare la destinazione hash sull'unità SSD locale se è abilitata l'opzione La destinazione hash si trova sull'unità SSD (Solid State Drive).

Destinazione dati

Definisce la cartella di destinazione dei dati per salvare i blocchi di dati univoci effettivi. Utilizzare un disco di maggiori dimensioni per l'archiviazione dei dati contenenti i blocchi di dati originali dell'origine.

Nota: il percorso **Destinazione dati** deve corrispondere a una cartella vuota.

Destinazione indice

Definisce la cartella di destinazione indice per archiviare i file di indice. Selezionare un disco diverso per migliorare il processo di deduplicazione.

Nota: il percorso **Destinazione indice** deve corrispondere a una cartella vuota.

Destinazione hash

Definisce il percorso per archiviare il database hash. Arcserve UDP utilizza l'algoritmo SHA1 per generare l'hash dei dati di origine. I valori hash sono gestiti dal database hash. La selezione di un'unità SSD (Solid State Drive) ad alta velocità può aumentare la capacità di deduplicazione richiedendo un'allocazione di memoria ridotta. Per ottenere prestazioni hash migliori, si consiglia di formattare il volume SSD come file system NTFS con dimensioni cluster del volume di 4 KB.

Nota: Il percorso **Destinazione hash** deve corrispondere a una cartella vuota.

Nota: Non è possibile specificare lo stesso percorso per le quattro cartelle seguenti: **Cartella archivio dati, Destinazione dati, Destinazione indice** e **Destinazione hash**.

Enable Compression (Abilita compressione)

Consente di specificare che le impostazioni di compressione dei dati siano abilitate.

Tipo di compressione

Specifica se utilizzare il tipo di compressione standard o massimo.

La compressione consente solitamente di ridurre l'utilizzo dello spazio su disco. Tuttavia, comporta una riduzione della velocità di backup a causa dell'aumento di utilizzo della CPU. In base alle necessità, è possibile selezionare una delle tre opzioni disponibili.

Nota: Per ulteriori informazioni, consultare la sezione Tipo di compressione.

Enable Encryption (Abilita crittografia)

Consente di specificare che le impostazioni di crittografia siano abilitate. Quando si seleziona questa opzione, è necessario specificare e confermare la password di crittografia.

La crittografia dei dati corrisponde alla conversione di dati in un modulo incomprensibile senza un meccanismo di decifratura. La soluzione Arcserve Unified Data Protection utilizza algoritmi protetti di crittografia AES (Advanced Encryption Standard) per ottenere la massima protezione e riservatezza dei dati. Per gli archivi dati, sono supportate le opzioni Crittografia o Nessuna crittografia. Per Crittografia, è disponibile solo AES-256.

Se il ripristino viene eseguito sullo stesso computer su cui è stato eseguito il backup, non è necessario immettere la password. La password viene richiesta in caso di ripristino su un computer diverso. Per impostazione predefinita, la password viene richiesta soltanto per il primo accesso. Per immettere la password anche in seguito al primo accesso, l'amministratore dovrà arrestare manualmente il servizio di estensione Explorer dell'agente Arcserve UDP.

Invia un avviso di posta elettronica quando una destinazione sta per raggiungere la capacità massima

Questa opzione consente di configurare l'archivio dati per l'invio di avvisi di posta elettronica. Il server RPS invia avvisi di posta elettronica ai destinatari quando la cartella di destinazione dell'archivio dati è quasi piena.

Configurazione della posta elettronica

Questo pulsante viene visualizzato solo quando si attiva l'opzione di *Invia un avviso di posta elettronica quando una destinazione sta per raggiungere la capacità massima*. Il pulsante consente di fornire un ID di posta elettronica per ricevere gli avvisi. Scegliere il pulsante **Configurazione del messaggio di posta elettronica** per caricare le impostazioni degli avvisi di posta elettronica globali da Console>Impostazioni>Configurazione posta elettronica e

avvisi. Se le impostazioni di posta elettronica globali non sono disponibili, facendo clic sul pulsante **Configurazione del messaggio di posta elettronica** si apre la finestra di dialogo **Impostazioni di posta elettronica** per impostare i dettagli di posta elettronica.

L'archivio dati è stato aggiornato.

Modifica della soglia dell'archivio dati

In questa sezione vengono fornite informazioni sulle posizioni del registro di soglia, il nome della chiave di soglia e i valori predefiniti, quando viene visualizzato un messaggio della soglia di errore o avviso e come modificare la soglia dell'archivio dati.

Un archivio dati dispone di una configurazione della soglia di capacità dello spazio che consente di monitorare le informazioni sull'utilizzo dello spazio libero della destinazione dell'archivio dati. In un archivio dati di deduplicazione, la soglia controlla la memoria allocata alla destinazione hash e lo spazio su disco allocato alla cartella di destinazione del backup, alla destinazione dell'indice e alla destinazione dati. Per un archivio dati di non deduplicazione, la soglia esegue il monitoraggio dello spazio di archiviazione soltanto della cartella di destinazione del backup. I cinque elementi per il monitoraggio delle soglie presentano due tipi di valori:

- Soglia di errore
- Soglia di avviso

Il valore soglia viene salvato nel registro di sistema. È possibile modificare manualmente il valore predefinito.

Percorsi del registro delle soglie

1. Cartella Archivio dati: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\CommStore]
2. Destinazione dati di deduplicazione: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\DataRole]
3. Destinazione hash e memoria di deduplicazione: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\HashRole]

   Nota: il ruolo hash controlla l'utilizzo della memoria e del disco. Path rappresenta l'utilizzo del disco e Mem rappresenta la memoria.
4. Destinazione indice di deduplicazione: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\IndexRole]

I nomi di chiave della soglia e i valori predefiniti

Tipo di percorso	Tipo di soglia	Nome della chiave di registro	Valore predefinito	Valore predefinito (Versioni precedenti a v6.5 Aggiornamento 1)
Cartella archivio dati	Avviso	Soglia percorso avviso	0.05	0.03

	Error	Soglia percorso errore	2048	100
Percorso indice di deduplicazione	Avviso	Soglia percorso avviso	0.05	0.03
	Error	Soglia percorso errore	2048	100
Percorso hash di deduplicazione	Avviso	Soglia percorso avviso	0.05	0.03
	Error	Soglia percorso errore	2048	100
Percorso ruolo dati di deduplicazione	Avviso	Soglia percorso avviso	0.05	0.03
	Error	Soglia percorso errore	2048	100
Memoria	Avviso	WarnMemThreshold	0.05	0.03
	Error	ErrorMemThreshold	30	10

- Un valore inferiore a 1 indica la percentuale di spazio libero, ad esempio 0,05 significa 5%. Se lo spazio disponibile è inferiore al 5% dello spazio totale, viene raggiunta la soglia di avviso.
- Un valore superiore o uguale a 1 indica la dimensione dello spazio libero effettivo e l'unità è MB. Ad esempio, predefinito 2048, significa 2048 MB. Se lo spazio disponibile è inferiore a 2048 MB, viene raggiunta la soglia di errore.

Il valore soglia predefinito serve per migliorare le prestazioni dell'archivio dati. È possibile modificare i valori della soglia. Si consiglia di non modificare questi valori, a meno che non sia necessario spazio aggiuntivo.

Per modificare la soglia, attenersi alla procedura seguente:

1. Accedere alla posizione del registro di sistema corrispondente.
2. Modificare manualmente il valore predefinito di soglia.

Modifica soltanto della destinazione hash

Quando viene modificato un archivio dati di deduplicazione, sarà possibile modificare soltanto la destinazione del percorso hash in una cartella vuota. Arcserve UDP rigenera il percorso hash per il nuovo archivio dati. Questo processo è utile quando lo spazio della cartella hash è in esaurimento e tutti i processi vengono annullati. È possibile modificare l'archivio dati e indicare una nuova cartella di destinazione hash.

Procedura per cambiare le modalità di destinazione hash

Quando si crea un archivio dati di deduplicazione, specificare se la destinazione hash si trova sull'unità SSD (modalità SSD) o sull'unità di disco rigido (modalità RAM). Se è stato configurato il disco rigido come destinazione hash, occorre ulteriore memoria per elaborare le chiavi hash. Di conseguenza, quando le dimensioni del backup aumentano, è possibile che si utilizzi tutta la memoria. In tal caso, è possibile aggiungere un'unità SSD per il backup di altri dati. Allo stesso modo, se è stato configurata un'unità SSD come destinazione hash, occorre meno memoria per elaborare le chiavi hash. Tuttavia, se è in corso il passaggio a un computer con più memoria, si può attivare la modalità RAM per un'elaborazione hash più veloce.

Per cambiare la destinazione hash da RAM a SSD o viceversa, Arcserve UDP consente di modificare un archivio dati esistente e di cambiare la modalità a seconda delle proprie esigenze.

È possibile modificare un archivio dati esistente anche quando viene eseguito, anche se si riavvia una volta salvate le modifiche.

Cambio dalla modalità RAM alla modalità SSD

Quando si cambia dalla modalità RAM alla modalità SSD, occorre meno memoria. Pertanto, Arcserve UDP riduce automaticamente il valore minimo per Allocazione memoria hash. Tuttavia, è possibile modificare manualmente l'allocazione di memoria hash. In questo caso, modificare le cartelle di destinazione hash nell'unità SSD. Quando si modifica la destinazione hash, Arcserve UDP copia automaticamente i file hash nella nuova posizione sull'unità SSD.

Cambio dalla modalità SSD alla modalità RAM

Quando si cambia dalla modalità SSD alla modalità RAM, le dimensioni della RAM devono essere sufficienti per ospitare il database hash corrente. Ad esempio, prima della modifica, l'archivio dati ha creato 30 GB di file hash sull'unità SSD. Dopo la modifica, è necessario allocare almeno 30 GB di memoria per i file hash. Se la RAM non è sufficiente, il cambio di modalità non riesce. In questo caso, Arcserve UDP aumenta automaticamente i due parametri seguenti:

- Valore minimo di allocazione memoria hash
- Allocazione memoria hash

In questo modo si garantisce l'avvio dell'archivio dati dopo la modifica.

In questo caso, modificare le cartelle di destinazione hash nell'unità di disco rigido. Quando si modifica la destinazione hash, Arcserve UDP copia automaticamente i file hash nella nuova posizione sull'unità di disco rigido.

Avvio di un archivio dati

Se un archivio dati in esecuzione è stato interrotto per qualsiasi controllo di mantenimento di routine, è possibile riavviarlo al completamento del controllo di mantenimento. Al riavvio dell'archivio dati, i processi in sospeso verranno ripresi dal punto in cui erano stati interrotti.

Nota: Per avviare un archivio dati di deduplicazione, a seconda delle dimensioni hash, i dati hash richiederanno del tempo per il caricamento dal disco rigido alla memoria. Nel riquadro destro, il progresso dell'archivio dati viene mostrato in percentuale.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni:** La pagina **Recovery Point Server** mostra l'elenco di Recovery Point Server disponibili.
3. Espandere un Recovery Point Server.

   È possibile visualizzare l'elenco di archivi dati associati al Recovery Point Server.
4. Eseguire una delle seguenti operazioni:
   - Fare clic con il tasto destro del mouse sul nome dell'archivio dati.
   - Selezionare l'archivio dati e dal riquadro centrale fare clic sul menu a discesa **Azioni**.

   Viene visualizzato un elenco di opzioni.
5. Fare clic su **Avvia**.

   Il riquadro destro mostra l'informazione dell'avvio dell'archivio dati. L'icona di stato dell'archivio dati selezionato da **Interrotto** a **In esecuzione**.

Interruzione di un archivio dati

Se non si desidera che un archivio dati venga eseguito, utilizzare l'opzione Arresta. Interrompendo l'archivio dati si assicura che non vi venga eseguito alcun processo.

Note:

- Se si interrompe un archivio dati, tutti i processi in esecuzione su tale archivio dati, inclusi i processi in coda, vengono annullati.
- Se un archivio dati viene interrotto mentre è in corso un processo di replica, quando l'archivio dati verrà riavviato il processo di replica verrà ripreso dalla stessa posizione in cui era stato interrotto l'archivio dati.
- Se l'archivio dati viene interrotto mentre è in corso un processo di replica (ad esempio, Processo 10) e allo stesso tempo altri due processi di backup vengono completati (ad esempio, Processo 11 e 12), al riavvio dell'archivio dati i processi di replica vengono completati in sequenza (Processo 10, 11 e 12 rispettivamente).

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni:** La pagina **Recovery Point Server** mostra l'elenco di Recovery Point Server disponibili.
3. Espandere un Recovery Point Server.

   È possibile visualizzare l'elenco di archivi dati associati al Recovery Point Server.
4. Eseguire una delle seguenti operazioni:
   - Fare clic con il tasto destro del mouse sul nome dell'archivio dati.
   - Selezionare l'archivio dati e dal riquadro centrale fare clic sul menu a discesa **Azioni**.

   Viene visualizzato un elenco di opzioni.
5. Fare clic su **Arresta**.

   Viene visualizzata la finestra di dialogo **Conferma**.
6. Selezionare **Sì** per arrestare l'esecuzione.

   Nel riquadro destro viene visualizzato un messaggio di conferma dell'arresto dell'archivio dati.

L'archivio dati viene arrestato e l'icona di stato dell'archivio dati selezionato passa da **In esecuzione** a **Interrotto**.

Eliminazione di un archivio dati della Console

Se non si desidera più utilizzare un archivio dati, è possibile cancellarlo. Una volta cancellato, l'archivio dati viene rimosso dalla Console. Tuttavia, l'archivio dati cancellato viene conservato nel Recovery Point Server.

Note:

- È possibile importare l'archivio dati eliminato, se necessario.
- Per eliminare un archivio dati associato ai piani, è necessario eliminare il piano associato all'archivio dati.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni:** La pagina **Recovery Point Server** mostra l'elenco di Recovery Point Server disponibili.
3. Espandere un Recovery Point Server.

   È possibile visualizzare l'elenco di archivi dati associati al Recovery Point Server.
4. Eseguire una delle seguenti operazioni:
   - Fare clic con il tasto destro del mouse sul nome dell'archivio dati.
   - Selezionare l'archivio dati e dal riquadro centrale fare clic sul menu a discesa **Azioni**.

   Viene visualizzato un elenco di opzioni.
5. Fare clic su **Elimina**.

   Viene visualizzata la finestra di dialogo **Conferma**.

   Nota: Se l'archivio dati è associato a un piano, viene visualizzata la finestra di dialogo **Avviso** al posto di quella di conferma.
6. Fare clic su **Sì**.

   L'archivio dati è stato rimosso.

Eliminazione dei dati del nodo dall'archivio dati

L'amministratore di archiviazione può eliminare i dati del nodo sottoposto a backup dall'archivio dati per creare spazio libero e gestire in modo efficace lo spazio di archiviazione. Arcserve UDP consente di selezionare ed eliminare i dati del nodo nell'archivio dati. È possibile selezionare più nodi nell'archivio dati. Si può eliminare qualsiasi tipo di dati del nodo, compresi i dati crittografati e deduplicati. L'archivio dati deve essere in esecuzione quando si avvia il processo, il quale è denominato Processo di eliminazione.

Nota: è possibile eseguire l'eliminazione soltanto quando il nodo non esegue alcun processo (ad esempio, il processo Backup / Ripristino / Unione).

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Fare clic sull'archivio dati che contiene i dati del nodo che si desiderano eliminare.
3. Viene visualizzata la pagina di **riepilogo dei punti di ripristino**.
4. Selezionare il nodo che si desidera eliminare.

   Avviso! Selezionare soltanto, non fare clic sul nome del nodo. Facendo clic sul nome del nodo l'utente viene reindirizzato a un'altra pagina da cui non sarà possibile eseguire l'azione di eliminazione.
5. Fare clic su **Azioni**, **Elimina**.

   Nota: se si utilizza l'archivio dati di deduplicazione, è possibile che lo spazio su disco non venga rilasciato immediatamente dopo l'eliminazione dei punti di ripristino di un nodo. Il ritardo si verifica a causa dell'archivio dati di deduplicazione:

   - Il processo di eliminazione e recupero del backend è programmato in base al tempo di inattività dell'archivio dati.
   - Una parte dei blocchi di dati dei punti di ripristino eliminati per il nodo potrà comunque essere utilizzata dai punti di ripristino di altri nodi.

     Il volume di recupero dello spazio su disco dipende dalla percentuale di deduplicazione del nodo che si desidera eliminare.
6. Confermare l'eliminazione dei dati del nodo.

   Il processo di eliminazione viene avviato e i dati del nodo vengono eliminati dall'origine dati. È possibile visualizzare lo stato del processo di eliminazione da **Eventi recenti** e dai registri.

Monitoraggio della capacità di spazio disponibile per l'archivio dati

Gli archivi dati ARCserve UDP vengono creati su volume RPS o dischi condivisi remoti. Il meccanismo di monitoraggio dello spazio disponibile per l'archivio dati consente di monitorare l'utilizzo della cartella di destinazione quando la destinazione è quasi piena. Lo spazio libero disponibile nella cartella di destinazione non è sufficiente per l'archivio di dati in esecuzione. Se l'archivio dati ha abilitato la configurazione avvisi di posta elettronica può essere inviato un avviso di posta elettronica e il registro attività fornisce l'output. Nel frattempo, gli archivi di dati in esecuzione vengono modificati per ripristinare solo lo stato. Di conseguenza, ai processi di nuovo backup/replica viene impedita l'esecuzione dei nuovi dati di backup.

Il monitoraggio include le seguenti opzioni:

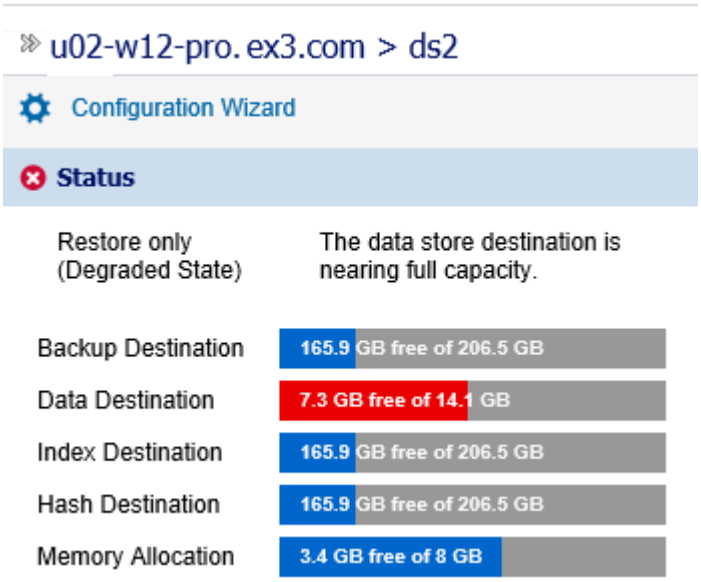
- Modifica della soglia dell'archivio dati
- Utilizzo della soglia di errore
- Utilizzo della soglia avviso
- Attivazione dell'avviso tramite posta elettronica e informazioni sul formato di posta elettronica

Utilizzo della soglia di errore

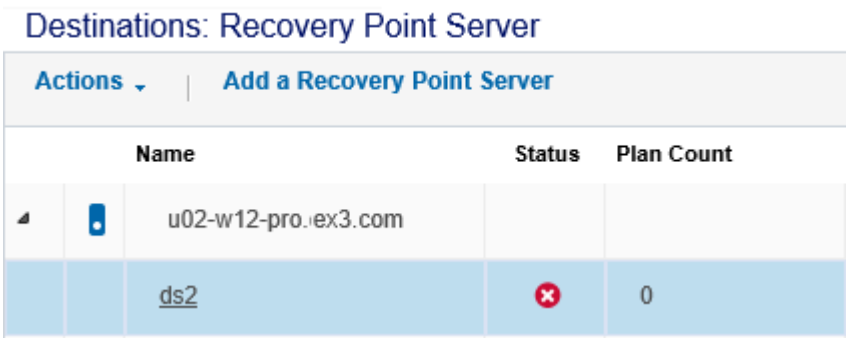
La soglia di errore indica l'assenza di spazio libero disponibile per l'archivio dati in esecuzione. Inoltre, alcuni componenti del kernel non funzionano correttamente. In questo caso, l'archivio dati viene modificato per ripristinare automaticamente solo lo stato se l'archivio dati non è stato arrestato manualmente.

Quando lo spazio libero disponibile per l'archivio dati raggiunge la soglia di avviso:

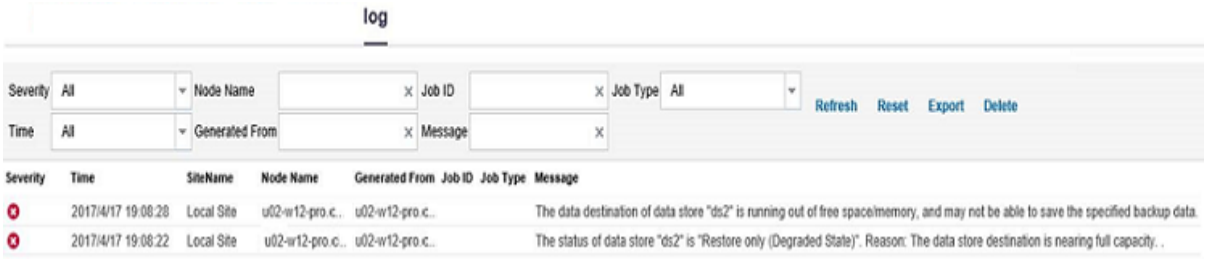
- Lo stato dell'archivio dati viene modificato automaticamente in “Ripristina solo (Danneggiato)”. Nel frattempo, non è possibile attivare alcun nuovo processo di backup/replica nell'archivio dati. Qualsiasi altro tipo di processo che non genera nuovi dati può essere ancora avviato. Ad esempio, processi di ripristino e processi di unione.
- La barra spaziatrice dell'archivio dati è contrassegnata con il colore rosso.



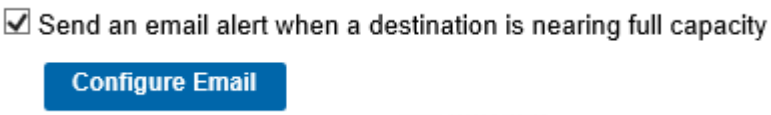
- Lo stato dell'archivio dati è contrassegnato con un'icona rossa.



- Vengono visualizzati i registri attività per informare che la cartella di destinazione archivio dati ha esaurito lo spazio disponibile, che potrebbe non essere possibile salvare nuovi dati di backup e che si rischia di raggiungere il livello di errore.



- Se l'archivio dati è configurato per inviare avvisi tramite posta elettronica quando la cartella di destinazione è quasi piena, RPS invia gli avvisi di posta elettronica ai destinatari.

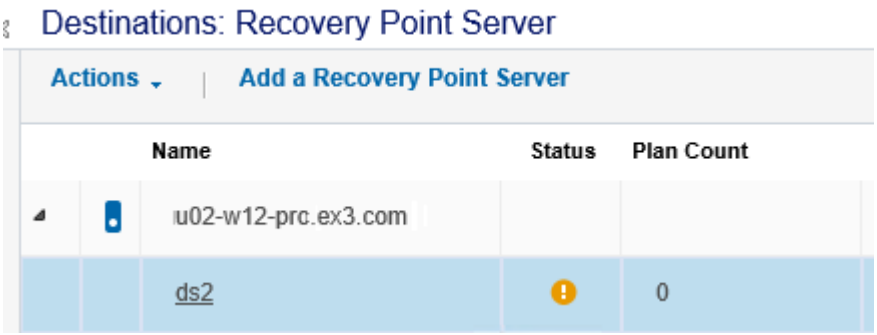


Utilizzo della soglia avviso

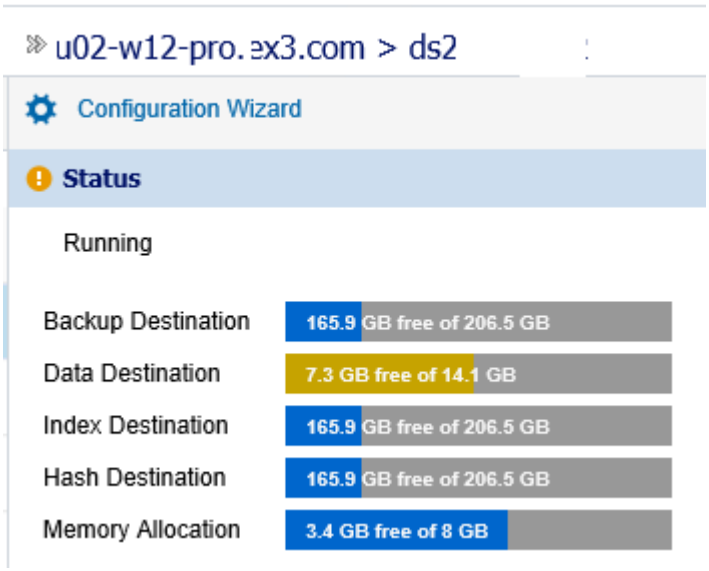
La soglia avviso indica che nella destinazione è rimasto dello spazio libero. Tuttavia, lo spazio potrebbe esaurirsi in tempi brevi se i nuovi processi di backup/replica stanno ancora lavorando.

Quando lo spazio di archiviazione dati libero raggiunge la soglia di avviso:

- Lo stato dell'archivio dati non risulta rallentato e mantiene ancora lo stato originale. Ad esempio, lo stato "esecuzione"...
- La pianificazione del processo non ne è interessata.
- Lo stato dell'archivio dati è contrassegnato con un punto esclamativo giallo.



- La barra spaziatrice dell'archivio dati è contrassegnata con il colore giallo.



- Viene visualizzato un registro attività per informare che la cartella di destinazione dell'archivio dati ha raggiunto la capacità massima e quindi il livello di avviso.



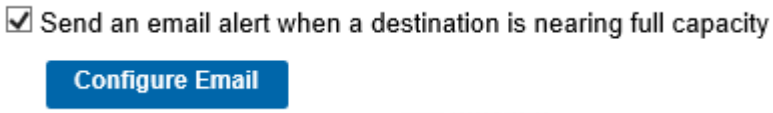
- Se l'archivio dati è configurato per inviare avvisi tramite posta elettronica quando la cartella di destinazione è quasi piena, RPS invia gli avvisi di posta elettronica ai destinatari.

Attivazione dell'avviso tramite posta elettronica e informazioni sul formato di posta elettronica

Quando la destinazione dell'archivio dati è quasi piena o lo spazio libero della cartella di destinazione raggiunge la soglia di avviso o di errore, viene inviato un avviso di posta elettronica ai destinatari speciali per informarli della situazione. Per ricevere l'avviso di posta elettronica è necessario configurare le impostazioni di posta elettronica e attivare l'opzione che consente di ricevere avvisi di posta elettronica.

Per attivare la configurazione, attenersi alla seguente procedura:

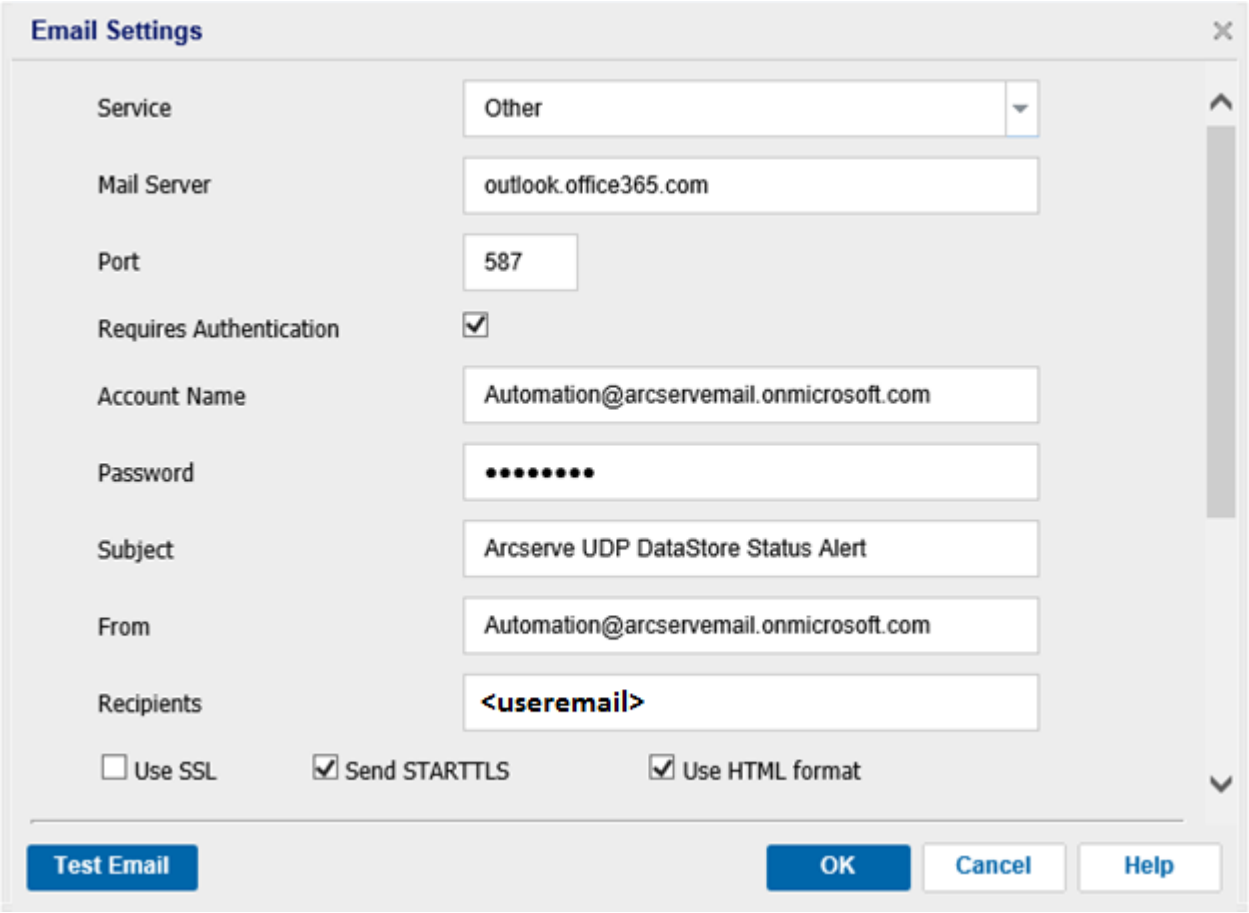
1. Selezionare la casella di controllo **Invia un avviso di posta elettronica quando una destinazione sta per raggiungere la capacità massima** durante l'aggiunta/modifica/importazione dell'archivio dati.

   Viene visualizzato il pulsante Configurazione del messaggio di posta elettronica.

2. Fare clic su **Configurazione del messaggio di posta elettronica**.

   Viene visualizzata la finestra di dialogo Impostazioni di posta elettronica.



3. Immettere i dettagli in Impostazioni di posta elettronica e fare clic su **OK**.

   La posta elettronica è configurata per ricevere tutti gli avvisi per l'archivio dati.

   Nota: Il **messaggio di posta elettronica di verifica** controlla se l'ID di posta elettronica dei destinatari riceve i messaggi di posta elettronica. Si consiglia di fare clic e procedere con la verifica prima di chiudere questa finestra di dialogo.

L'avviso di posta elettronica viene inviato ai destinatari configurati quando:

- La capacità del percorso dell'archivio dati viene modificata da integra in intervallo di avviso (quando raggiunge il valore soglia di avviso).
- La capacità del percorso dell'archivio dati viene modificata dall'intervallo di avviso all'intervallo di errore (quando raggiunge il valore soglia di errore).
- La cartella di destinazione dell'archivio di dati libera spazio (ad esempio, dopo un processo di unione dell'archivio dati, aumentando lo spazio di destinazione e così via) e fa tornare la soglia di avviso/errore a un intervallo integro.

Formato dell'avviso ricevuto tramite posta elettronica

Arcserve UDP Data Store Capacity Error Alert

Arcserve UDP Recovery Point Server	u02-w12-pro	
Data Store Name:	ds2	
Data Store Path:	e:\ds2\c	
Level:	Error	
Backup Destination:	Total Size:	211454 MB
	Free Size:	169924 MB (80.36%)
Data Destination:	Total Size:	14399 MB
	Free Size:	7435 MB (51.64%)
Index Destination:	Total Size:	211454 MB
	Free Size:	169924 MB (80.36%)
Hash Destination:	Total Size:	211454 MB
	Free Size:	169924 MB (80.36%)
Memory Allocation:	Total Size:	8191 MB
	Free Size:	3441 MB (42.01%)
Occurrence Time:	2017/4/17 19:38:01	

To view current data store capacity, access address: https://u02-w12-pro.ex3.com

See more about data store capacity configuration, click here.

Accesso ai punti di ripristino in un archivio dati

È possibile utilizzare l'opzione **Sfoglia punti di ripristino** per visualizzare i dettagli relativi ai punti di ripristino e dei piani associati all'archivio dati. Ad esempio, è possibile visualizzare i dettagli relativi alle impostazioni dell'archivio dati e gli eventi recenti.

È inoltre possibile esplorare i punti di ripristino dalla visualizzazione Cartelle condivise.

Per eliminare un nodo dall'archivio dati, consultare la sezione Eliminazione dei dati del nodo dall'archivio dati.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni:** La pagina **Recovery Point Server** mostra l'elenco di Recovery Point Server disponibili.
3. Espandere un Recovery Point Server.

   È possibile visualizzare l'elenco di archivi dati associati al Recovery Point Server.
4. Eseguire una delle seguenti operazioni:
   - Fare clic con il tasto destro del mouse sul nome dell'archivio dati.
   - Selezionare l'archivio dati e dal riquadro centrale fare clic sul menu a discesa **Azioni**.

   Viene visualizzato un elenco di opzioni.

   Nota: È inoltre possibile fare clic sul nome di un archivio dati per accedere all'archivio dati corrispondente.
5. Fare clic su **Sfoglia punti di ripristino** dalle opzioni visualizzate in seguito alla selezione di un archivio dati.

   La pagina dell'archivio dati selezionato conterrà le informazioni di riepilogo relative ai **Punti di ripristino**. Ad esempio, nella pagina vengono visualizzati i dettagli relativi a **Impostazioni archivio dati** e **Eventi recenti**.
6. Per aggiornare le informazioni relative al piano o all'archivio dati, selezionare il piano o l'archivio dati corrispondente, quindi fare clic su **Azioni**, **Aggiorna**.
7. Per eseguire il ripristino, selezionare il nodo Agente, quindi fare clic su **Azioni**, **Ripristino**.

La finestra di dialogo **Ripristino** consente di selezionare le opzioni di ripristino che si desidera eseguire per l'archivio dati.

Supporto FQDN per un archivio dati

Durante la creazione di un archivio dati in un disco locale, Arcserve UDP crea una cartella condivisa per l'archivio dati, per consentire ai processi in esecuzione su altri server di accedere ai dati.

In Arcserve UDP Versione 5.0, la cartella era condivisa con il nome host (ad esempio, <hostname>\sharename). Di conseguenza, se il server remoto poteva accedere al server RPS con l'FQDN (nome completo di dominio), non poteva accedervi con il nome host, causando la mancata riuscita dei processi.

Adesso, la cartella dell'archivio dati può essere condivisa con l'FQDN o con l'indirizzo IP. Ciò consente al server remoto di accedere all'archivio dati.

A tale scopo, aggiornare il Recovery Point Server nella console in base all'FQDN o all'indirizzo IP e creare un nuovo archivio dati.

Nota: Per un database esistente, interrompere l'archivio dati e importarlo nuovamente. È possibile sovrascrivere l'archivio dati invece di eliminarlo. Quindi, ripetere la distribuzione dei piani che utilizzano l'archivio dati.

Esecuzione manuale o su richiesta di un processo di unione

In qualità di amministratore di archiviazione, è possibile eseguire un processo di unione su richiesta e specificare il numero di punti di ripristino da conservare. I valori possono essere diversi dalle impostazioni del piano. Il processo di unione consente di eliminare le sessioni di backup selezionate da un archivio dati per liberare spazio e gestire in modo efficace lo spazio di archiviazione. È possibile selezionare più nodi ed eseguire il processo di unione on-demand.

Nota: Quando è configurata un'attività di replica e si esegue un processo di unione su richiesta dall'archivio dati di origine, il processo non verifica se le sessioni sono state già replicate. Di conseguenza, le sessioni unite non possono essere replicate nell'archivio dati di destinazione e si andranno a replicare ulteriori dati. Ad esempio, si supponga di avere cinque sessioni: s1, s2, s3, s4 ed s5. Le sessioni s1 e s2 sono state replicate. A questo punto, si esegue un processo di unione su richiesta sul lato di origine e si conservano due sessioni, s4 ed s5. s4 è una sessione completa. Pertanto, all'avvio del successivo processo di replica, si dovrà replicare una sessione completa.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.
3. Nel riquadro centrale, fare clic sull'archivio dati che contiene i dati del nodo che si desidera unire.

   Viene visualizzata la pagina con il **riepilogo dei punti di ripristino**.
4. Selezionare il nodo che si desidera unire.
5. Fare clic su **Azioni**, **Unisci ora**.

   Nota: Per unire più nodi dall'archivio dati, premere il tasto Ctrl o Maiusc e selezionare i nodi, quindi fare clic su **Azione**, **Unisci ora**.

   Viene visualizzata la finestra di dialogo **Esegui unione ora**.
6. Specificare il numero di punti di ripristino che si desiderano conservare, quindi fare clic su **OK**.

   Il processo di unione su richiesta viene avviato e i dati del nodo vengono eliminati dall'origine dati. È possibile visualizzare lo stato del processo di unione da Eventi recenti e dai registri.

Modifica del limite di nodi attivi simultanei per il backup manuale

Per inviare simultaneamente i backup manuali per più nodi non controllati dall'opzione *Limite nodi attivi simultaneamente*, aggiungere una chiave di registro al Recovery Point Server. Limiti per i nodi attivi simultanei sono configurati nell'archivio dati dell'interfaccia utente.

Effettuare le operazioni seguenti:

1. Aprire l'editor del registro di sistema. Per aprirlo, è possibile fare clic su **Start**, digitare *regedit* nel campo Cerca programmi e file e premere **Invio**.

   Nota: Potrebbe essere necessario fornire le credenziali di amministratore per accedere all'editor del Registro di sistema di Windows.

2. Individuare e fare clic sulla chiave di registro seguente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

3. Dal menu Modifica, fare clic su **Nuovo**, quindi sul **valore DWORD (32 bit)**.

   È possibile visualizzare l'elenco di archivi dati associati al Recovery Point Server.

4. Specificare ManualJobsIgnoreConcurrentJobLimit come nome della nuova voce, quindi premere **Invio**.

5. Fare clic con il tasto destro del mouse su ManualJobsIgnoreConcurrentJobLimit, quindi selezionare **Modifica**.

6. Specificare 1 nel campo **Dati valore** e fare clic su **OK**.

7. Uscire dall'editor del Registro di sistema.

   Nota: dopo essere stata abilitata con 1, la chiave di registro ManualJobsIgnoreConcurrentJobLimit funzionerà per tutti gli archivi dati sul server RPS.

Risoluzione dei problemi: utilizzo di un archivio dati quando una o più cartelle sono piene

Sintomo:

Come continuare a utilizzare l'archivio dati quando una delle seguenti cartelle è piena:

- Destinazione di backup dell'archivio dati
- Indice di deduplicazione
- Hash
- Dati

Soluzione:

Modificare il percorso di destinazione del backup

1. Arrestare l'archivio dati.
2. Modificare i piani che utilizzano l'archivio dati. Nella scheda Destinazione, impostare la destinazione su un altro archivio dati o su una cartella condivisa, selezionare la casella di controllo **Sospendi questo piano**, quindi **salvare** il piano.
3. Eliminare l'archivio dati.
4. Copiare la cartella di destinazione del backup corrispondente in un volume di grandi dimensioni. Verificare che le dimensioni e il numero di file delle cartelle di origine e destinazione coincidano.

   Nota: accertarsi di arrestare l'archivio dati prima di copiare la cartella. Durante il processo di copia, assicurarsi che tutti i file vengano copiati nelle cartelle di destinazione, senza ignorare i file.

   Avviso: se si ignorano alcuni file, i dati potrebbero venire danneggiati. Se il numero di file o la dimensione della cartella di origine non corrisponde a quella della cartella di destinazione, non proseguire con il passaggio successivo.
5. Importare l'archivio dati. Specificare il nuovo percorso dei dati o dell'indice durante l'importazione dell'archivio dati.
6. Dalla Console UDP, accedere a Risorse, Destinazioni, Recovery Point Server.
7. Selezionare l'archivio dati nel server RPS.
8. Dal riquadro di destra, in Impostazioni verificare che il percorso di destinazione dei dati o dell'indice punti alla posizione corretta.

Importante: durante l'esecuzione delle operazioni precedenti, NON avviare l'archivio dati fino al termine del Passaggio 8.

9. Avviare l'archivio dati
10. Modificare i piani sospesi, quindi riconfigurarli in modo da utilizzare l'archivio dati importato (in base alle esigenze). Deselezionare l'opzione **Sospendi questo piano** e **salvare** il piano.

    Nota: dopo l'importazione dell'archivio dati per il collegamento alla nuova posizione e l'avvio dell'archivio dati, **NON tornare** al percorso originale. Tale operazione potrebbe causare il danneggiamento dei dati.

Modificare il percorso di destinazione dei dati o dell'indice

1. Arrestare l'archivio dati.
2. Copiare la cartella corrispondente (Dati/Indice a seconda delle esigenze) in un volume di grandi dimensioni. Verificare che le dimensioni e il numero di file delle cartelle di origine e destinazione coincidano.

   Nota: accertarsi di arrestare l'archivio dati prima di copiare la cartella. Durante il processo di copia, assicurarsi che tutti i file vengano copiati nelle cartelle di destinazione, senza ignorare i file.

   Avviso: se si ignorano alcuni file, i dati potrebbero venire danneggiati. Se il numero di file o la dimensione della cartella di origine non corrisponde a quella della cartella di destinazione, non proseguire con il passaggio successivo.
3. Importare l'archivio dati. Specificare il nuovo percorso dei dati o dell'indice durante l'importazione dell'archivio dati.
4. Dalla Console UDP, accedere a Risorse, Destinazioni, Recovery Point Server.
5. Selezionare l'archivio dati nel server RPS.
6. Dal riquadro di destra, in Impostazioni verificare che il percorso di destinazione dei dati o dell'indice punti alla posizione corretta.

   Importante: durante l'esecuzione delle operazioni precedenti, NON avviare l'archivio dati fino al termine del Passaggio 6.
7. Avviare l'archivio dati

   Nota: dopo l'importazione dell'archivio dati per il collegamento alla nuova posizione e l'avvio dell'archivio dati, **NON tornare** al percorso originale. Tale operazione potrebbe causare il danneggiamento dei dati.

Modificare il percorso di destinazione hash

Per ulteriori informazioni, consultare la sezione Modificare il percorso hash.

Gestione di un Recovery Point Server

Arcserve UDP consente di eseguire varie operazioni sul Recovery Point Server esistente come aggiornamento, eliminazione, importazione e aggiornamento a versioni successive.

Il Recovery Point Server viene visualizzato sotto **Nome** nella pagina **Destinazioni: Recovery Point Server.** Fare clic sulla scheda **Azioni** o sul nome del Recovery Point Server nella pagina **Destinazioni: Recovery Point Server** per ricevere tutte le opzioni per la gestione del Recovery Point Server.

Come procedere?

- Revisione dei prerequisiti
- Aggiornamento di un Recovery Point Server
- Eliminazione di un Recovery Point Server dalla Console
- Importazione di un archivio dati
- Installazione/Aggiornamento del Recovery Point Server

Verifica dei prerequisiti

Per gestire un server del punto di ripristino, completare i prerequisiti seguenti:

- Accedere alla console.
- Aggiungere un punto di ripristino.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Aggiornamento di un Recovery Point Server

Quando le credenziali o il protocollo vengono modificate per il Recovery Point Server, sarà necessario aggiornare il Recovery Point Server. In caso contrario, il Recovery Point Server non funzionerà correttamente.

Nota: Se un nodo funge da Recovery Point Server e da agente e vengono modificate le credenziali o il protocollo per tale nodo, eseguire l'aggiornamento del nodo dalla pagina **Destinazioni: Recovery Point Server**. Il piano verrà distribuito automaticamente sull'agente dopo l'aggiornamento del Recovery Point Server. Se si aggiorna il nodo dalla pagina **Nodi: Tutti i nodi**, i piani relativi a tali nodi non vengono distribuiti correttamente. Per effettuare la distribuzione del piano, aggiornare nuovamente il nodo dalla pagina **Destinazioni: Recovery Point Server**.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: Recovery Point Server**.
3. Eseguire una delle seguenti operazioni:
   - Fare clic su un Recovery Point Server.
   - Selezionare un Recovery Point Server e dal menu centrale fare clic sul menu a discesa **Azioni**.
4. Fare clic su **Aggiorna**.

   Viene visualizzata la finestra di dialogo **Aggiorna nodo**.
5. Modificare i dettagli come desiderato e fare clic su **OK**.

   Il Recovery Point Server è stato aggiornato.

Eliminazione di un Recovery Point Server dalla Console

Per rimuovere un Recovery Point Server dalla Console, utilizzare l'opzione **Elimina.**

Nota: Quando si rimuove un Recovery Point Server, gli archivi dati associati non vengono eliminati. Un Recovery Point Server che viene utilizzato in un piano qualsiasi non può essere eliminato.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: Recovery Point Server**.
3. Eseguire una delle seguenti operazioni:
   - Fare clic su un Recovery Point Server.
   - Selezionare un Recovery Point Server e dal menu centrale fare clic sul menu a discesa **Azioni**.
4. Fare clic su **Elimina**.

   Viene visualizzata la finestra di dialogo **Conferma**.
5. Fare clic su **Sì**.

   Il Recovery Point Server è stato eliminato.

Importazione di un archivio dati

La funzionalità **Importa archivio dati** consente di aggiungere un archivio dati al Recovery Point Server. È possibile importare in un Recovery Point Server qualsiasi archivio dati esistente. Gli archivi dati eliminati in precedenza da un Recovery Point Server sono disponibili per l'importazione.

Nota: se i dati hash dell'archivio dati di deduplicazione vengono ignorati o sono corrotti, sarà comunque possibile importare l'archivio dati. Fornire una cartella vuota come cartella hash. L'archivio dati, quindi, viene avviato soltanto nello **stato di ripristino** e viene visualizzato un messaggio di errore indicante che il ruolo hash non è funzionante per la cartella hash vuota. L'utilizzo di questo metodo consente di utilizzare l'archivio dati soltanto per i processi di ripristino. Se si desidera eseguire il processo di backup, rigenerare l'hash.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Viene visualizzata la pagina **Destinazioni: Recovery Point Server**.
3. Eseguire una delle seguenti operazioni:
   - Fare clic su un Recovery Point Server.
   - Selezionare un Recovery Point Server e dal menu centrale fare clic sul menu a discesa **Azioni**.
   - Per ricevere avvisi di posta elettronica, selezionare la casella di controllo di *Invia un avviso di posta elettronica quando una destinazione sta per raggiungere la capacità massima*.

     Nota: Se non precedentemente configurate, fare clic su **Configurazione del messaggio di posta elettronica** per fornire le impostazioni di posta elettronica.
4. Fare clic su **Importa archivio dati**.

   Viene visualizzata la pagina **Importa archivio dati**.
5. Selezionare le opzioni seguenti e fare clic su **Avanti**:
   - **Sfogliare** per selezionare la **Cartella di destinazione del backup** in cui importare l'archivio dati.
   - Immettere la **Password di crittografia**.

   Nota: Lasciarla vuota se l'archivio dati non è crittografato.

Dopo avere autenticato la **Cartella di destinazione del backup**, la pagina **Importa archivio dati** mostra i dettagli dell'archivio dati.

6. Modificare i dettagli, se necessario, quindi fare clic su **Salva**.

   Se sono state copiate cartelle della Destinazione dati, Destinazione indice e della Destinazione hash per l'archivio dati di deduplicazione, sarà necessario modificare il percorso della cartella.

   Nota: Non è possibile abilitare o disabilitare l'opzione di crittografia per un archivio dati esistente.

   L'archivio dati viene aggiunto al Recovery Point Server e visualizzato nella finestra di dialogo **Destinazioni: Recovery Point Server**.

Installazione/Aggiornamento del Recovery Point Server

Utilizzare l'opzione **Installa/Aggiorna Recovery Point Server** nei casi seguenti:

- Quando l'installazione non riesce.
- Quando si desidera eseguire l'aggiornamento del prodotto.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: Recovery Point Server**.
3. Eseguire una delle seguenti operazioni:
   - Fare clic su un Recovery Point Server.
   - Selezionare un Recovery Point Server e dal menu centrale fare clic sul menu a discesa **Azioni**.
4. Fare clic su **Installazione o aggiornamento del Recovery Point Server**.

   I dettagli relativi al percorso di installazione vengono visualizzati nella stessa pagina, sopra l'elenco del Recovery Point Server aggiunto.
5. Aggiornare i dettagli richiesti.
6. Specificare la pianificazione per l'installazione/aggiornamento, quindi fare clic su **OK**.

   L'installazione o l'aggiornamento della pianificazione si avvia. È possibile visualizzare l'avanzamento dell'installazione o dell'aggiornamento nel riquadro destro.

   Nota: È possibile annullare la distribuzione di un Recovery Point Server se è pianificata per l'esecuzione in un secondo momento. Per annullare la distribuzione di un Recovery Point Server, selezionare l'agente e fare clic su Azioni, Annulla Distribuzione agente.

Gestione dei server Arcserve Backup

È possibile gestire i server Arcserve Backup dalla console di Arcserve UDP. È inoltre possibile aggiornare e eliminare il server Arcserve Backup dalla console.

Aggiornamento del server Arcserve Backup

Quando le credenziali o la porta del servizio web Arcserve del server Arcserve Backup vengono modificate, è necessario aggiornare le stesse nella console.

Effettuare le operazioni seguenti:

1. Accedere alla console e fare clic sulla scheda **risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Server Arcserve Backup**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni:** Nel riquadro centrale viene visualizzata la pagina **Server Arcserve Backup**.
3. Selezionare un server Arcserve Backup, fare clic con il tasto destro del mouse e selezionare **Aggiorna**.

   Viene visualizzata la pagina **Aggiorna server Arcserve Backup**.
4. Aggiornare i campi obbligatori, quindi fare clic su **Salva**.

   La pagina **Aggiorna server Arcserve Backup** viene chiusa.

   Il server Arcserve Backup è stato aggiornato correttamente.

Eliminazione del server Arcserve Backup

Se non è più necessario un server Arcserve Backup, è possibile eliminare il server dalla console. Prima di eliminare un server Arcserve Backup, verificare che il server Arcserve Backup non sia incluso in un'attività in un piano. Se il server è incluso in un'attività, eliminare l'attività o modificare la destinazione di backup.

Effettuare le operazioni seguenti:

1. Accedere alla console e fare clic sulla scheda **risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Server Arcserve Backup**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni:** Nel riquadro centrale viene visualizzata la pagina **Server Arcserve Backup**.
3. Selezionare un server Arcserve Backup, fare clic con il tasto destro del mouse e selezionare **Elimina**.

   Verrà visualizzata la finestra di dialogo di conferma.
4. Fare clic su **Sì**.

   Il server Arcserve Backup viene eliminato dalla console.

Gestione di una cartella condivisa

È possibile gestire le cartelle condivise dalla console Arcserve UDP. È inoltre possibile modificare ed eliminare la cartella condivisa dalla console.

Modifica di una cartella condivisa

Arcserve UDP consente di modificare i dettagli di una cartella condivisa aggiunta. Se le informazioni relative alla cartella condivisa vengono modificate, è necessario modificare la cartella condivisa aggiunta in Arcserve UDP in modo da rendere i piani funzionanti.

Effettuare le operazioni seguenti:

1. Accedere ad Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni** e fare clic su **Cartelle condivise**.

   La pagina **Destinazioni: Cartelle condivise** mostra le cartelle condivise nel riquadro centrale.
3. Per gestire le cartelle, fare clic con il tasto destro del mouse su una delle cartelle condivise aggiunte, oppure selezionare una cartella condivisa e fare clic su **Azioni**.
4. Selezionare una delle opzioni disponibili, quindi fare clic su **Aggiorna**.

   Viene visualizzata la finestra di dialogo **Aggiorna**.
5. Modificare le informazioni e fare clic su **OK**.

   La cartella condivisa è stata aggiornata.

Eliminazione di una cartella condivisa

Arcserve UDP consente di eliminare una cartella condivisa aggiunta.

Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni** e fare clic su **Cartelle condivise**.

   La pagina **Destinazioni: Cartelle condivise** mostra le cartelle condivise nel riquadro centrale.
3. Per gestire le cartelle, fare clic con il tasto destro del mouse su una delle cartelle condivise aggiunte, oppure selezionare una cartella condivisa e fare clic su **Azioni**.
4. Selezionare una delle opzioni disponibili, quindi fare clic su **Elimina**.

   Viene visualizzata una finestra di dialogo **Conferma** oppure **Errore**.
5. Per il messaggio di conferma, fare clic su **OK** da eliminare.
6. (Facoltativo) Per il messaggio di errore, correggere l'errore e ripetere l'operazione di eliminazione.

   La cartella condivisa è stata aggiornata.

Gestione di una console remota

Dopo aver creato una console remota, potrebbe essere necessario eseguire alcune operazioni, ad esempio, modificare, eliminare o eseguire il test della connessione.

Come procedere?

- Modifica di una console remota
- Eliminazione di una console remota
- Verifica della connessione della console remota

Modifica di una console remota

Arcserve UDP consente di modificare i dettagli di una console remota aggiunta. Se le informazioni di connessione vengono modificate per la console remota, è necessario modificare l'account della console remota aggiunta in Arcserve UDP.

Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Nel riquadro a sinistra, accedere a **Destinazioni**, quindi fare clic su **Console remota**.

   La pagina **Destinazioni: Console remota** mostra la console remota aggiunta nel riquadro centrale.
3. Per gestire la console, fare clic con il tasto destro del mouse su una delle console remote aggiunte, oppure selezionare una console remota e fare clic su **Azioni**.

   Viene visualizzata la pagina **Modifica una console remota**.
4. Modificare le informazioni e fare clic su **OK**.

   La console remota è aggiornata.

Eliminazione di una console remota

Arcserve UDP consente di rimuovere una console remota, se richiesto.

Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Nel riquadro a sinistra, accedere a **Destinazioni**, quindi fare clic su **Console remota**.

   La pagina **Destinazioni: Console remota** mostra la console remota aggiunta nel riquadro centrale.
3. Per gestire la console, fare clic con il tasto destro del mouse su una delle console remote aggiunte oppure selezionare una console remota e fare clic su **Azioni**.

   Viene visualizzato un messaggio di **Conferma** o di **Errore**.

   Messaggio di conferma

   Viene visualizzato se la console remota non viene aggiunta ad alcun piano.

   Messaggio di errore

   Viene visualizzato se la console remota appartiene a un piano esistente.
4. (Facoltativo) Se viene visualizzato il messaggio di errore:
   a. Fare clic su **OK** per chiudere il messaggio di errore.
   b. Aprire il piano a cui è associata la console remota.
   c. Eliminare il piano correlato o modificare il piano per modificare la console remota nella scheda di destinazione del piano **Replica su server RPS gestito in remoto**.

   Dopo aver rimosso la console remota dal piano, tornare alla pagina Console remota e provare ad eliminare nuovamente la console remota.
5. Dal messaggio di conferma, fare clic su **Sì**.

   La console remota è stata rimossa.

Verifica della connessione della console remota

Arcserve UDP consente di verificare la connessione di una console remota aggiunta. È necessaria una connessione con esito positivo per la console remota in modo da garantire il corretto funzionamento del piano di replica. La console remota è infatti associata al piano.

La connessione alla console remota potrebbe non riuscire per diversi motivi:

- Se le informazioni aggiunte per la destinazione della console remota non sono corrette.
- Se le informazioni relative alle credenziali della console remota, alla porta, al protocollo o al proxy sono state modificate ma le stesse informazioni non sono state aggiornate nella Console Arcserve UDP.
- Se la connessione di rete viene interrotta tra la console e la console remota.
- Se il servizio di gestione di Arcserve UDP viene interrotto nella console remota.

È possibile utilizzare l'opzione di test della connessione della console remota per verificare se la connessione della console remota e la correttezza delle informazioni fornite.

Effettuare le operazioni seguenti:

1. Accedere a Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Nel riquadro a sinistra, accedere a **Destinazioni**, quindi fare clic su **Console remota**.

   La pagina **Destinazioni: Console remota** mostra la console remota aggiunta nel riquadro centrale.
3. Per gestire la console, fare clic con il tasto destro del mouse su una delle console remote aggiunte oppure selezionare una console remota e fare clic su **Azioni**.

   Vengono visualizzate più opzioni.
4. Dalle diverse opzioni visualizzate, fare clic su **Verifica connessione alla console remota**.

   Viene visualizzato un messaggio **informativo** se i dettagli della console remota sono corretti.

   Viene visualizzato un messaggio di **errore** se i dettagli della console remota non sono corretti. Fornire i dettagli corretti di connessione e riprovare.

5. (Facoltativo) Se viene visualizzato un messaggio di errore, correggere la connessione interrotta verificando uno dei seguenti motivi (oppure tutti):
   - Le informazioni relative all'account sono corrette.
   - Viene stabilita la connessione di rete.
   - Lo stato del servizio di gestione Arcserve UDP nella console remota non viene interrotto.

   La connessione delle console remota è stata verificata correttamente.

Chapter 10: Creazione di piani per la protezione dei dati

La presente sezione descrive i seguenti argomenti:

Presentazione dei piani e delle attività

Per proteggere un nodo, è necessario creare un piano con un'attività di backup. Un piano è un gruppo di attività per la gestione del backup, della replica e della creazione di nodi di standby virtuali. Un piano è composto da un'attività singola o da più attività. Le attività sono un insieme di attività per la definizione dell'origine, della destinazione, della pianificazione e dei parametri avanzati.

È possibile creare le attività seguenti:

Attività di backup

Consente di creare un'attività di backup per proteggere i nodi di computer virtuali Windows, Linux e basati su host. A seconda del tipo di nodi che si desidera proteggere, utilizzare una delle seguenti attività di backup:

Backup di Windows basato su agente

Definisce un'attività di backup per la protezione dei nodi di Windows. In un metodo di backup basato su agente, viene utilizzato un componente di agente per eseguire il backup dei dati. L'agente è installato sul nodo di origine.

Backup senza agente basato su host

Definisce un'attività di backup per la protezione dei computer virtuali basati su host in un server VMware vCenter/ESX o Microsoft Hyper-V. In un metodo di backup senza agente, non è necessario installare un componente di agente né sul server, né sul computer virtuale. Tuttavia, è necessario installare l'agente su un server proxy.

Linux basato su agente

Definisce un'attività di backup per la protezione di nodi Linux. L'agente viene installato su un server di backup di Linux e non sui nodi di origine che si desidera proteggere.

Attività di replica da un Recovery Point Server remoto

Consente di creare un'attività per ricevere dati da un Recovery Point Server remoto.

Attività di replica

Consente di creare un'attività per la replica dei dati di backup da un Recovery Point Server a un altro.

Attività di Virtual Standby

Consente di creare un'attività per la creazione di un nodo di standby virtuale.

Attività di copia file

Consente di copiare i file selezionati dal nodo di origine e archiviare i file copiati in una cartella locale o condivisa. È possibile inoltre archiviare i file in un'archiviazione cloud.

Attività di copia dei punti di ripristino

Consente di copiare i punti di ripristino in una cartella locale o condivisa oppure su cloud.

Attività di replica in un Recovery Point Server gestito da remoto

Consente di creare un'attività di replica o inviare dati in un Recovery Point Server remoto.

Attività di archiviazione file

Consente di copiare i punti di ripristino in una condivisione di rete, in un'archiviazione cloud o in un volume su un nodo protetto. Quando i punti di ripristino vengono copiati nella destinazione, i file di origine vengono eliminati.

Attività di copia su nastro

Consente di copiare i punti di ripristino su nastro con la funzionalità di ripristino granulare direttamente dal nastro.

Problemi correlati ad Assured Recovery

Consente di verificare l'accessibilità e i valori di Assured Recovery dei dati.

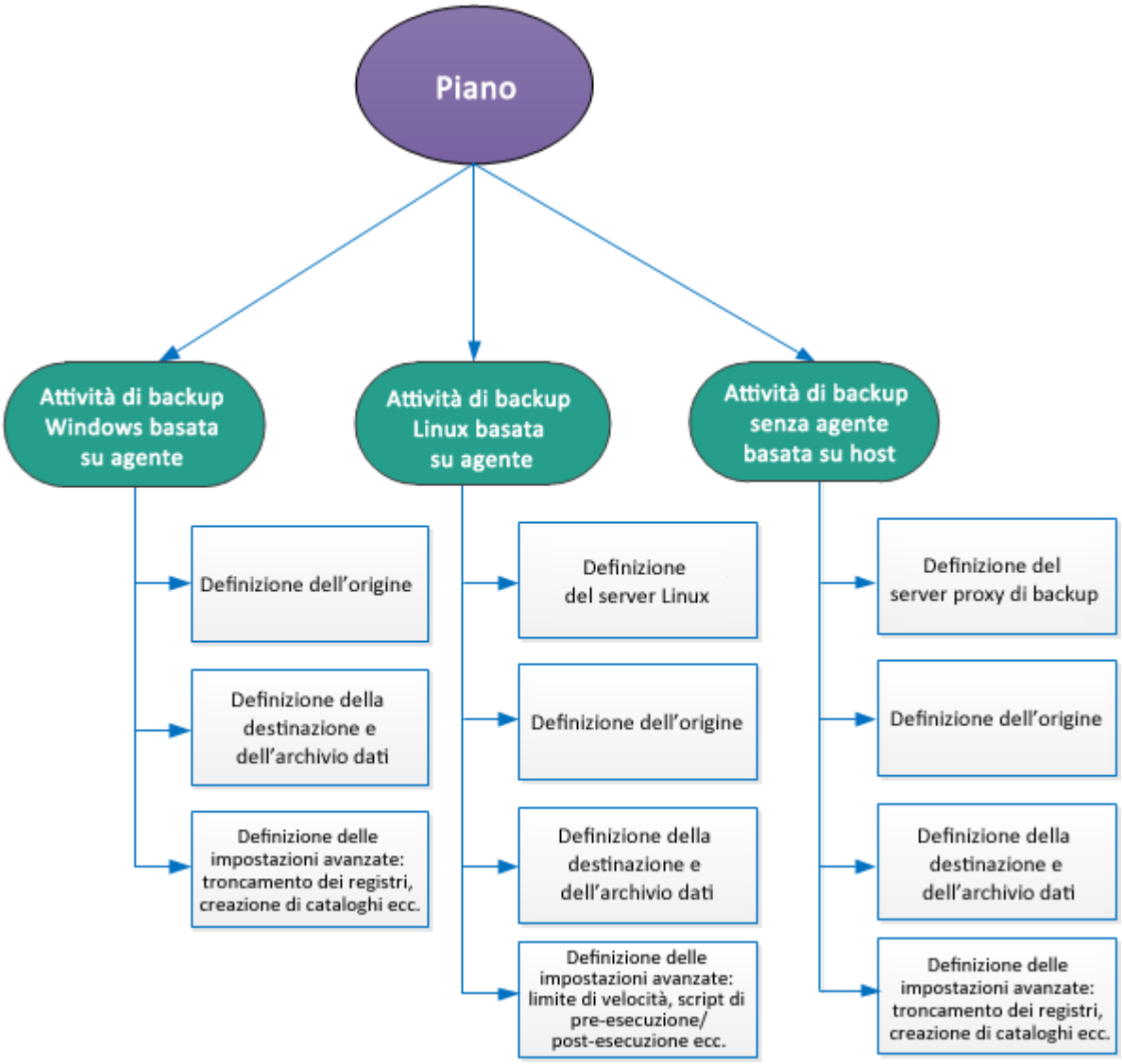
Nella seguente tabella viene riportato un elenco di attività di completamento che è possibile aggiungere dopo l'Attività 1:

Attività 1	Attività di completamento
Backup: Windows basato su Agente	■ Replica ■ Virtual Standby ■ Copia punti di ripristino ■ Copia file ■ Replica in un Recovery Point Server gestito remotamente ■ Archiviazione file ■ Copia su nastro ■ Verifica di Assured Recovery
Backup: senza Agente basato su host	■ Replica ■ Virtual Standby ■ Copia punti di ripristino ■ Replica in un Recovery Point Server gestito remotamente

	■ Copia su nastro ■ Verifica di Assured Recovery
Backup: Linux basato su agente	■ Replica ■ Replica in un Recovery Point Server gestito remotamente ■ Copia su nastro ■ Verifica di Assured Recovery
Replica di dati da un Recovery Point Server remoto	■ Virtual Standby ■ Replica ■ Verifica di Assured Recovery
Backup: Office 365 Exchange Online	■ Replica ■ Copia punti di ripristino ■ Replica in un Recovery Point Server gestito remotamente ■ Copia su nastro ■ Verifica di Assured Recovery
Backup: Office 365 OneDrive	■ Replica ■ Copia punti di ripristino ■ Replica in un Recovery Point Server gestito remotamente ■ Copia su nastro ■ Verifica di Assured Recovery
Backup: Office 365 SharePoint Online	■ Replica ■ Copia punti di ripristino ■ Replica in un Recovery Point Server gestito remotamente ■ Copia su nastro ■ Verifica di Assured Recovery
Backup: File nel percorso UNC o NFS	■ Replica ■ Copia punti di ripristino ■ Replica in un Recovery Point Server gestito remotamente ■ Copia su nastro

	■ Verifica di Assured Recovery

Nel diagramma seguente viene mostrato come le diverse attività formino un piano di backup. Nel diagramma seguente vengono mostrati anche i parametri che è possibile definire in ciascuna attività.



Creazione di un piano di backup di Windows

Per proteggere i nodi o i nodi del cluster di Windows, è necessario creare un piano. Un piano di backup per i nodi di Windows consiste in un'attività di backup. Questa attività di backup consente di specificare i nodi che si desidera proteggere, la destinazione di backup e la pianificazione dei backup. La destinazione di backup è un Recovery Point Server su cui archiviare i dati sottoposti a backup. La destinazione può essere una destinazione locale o una cartella di condivisione remota.

È possibile eseguire il backup di un database Oracle. Prima di creare un piano per eseguire il backup di un database Oracle, rivedere i prerequisiti seguenti:

- Prerequisiti per il backup di un database Oracle

Per eseguire il backup di dischi condivisi e nodi del cluster Microsoft, rivedere i prerequisiti seguenti:

- Verifica dei prerequisiti per eseguire il backup di dischi condivisi e nodi del cluster Microsoft

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di un piano di backup
3. (Facoltativo) Esecuzione di un backup manuale
4. Verifica del backup

Verifica delle considerazioni e dei prerequisiti

Verificare il completamento delle seguenti azioni preliminari:

- La versione più recente dell'agente Arcserve UDP (Windows) è installata.
- Accedere alla console.
- (Facoltativo) Creare un archivio dati per archiviare i dati di backup.
- Verifica dei prerequisiti per il database Oracle con l'agente Windows di UDP.
- Verificare i prerequisiti per eseguire il backup di dischi condivisi e nodi del cluster Microsoft.
- (Per il backup di SQL se il database è in modalità completa) Rivedere la sezione Abilitazione dei troncamenti di registro quando il database SQL è in modalità di ripristino completo.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

I seguenti prerequisiti valgono per le snapshot hardware:

- Installare un provider hardware VSS in grado di supportare la snapshot hardware sugli agenti Arcserve UDP. La configurazione tipica di un provider hardware VSS include:
  - Definizione di un server che controlla la LUN.
  - Definizione delle credenziali dell'array di dischi per accedere all'array di dischi.

  Nota: per ulteriori informazioni sulla configurazione del provider di hardware VSS, contattare il rivenditore del provider hardware.

I prerequisiti seguenti sono specifici del backup di rete:

- L'agente Windows e RPS devono essere contenuti nella stessa rete.
- Il nodo di protezione di Windows è pianificato.
- Il server RPS locale con più NIC è connesso.

Verifica dei prerequisiti per il database Oracle con l'agente Windows di UDP

Per eseguire il backup di un database Oracle con dati coerenti, verificare che la modalità ARCHIVELOG sia abilitata per archiviare i registri Redo.

Nota: il volume di dati deve includere file di dati Oracle, file di controllo, file di parametro del server e registri di ripristino in linea. I registri di ripristino archiviati devono trovarsi fisicamente in un volume separato.

Attenersi alla seguente procedura per verificare che la modalità ARCHIVELOG sia abilitata:

a. Accedere come utente Oracle con privilegi SYSDBA al server Oracle.

b. Al prompt SQL*Plus, immettere il seguente comando:

   ARCHIVE LOG LIST;

   Vengono visualizzate le impostazioni Archive log per l'istanza corrente.

c. Configurare le impostazioni seguenti:

   Database log mode: Archive Mode

   Automatic archival: Enabled

d. Avviare la modalità ARCHIVELOG.

   Nota: se non è attivata la modalità ARCHIVELOG, avviare la modalità ARCHIVELOG per eseguire il backup del database.

Completare le operazioni seguenti per avviare la modalità ARCHIVELOG:

a. Chiudere Oracle Server.

b. Eseguire le istruzioni sotto riportate in Oracle:

   CONNECT SYS/SYS_PASSWORD AS SYSDBA

   STARTUP MOUNT;

   ALTER DATABASE ARCHIVELOG;

   ALTER DATABASE OPEN;

   Per impostazione predefinita, i registri di archivio verranno scritti nell'area di ripristino flash. Se non si desidera scrivere i registri di archivio nell'area di ripristino flash, è possibile impostare il parametro LOG_ARCHIVE_DEST_n nella posizione in cui scrivere i registri di archivio.

   SQL>ALTER SYSTEM SET LOG_ARCHIVE_DEST_
   1='LOCATION=e:\app\administrator\oradata\<oracle_database_name>\arch'
   SCOPE= BOTH;

Sistema modificato.

SQL> ARCHIVE LOG LIST;

Vengono visualizzate le impostazioni Archive log per l'istanza corrente.

c. Configurare le impostazioni seguenti:

Database log mode: Archive Mode

Automatic archival: Enabled

Archive destination: E:\app\oracle\oradata\<oracle_database_name>\arch

Oldest online log sequence: 21

Current log sequence: 23

Il servizio di scrittura Oracle VSS viene avviato correttamente.

Nota: Se il servizio writer Oracle VSS non è in esecuzione, verrà avviato automaticamente dall'agente Arcserve UDP (Windows) prima dell'acquisizione della snapshot.

- L'agente Arcserve UDP (Windows) viene installato e viene programmato un piano.

  Verificare di aver selezionato i volumi che includono tutti i file di dati, il file dei parametri per il server, i file di controllo, i registri di ripristino archiviati e in linea di Oracle per il backup.

- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Se si desidera utilizzare un ripristino bare metal in caso di Disaster Recovery, verificare di aver selezionato i volumi di sistema e i volumi che includono tutti i file di installazione di Oracle.

Verifica dei prerequisiti per eseguire il backup di dischi condivisi e nodi del cluster Microsoft

Rivedere i seguenti passaggi preliminari durante l'esecuzione del backup di dischi condivisi e nodi del cluster Microsoft:

- Installare l'agente Arcserve UDP su tutti i nodi cluster.
- Aggiungere tutti gli agenti o i nodi nello stesso piano di backup.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Nota: I dischi condivisi verranno sottoposti a backup insieme al relativo agente proprietario. Se il disco condiviso viene spostato dal Nodo A al Nodo B durante il failover, per il successivo processo di backup sul Nodo B, verrà eseguito il backup del disco come completo anche se il processo sembra incrementale. Dopo un altro failover se il disco condiviso viene rispostato nel Nodo A, viene eseguito ancora il backup del disco come completo anche se il processo sembra incrementale.

Abilitazione dei troncamenti di registro quando il database SQL è in modalità di ripristino Estesa

Sintomo

Se il database è in modalità Estesa e viene eseguito un backup completo del database, non è possibile troncare il registro di troncamento SQL.

Soluzione

Per risolvere questo problema, aggiungere un valore del Registro di sistema per consentire ad Arcserve UDP di eseguire il comando BACKUP LOG per eseguire il backup del registro transazioni. Questo comando contrassegna lo spazio, già scritto nel file di database, come riutilizzabile.

Per aggiungere il valore del Registro di sistema, attenersi alla procedura seguente:

1. Aprire l'editor della tabella del Registro di sistema sul computer dell'agente utilizzando il comando seguente:

   ```
   regedit
   ```

2. Accedere alle seguenti chiavi a seconda del tipo di backup: basato su agente o senza agente:

   Per il backup basato su agente per sistemi operativi a 32 bit e a 64 bit, individuare la chiave seguente nel computer dell'agente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Se si utilizza una versione precedente a Arcserve UDP v6.5 Aggiornamento 2, per il backup senza agente accedere alla chiave seguente. Creare il valore di tabella del Registro di sistema nel computer virtuale che si desidera sottoporre a backup sul server proxy. Se la chiave della tabella del Registro di sistema non è disponibile, creare il percorso completo della chiave.

   - **Sistema operativo a 32 bit:**

     HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   - **Sistema operativo a 64 bit:**

     HKEY_LOCAL_MACHINE\SOFTWARE\WoW6432Node\Arcserve\Unified Data Protection\Engine\AFBackupDll

3. Creare i due valori seguenti per il Registro di sistema e impostare entrambi su 1:

- valore dword denominato BackupSQLLog4Purge
- valore dword denominato ForceShrinkSQLLog

  Il valore del Registro di sistema è stato aggiunto.

La soluzione è attiva alla successiva esecuzione del processo di eliminazione.

Creazione di un piano con un'attività di backup

Un piano di backup include un'attività di backup che esegue un backup del nodo fisico e archivia i dati nella destinazione specificata. Ciascuna attività consiste di parametri che definiscono l'origine, la destinazione, la pianificazione, e altri dettagli di backup.

Effettuare le operazioni seguenti:

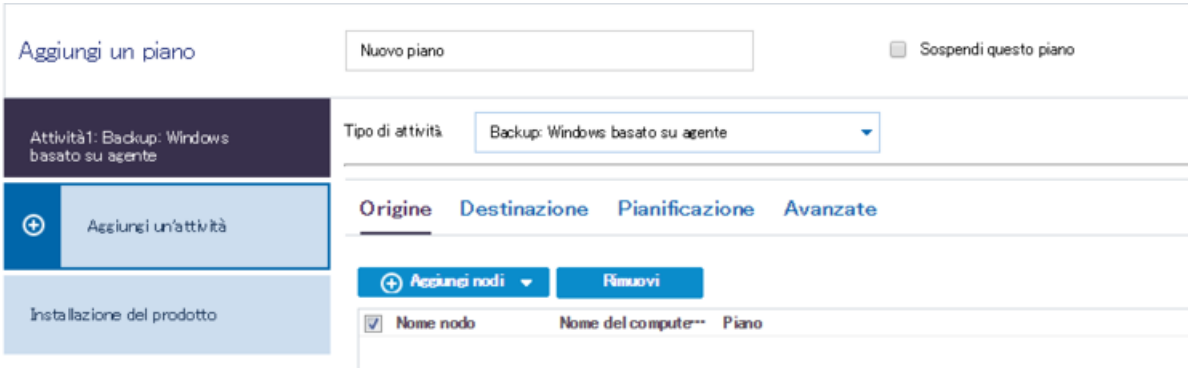
1. Accedere alla console Arcserve UDP.
2. Accedere a **Risorse** > **Piani** > **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina Aggiungi un piano.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa Tipo di attività, selezionare **Backup, Windows basato su agente**.



Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine che si desidera proteggere. È possibile selezionare più di un nodo per un piano. Se non sono stati aggiunti nodi alla console, è possibile aggiungerli in fase di creazione o modifica di un piano dalla pagina Origine. È inoltre possibile salvare un piano senza aggiungere nessun nodo di origine. Il piano viene distribuito soltanto dopo l'aggiunta dei nodi di origine.

Effettuare le operazioni seguenti:

1. Nella scheda Origine, fare clic su **Aggiungi**.
2. Selezionare una delle seguenti opzioni:

   Selezionare i nodi da proteggere in Arcserve UDP

   Consente di visualizzare la finestra di dialogo Selezionare i nodi da proteggere in Arcserve UDP. Selezionare i nodi dall'elenco visualizzato. Selezionare questa opzione se sono stati già aggiunti nodi alla Console.

   Aggiungi nodo Windows

   Viene visualizzata la finestra di dialogo Aggiungi nodi a un piano. Selezionare questa opzione se non sono stati aggiunti nodi e si desidera aggiungere manualmente i nodi da proteggere.

   Rileva nodi da Active Directory

   Consente di aprire la finestra di dialogo Aggiungi nodi alla Console Arcserve UDP. Selezionare questa opzione se si desidera rilevare e aggiungere nodi da Active Directory.

3. Se è stata selezionata l'opzione **Selezionare i nodi da proteggere in Arcserve UDP**, nella finestra di dialogo Selezionare i nodi da proteggere, procedere come segue:

   a. (Facoltativo) Selezionare un filtro dall'elenco a discesa Gruppi per filtrare i nodi. Immettere parole chiave per applicare ulteriori filtri ai nodi.

      I nodi vengono visualizzati nella colonna Nodi disponibili.

   b. Selezionare i nodi dalla colonna Nodi disponibili, quindi fare clic sulla freccia destra singola (>) o sulla freccia destra doppia (>>) per spostare rispettivamente i nodi selezionati o tutti i nodi nella colonna Nodi selezionati.

      I nodi vengono visualizzati nella colonna Nodi selezionati.

   c. Fare clic su **OK** per chiudere la finestra di dialogo.



4. Per scegliere il Tipo di protezione, selezionare una delle seguenti opzioni:

   Backup di tutti i volumi

   Prepara una snapshot del backup di tutti i volumi.

   Backup dei volumi selezionati

   Prepara una snapshot del backup del volume selezionato.

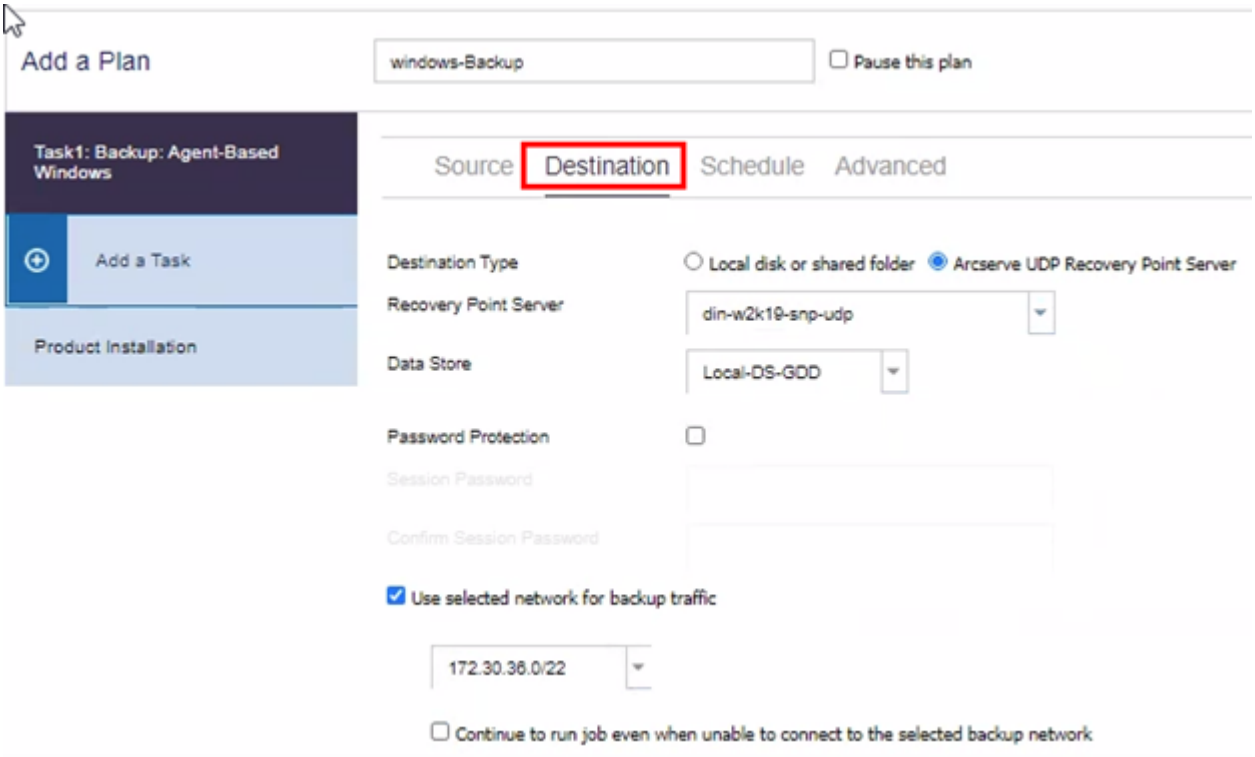
   L'origine viene specificata.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Destinazione**.



2. Selezionare uno dei seguenti tipi di destinazione:

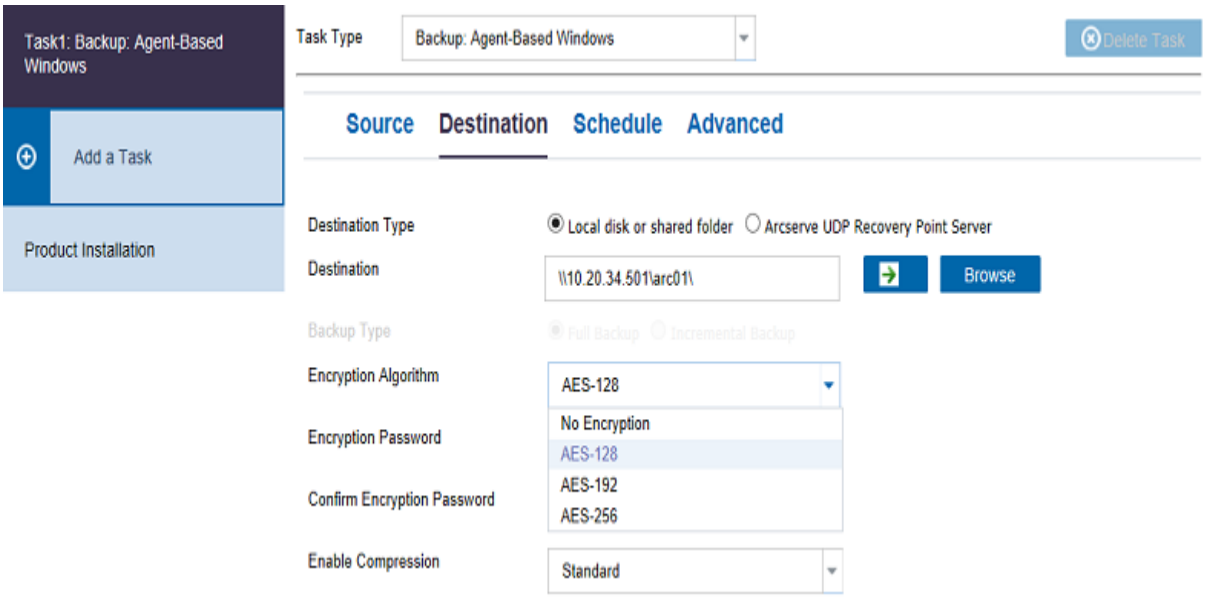
   Disco locale o cartella condivisa

   Specifica che la destinazione di backup è una destinazione locale o una cartella condivisa. Se si seleziona questa opzione, è possibile salvare i dati come punti di ripristino o set di ripristino. Le opzioni dei punti di ripristino e dei set di ripristino sono disponibili nella scheda Pianificazione.

   Recovery Point Server di Arcserve UDP

   Specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono memorizzati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.

3. Se si seleziona il **disco locale o la cartella condivisa** come tipo di destinazione, fornire i seguenti dettagli:



- Destinazione: fornire il percorso completo della destinazione locale o di rete. Per la destinazione di rete, specificare le credenziali con l'accesso di scrittura. Fare clic su **Sfoglia** per individuare la destinazione oppure fare clic sull'icona della freccia avanti per eseguire il test della connessione e fornire le credenziali per la cartella di destinazione specificata.
- Algoritmo di crittografia: dall'elenco a discesa delle opzioni disponibili, selezionare l'algoritmo di crittografia. Per ulteriori informazioni, consultare la sezione Impostazioni di crittografia.
- (Facoltativo) Password di crittografia: fornire una password di crittografia.
- Conferma password di crittografia: immettere nuovamente la password di crittografia per confermare.
- Abilita compressione: selezionare un tipo di compressione dall'elenco a discesa. Per ulteriori informazioni, consultare la sezione Tipo di compressione.

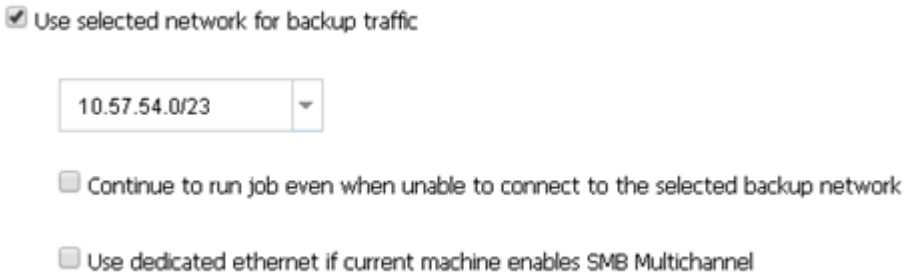
Nota: Se si archiviano i dati in un disco locale o in una cartella condivisa, non è possibile replicare i dati in un altro Recovery Point Server. La replica è supportata solo se si archiviano i dati in un Recovery Point Server.

4. Se si seleziona il **Recovery Point Server di Arcserve UDP** come tipo di destinazione, procedere come segue:
   - Recovery Point Server: dall'elenco a discesa, selezionare il Recovery Point Server (RPS) di destinazione.

- Archivio dati: dall'elenco a discesa, selezionare l'archivio dati di destinazione.
- Protezione password: selezionare la casella di controllo **Protezione password**, fornire la password di sessione, quindi digitare nuovamente la password di sessione per confermare.

  Nota: la password di sessione è facoltativa se la destinazione di backup è un archivio di dati RPS non crittografato.
- (Facoltativo) Selezionare la casella di controllo **Usa rete selezionata per il traffico di backup** e attenersi alla seguente procedura:

  a. Per abilitare la comunicazione tra l'agente Windows e il Recovery Point Server, selezionare la rete CIDR dall'elenco a discesa.

  Nota: se la rete di backup selezionata non è accessibile e si desidera continuare il processo con la rete disponibile o con la rete predefinita, fare clic sulla casella di controllo **Procedere con l'esecuzione del processo anche nel caso in cui sia impossibile stabilire la connessione al CIDR selezionato**.

  b. Per disabilitare SMB Multichannel in modo che i dati vengano trasferiti solo tramite la rete selezionata, selezionare la casella di controllo **Usa l'ethernet apposita se il computer corrente abilita SMB Multichannel**.

  Note:

  - Per impostazione predefinita, questa opzione non è disponibile. Per attivare questa opzione, accedere al seguente percorso nella cartella C:\Programmi\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. Impostare quindi il valore per *useDedicatedEthernet* su True.

```
- <SpecifyNetwork>
    <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

La funzione Definisci rete viene disabilitata nel caso di un archivio dati remoto che utilizza la cartella di rete condivisa come destinazione.

- Quando i servizi di gestione di Arcserve UDP vengono riavviati, la funzionalità SMB Multichannel viene abilitata.
- La funzionalità SMB Multichannel è abilitata in Windows per impostazione predefinita.

La destinazione viene specificata.

Definizione della pianificazione

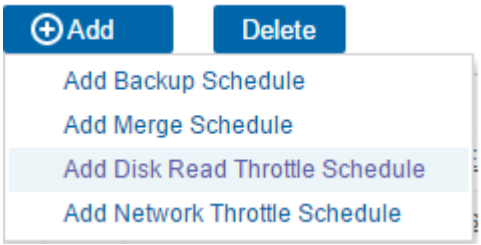
La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito una pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

Effettuare le operazioni seguenti:

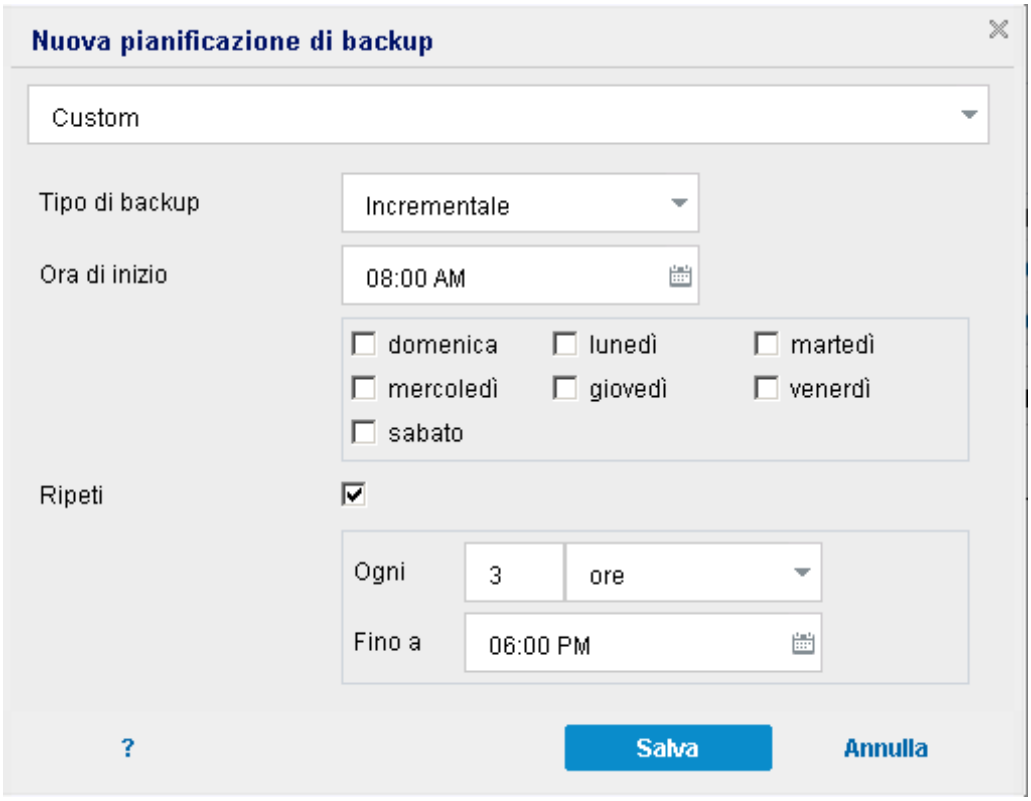
1. Aggiungere le pianificazioni di backup, di unione, Limitazione di lettura del disco e Limite delle risorse di rete.



Aggiunta di una pianificazione di backup

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

   Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni del backup.

Verifica

Specifica la pianificazione dei backup di verifica.

Arcserve UDP controlla che i dati protetti siano validi e completi eseguendo una verifica di affidabilità dell'immagine di backup archiviata sull'origine di backup. Se necessario esegue la risincronizzazione dell'immagine. Un backup di verifica controlla il backup più recente di ogni blocco e lo confronta con il contenuto e le informazioni di origine. Questo confronto consente di verificare che il blocco di backup più recente rappresenti le informazioni corrispondenti all'origine. Se l'immagine di backup di un blocco non corrisponde all'origine (probabilmente a causa di modifiche apportate al sistema dall'ultimo backup), Arcserve UDP aggiorna (risincronizza) il backup del blocco non corrispondente. Sebbene si tratti di una procedura poco frequente, il backup di verifica può essere utilizzato per ottenere le stesse garanzie di un backup completo, ma senza occupare lo stesso spazio.

Vantaggi: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.

Svantaggi: il backup di verifica richiede tempi di esecuzione più lunghi, in quanto esegue il confronto di tutti i blocchi originali con i blocchi del backup più recente.

Incrementale

Specifica la pianificazione dei backup incrementali.

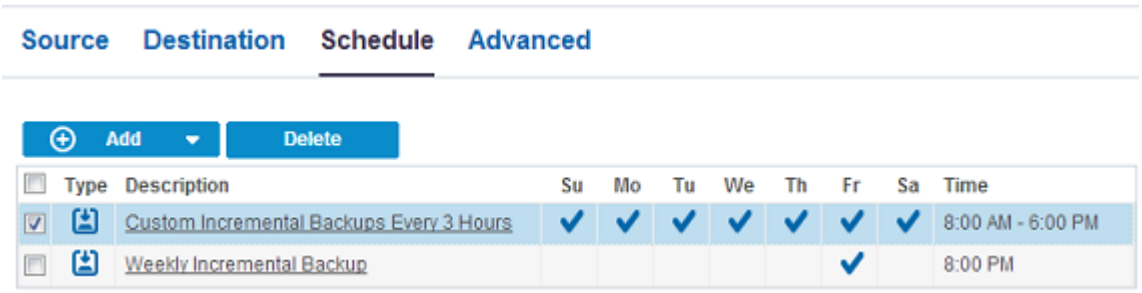
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

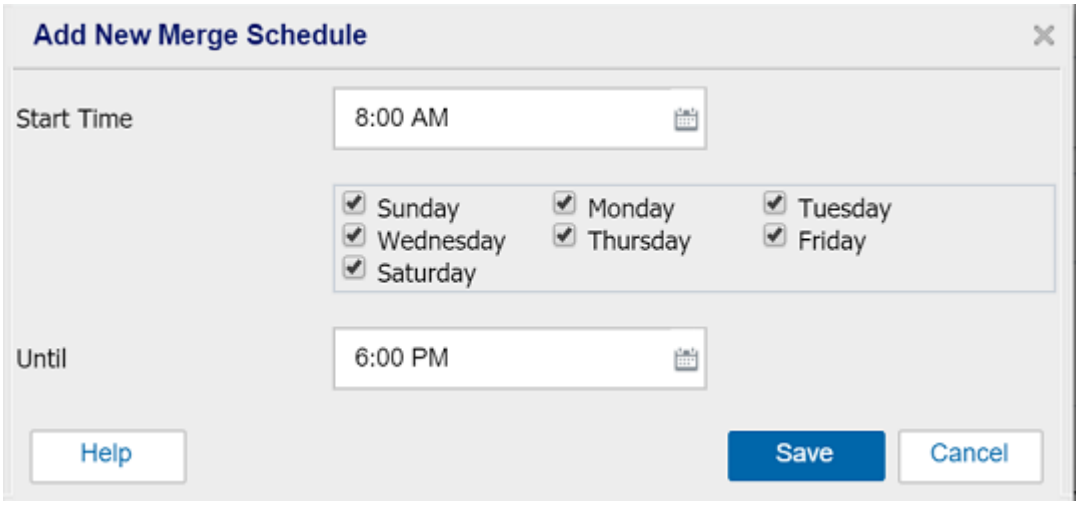
La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di unione**.

   La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.



b. Specificare l'ora di inizio per l'avvio del processo di unione.

c. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

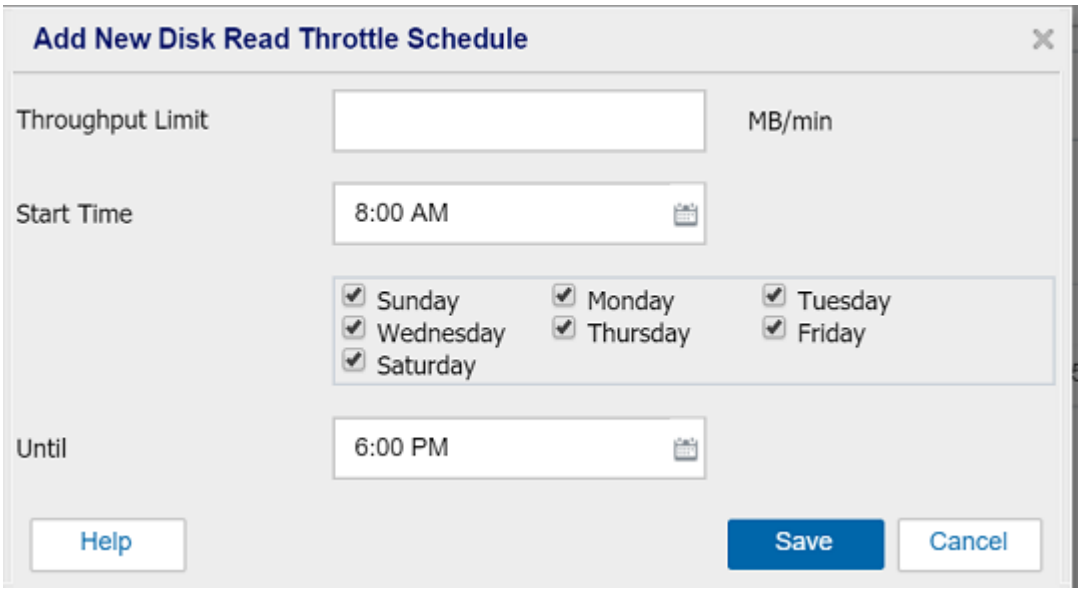
d. Fare clic su **Salva**.

La Pianificazione di unione viene specificata e viene visualizzata nella pagina **Pianificazione**.

Aggiunta della pianificazione di limitazione di lettura del disco

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di limitazione di lettura del disco**.

   Viene visualizzata la finestra di dialogo **Aggiungi nuova pianificazione della limitazione di lettura del disco**.



b. Specificare il limite di velocità effettiva in MB per unità di minuti.

c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

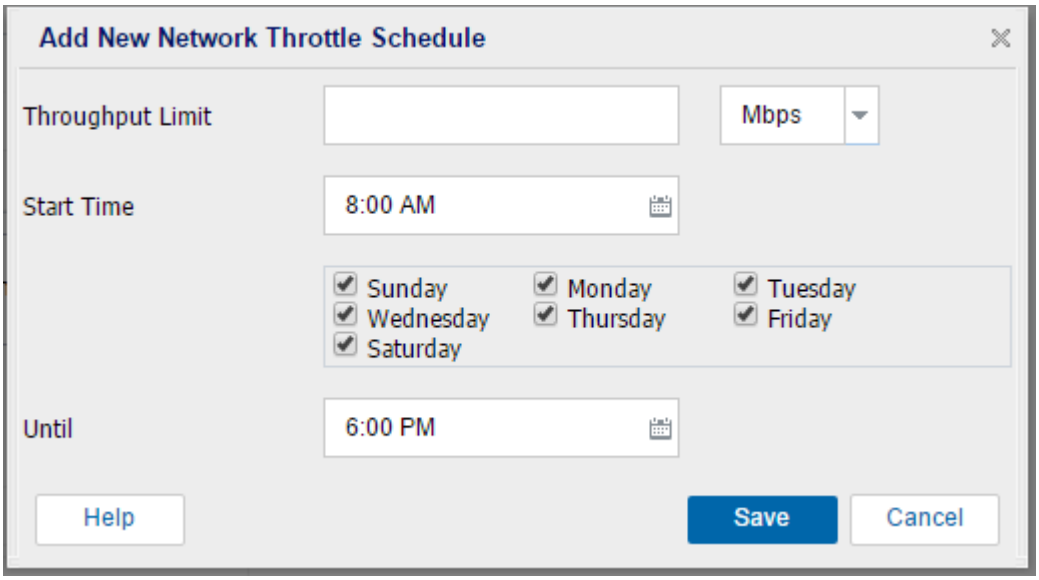
La pianificazione della limitazione di lettura del disco specificata viene visualizzata nella pagina **Pianificazione**.

Aggiunta di una pianificazione del limite delle risorse di rete

Nota: La pianificazione Limite delle risorse di rete viene visualizzata solo per il backup basato sull'agente Windows quando viene definita come destinazione per il piano un archivio dati con deduplicazione abilitata.

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse di rete**.

   Viene visualizzata la finestra di dialogo **Aggiungi una nuova pianificazione del limite delle risorse di rete**.



b. Specificare il limite di velocità effettiva in Mbps o Kbps.

   Nota: Il valore minimo predefinito è 500 kbps. Per modificare il valore predefinito valore procedere come segue:

   i. Dal percorso di registro SOFTWARE\Arcserve\Unified Data Protection\Management\Console, aggiungere una chiave MinNetworkThrottleValueInKpbs, tipo REG_SZ e impostare il valore.

   ii. Riavviare il servizio di gestione di Arcserve UDP.

   iii. Modificare il piano o crearne uno nuovo.

   Il valore personalizzato inizia ad avere effetto.

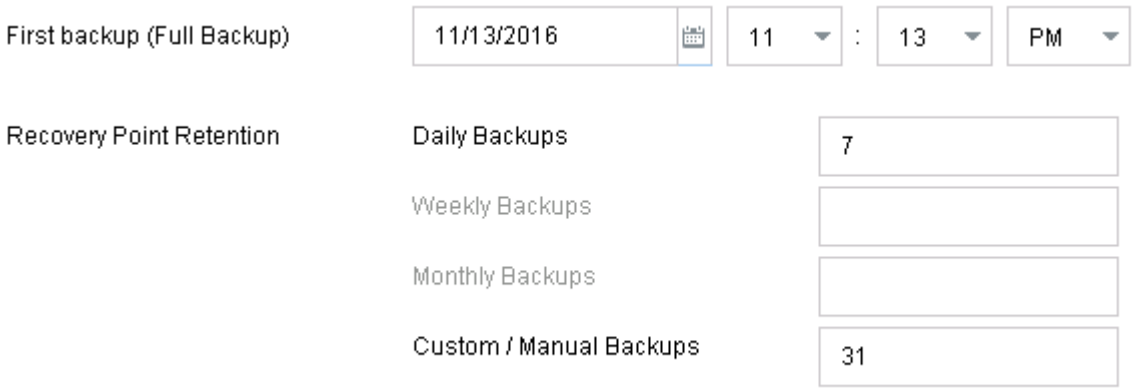
c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

La pianificazione del limite delle risorse di rete specificata viene visualizzata nella pagina **Pianificazione**.

2. Specificare l'ora di inizio per il backup pianificato.



3. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo Pianificazione di backup.

   Viene specificata la pianificazione.

Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione

L'opzione di pianificazione consente di specificare una pianificazione personalizzata o una pianificazione giornaliera/settimanale/mensile o entrambe. Nella pianificazione personalizzata è possibile configurare la pianificazione del backup per ciascun giorno della settimana e aggiungere fino a quattro pianificazioni di backup ogni giorno. È possibile selezionare un giorno specifico di una settimana e creare un intervallo di tempo per definire quando eseguire il backup e la frequenza.

Pianificazione	Processo supportato	Commenti
Backup	Processo di backup	Definire gli intervalli di tempo per eseguire i processi di backup.
Limitazione della velocità di backup	Processo di backup	Definire gli intervalli di tempo per controllare la velocità di backup.
Unione	Processo di unione	Definire quando unire i processi.
Pianificazione quotidiana	Processo di backup	Definire quando eseguire processi di backup quotidiani.
Pianificazione settimanale	Processo di backup	Definire quando eseguire processi di backup settimanali.
Pianificazione mensile	Processo di backup	Definire quando eseguire processi di backup mensili.

È inoltre possibile specificare le impostazioni di memorizzazione per i punti di ripristino.

Nota: All'interno di ogni piano è necessario configurare le impostazioni di conservazione per controllare il modo in cui i nodi assegnati a tale piano vengono memorizzati nell'archivio dati di destinazione.

Le pianificazioni per i backup giornalieri/settimanali/mensili sono indipendenti dalla pianificazione personalizzata e gli uni dagli altri. È possibile configurare di eseguire solo il backup giornaliero, il backup settimanale o il backup mensile senza configurare la pianificazione personalizzata.

Pianificazione del processo di backup

È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del backup. Un intervallo di tempo valido è dalle 00:00 alle 23:59. Non è possibile specificare un intervallo di tempo come ad esempio dalle 18:00 alle 06:00. In tali casi, si devono specificare manualmente due intervalli di tempo diversi.

Per ogni intervallo di tempo l'ora di inizio è inclusa e l'ora di fine è esclusa. Ad esempio, si è configurato il backup incrementale da eseguire ogni ora tra le 06:00 e le 09:00 e il backup inizierà alle 06:00. Ciò significa che il backup verrà eseguito alle 06:00, alle 07:00 e 08:00, ma NON alle 09:00.

Nota: Se si desidera eseguire il processo di backup ripetutamente fino al termine della giornata, impostare la pianificazione fino alle 00:00. Ad esempio, per eseguire un processo di backup ogni 15 minuti per l'intera giornata, impostare la pianificazione dalle 00:00 alle 00:00 ogni 15 minuti.

Pianificazione del limite delle risorse di backup

La pianificazione del limite delle risorse di backup consente di controllare la velocità effettiva di backup, che a sua volta controlla l'utilizzo delle risorse (I/O del disco, CPU, larghezza di banda della rete) del server di cui si esegue il backup. Questo è utile se non si desidera influire sulle prestazioni del server durante i normali orari di ufficio. È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del limite delle risorse di backup. Per ogni intervallo di tempo è possibile specificare un valore, in MB per minuto. Questo valore viene utilizzato per controllare la velocità effettiva di backup. I valori validi sono compresi tra 1 MB/minuto a 99999 MB/minuto.

Se un processo di backup si estende oltre il tempo specificato, il limite della velocità cambia in conformità all'intervallo di tempo specificato. Ad esempio, il limite delle risorse di backup definito è 500 MB/minuto dalle 08:00 alle 20:00 e 2500 MB/minuto dalle 20:00 alle 22:00. Se un processo di backup inizia alle 19:00 e viene eseguito per tre ore, dalle 19:00 alle 20:00 il limite della velocità è pari a 500 MB/minuto e dalle 20:00 alle 22:00 a 2500 MB/minuto.

Se non si definisce alcuna pianificazione del backup e della sua velocità effettiva, il backup viene eseguito il più rapidamente possibile.

Pianificazione di unione

Consente di unire i punti di ripristino in base alla pianificazione fornita.

Considerare i punti seguenti per il processo di unione:

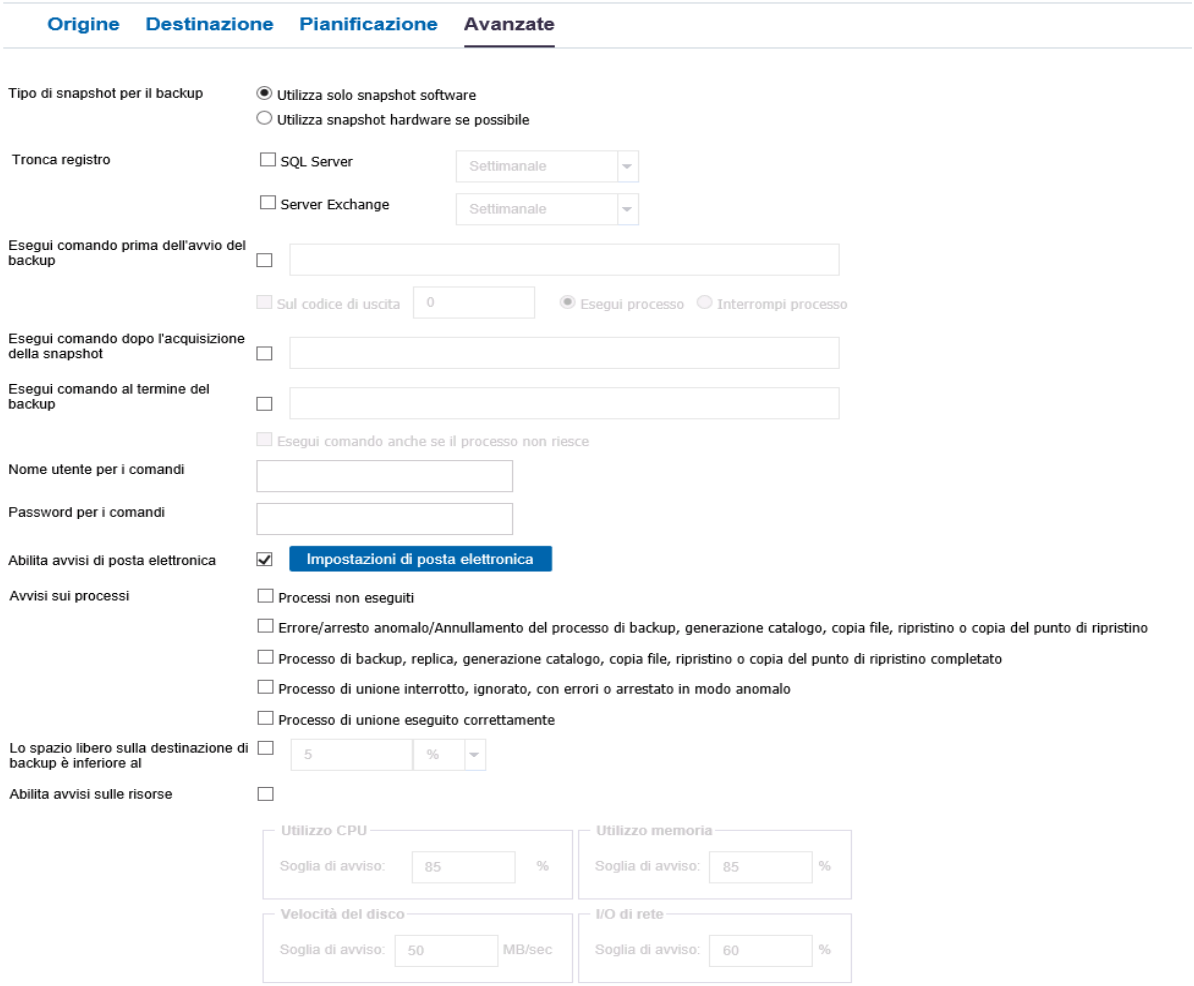
- In qualsiasi momento è possibile eseguire solo un processo di unione per un nodo.
- Se un processo di unione inizia, esso deve essere completato prima di poter avviare il processo di unione successivo. Ciò significa che se uno o più set di punti di ripristino vengono uniti, non è possibile aggiungere nuovi punti di ripristino a questo processo di unione finché il processo di unione dell'insieme corrente dei punti di ripristino non viene completato.

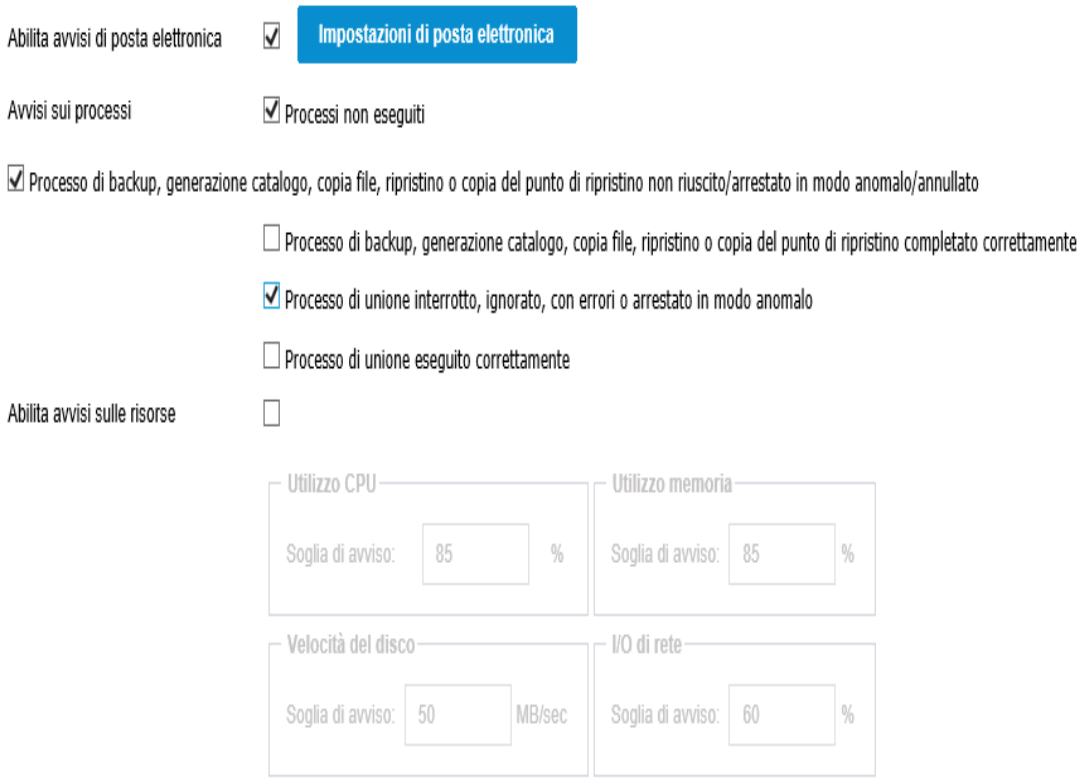
- Se un processo di unione sta elaborando più di un set di punti di ripristino (ad esempio set [1~4], set [5~11] e set [12~14] sono tre set distinti), il Recovery Point Server elabora tali set uno alla volta.
- Se un processo di unione viene ripreso dopo una pausa, il processo individua in quale punto era stato interrotto e riprende l'unione da tale punto.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione delle impostazioni per troncare i registri, l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda Avanzate:


Origine
Destinazione
Pianificazione
Avanzate
Tipo di snapshot per il backup
Utilizza solo snapshot software
Utilizza snapshot hardware se possibile
Tronca registro
SQL Server
Settimanale
Server Exchange
Settimanale
Esegui comando prima dell'avvio del backup
Sul codice di uscita
0
Esegui processo
Interrompi processo
Esegui comando dopo l'acquisizione della snapshot
Esegui comando al termine del backup
Esegui comando anche se il processo non riesce
Nome utente per i comandi
Password per i comandi
Abilita avvisi di posta elettronica
Impostazioni di posta elettronica
Avvisi sui processi
Processi non eseguiti
Errore/arresto anomalo/Annullamento del processo di backup, generazione catalogo, copia file, ripristino o copia del punto di ripristino
Processo di backup, replica, generazione catalogo, copia file, ripristino o copia del punto di ripristino completato
Processo di unione interrotto, ignorato, con errori o arrestato in modo anomalo
Processo di unione eseguito correttamente
Lo spazio libero sulla destinazione di backup è inferiore al
5
%
Abilita avvisi sulle risorse
Utilizzo CPU
Soglia di avviso:
85
%
Utilizzo memoria
Soglia di avviso:
85
%
Velocità del disco
Soglia di avviso:
50
MB/sec
I/O di rete
Soglia di avviso:
60
%



Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

   Tipo di snapshot per il backup

   Selezionare una delle seguenti opzioni per la snapshot del backup:

   Utilizza solo snapshot software

   Specifica che il tipo di backup utilizza solo la snapshot software. Arcserve UDP non cercherà la snapshot hardware. La snapshot software utilizza un numero minore di risorse sui computer virtuali. È possibile utilizzare questa opzione se il server presenta configurazioni e velocità di elaborazione inferiori.

   Utilizza snapshot hardware se possibile

   Specificare che il tipo di backup verifica innanzitutto una la presenza di una snapshot hardware. Se tutti i criteri vengono soddisfatti, il tipo di backup utilizza la snapshot hardware.

   Nota: Per ulteriori informazioni sui criteri della snapshot hardware, consultare la sezione dedicata ai prerequisiti.

   Tronca registro

Consente di specificare la pianificazione per troncare i registri per SQL Server ed Exchange Server. È possibile specificare la pianificazione come **Giornaliero**, **Settimanale** o **Mensile**.

Abilitare l'eliminazione dei registri con cadenza oraria per SQL Server tramite un'opzione del Registro di sistema

- Configurare le impostazioni del piano. Selezionare l'opzione "SQL Server" nella sezione "Tronca registro" della scheda "Avanzate", quindi selezionare "Ogni giorno".
- Impostare la chiave del Registro di sistema sul computer SQL Server che ospita l'agente UDP. "PurgeSqlLogPerHour" è dell'intervallo di tempo in ore per l'eliminazione del registro di SQL Server.

  Percorso: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

  Nome valore: PurgeSqlLogPerHour (indica l'intervallo di tempo in ore per l'eliminazione del registro di SQL Server).

  Tipo valore: REG_DWORD

Nome utente

Consente di specificare l'utente autorizzato per l'esecuzione di uno script.

Password

Consente di specificare la password dell'utente autorizzato all'esecuzione dello script.

Esegui un comando prima dell'avvio del backup

Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso completo di archiviazione dello script. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Esegui processo** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

Esegui un comando dopo l'acquisizione della snapshot

Consente di eseguire uno script dopo l'acquisizione della snapshot del backup. Specificare il percorso completo di archiviazione dello script.

Per eseguire lo script successivo alla snapshot anche durante un errore di snapshot, selezionare l'opzione **Esegui il comando anche se la snapshot non riesce**.

Esegui un comando al completamento del backup

Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso completo di archiviazione dello script.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere mediante posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy. Per ulteriori informazioni sulla configurazione delle impostazioni di posta elettronica, consultare la sezione Configurazione di posta elettronica e avvisi.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

Abilita avvisi sulle risorse

Consente di specificare una soglia per Utilizzo CPU, Memoria, Velocità del disco, I/O di rete. È possibile fornire il valore in percentuale. Si riceve un messaggio di posta elettronica al superamento del valore Soglia di avviso.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su Salva.

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: Se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo.

Il piano di backup viene creato e distribuito automaticamente al nodo di origine. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

(Facoltativo) Esecuzione di un backup manuale

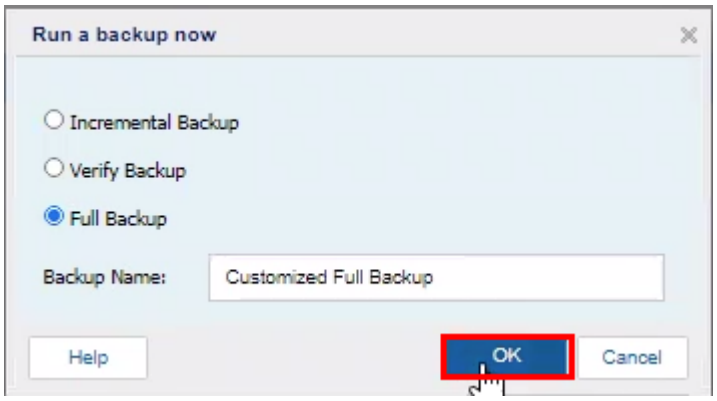
In genere, i backup vengono eseguiti automaticamente e vengono controllati attraverso le impostazioni di pianificazione. In aggiunta al backup pianificato, un backup manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze. Ad esempio, se si dispone di una pianificazione di ripetizione per backup completi, incrementali e di verifica e si desidera apportare modifiche sostanziali al computer, sarà necessario eseguire un backup manuale immediato senza attendere l'esecuzione del successivo backup pianificato.

Effettuare le operazioni seguenti:

1. Accedere alla console Arcserve UDP.
2. Accedere a **Risorse** > **Piano** > **Tutti i piani**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i piani.
3. Fare clic con il pulsante destro del mouse sul piano, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
4. Nella finestra di dialogo Esegui backup immediato, selezionare il tipo di backup che si desidera eseguire, quindi specificare il nome del backup, se necessario.



Le opzioni disponibili sono:

Backup incrementale

Avvia un backup incrementale del computer. Un backup incrementale esegue il backup solo dei blocchi modificati dopo l'ultimo backup.

Nota: se si esegue un backup per la prima volta, il backup completo viene avviato automaticamente anche se è stata selezionata l'opzione Backup incrementale.

I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup con dimensioni molto ridotte. Questa modalità di esecuzione backup è ottimale.

Backup di verifica

Avvia un backup di verifica individuando il backup più recente di ciascun blocco e ne confronta il contenuto e le informazioni con l'origine. Questo confronto consente di verificare che il blocco di backup più recente rappresenti le informazioni corrispondenti all'origine. Se l'immagine di backup di un blocco non corrisponde all'origine, l'agente Arcserve UDP (Windows) aggiornerà (risincronizzerà) il backup di tale blocco.

Vantaggi: viene prodotta un'immagine di backup di dimensioni molto ridotte rispetto al backup completo, poiché viene eseguito solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono all'ultimo backup.

Svantaggi: la velocità del backup è ridotta poiché tutti i blocchi del disco di origine vengono confrontati con i blocchi dell'ultimo backup.

Backup completo

Avvia un backup completo dell'intero computer o dei volumi selezionati.

Note:

- Se si aggiunge un nuovo volume all'origine di backup, il volume appena aggiunto verrà sottoposto a un backup completo, indipendentemente dal metodo di backup generale utilizzato.
- Se non viene specificato alcun nome di backup, per impostazione predefinita viene automaticamente denominato Backup completo personalizzato/Incrementale/Di verifica.

5. Fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.

6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.

7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Nota: è possibile eseguire un solo processo alla volta. Se si tenta di avviare manualmente un processo di backup durante l'esecuzione di un altro processo, verrà visualizzato un messaggio di avviso indicante che un altro processo è in esecuzione, per cui sarà necessario riprovare in un momento successivo.

   Il backup manuale è stato eseguito correttamente.

Verifica del backup

Per verificare il processo di backup, confermare di avere creato correttamente il piano di backup. Dopo avere verificato che il piano è stato creato correttamente, confermare se il processo di backup è in esecuzione secondo quanto pianificato. È possibile verificare lo stato dei processi di backup dalla scheda **Processi**.

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Attenersi a uno dei seguenti metodi per verificare i processi di backup:

Metodo 1

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Tutti i processi completati**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Metodo 2

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Processi completati correttamente**.

   L'elenco dei processi di backup completati viene visualizzato nel riquadro centrale.
3. Fare clic sul processo che si desidera verificare.

   Il riquadro destro viene aggiornato.
4. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
5. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Creazione di un piano di backup di Nutanix

Per proteggere i nodi Nutanix, è necessario creare un piano. I nodi del piano sono costituiti dalle attività di backup. Questa attività di backup consente di specificare i nodi che si desidera proteggere, la destinazione di backup e la pianificazione dei backup. La destinazione di backup è un Recovery Point Server su cui archiviare i dati sottoposti a backup. La destinazione può essere una destinazione locale o una cartella di condivisione remota.

Per esplorare le funzioni disponibili per la funzione Nutanix in Arcserve UDP, consultare la sezione Come utilizzare Nutanix con Arcserve UDP.

Creazione di un piano di Virtual Standby per Nutanix AHV

Per proteggere Virtual Standby su Nutanix AHV, consultare la sezione Protezione di Virtual Standby su AHV Nutanix.

Creazione di un computer virtuale istantaneo su Nutanix AHV

Per creare un computer virtuale istantaneo su Nutanix AHV, fare riferimento alla sezione Creazione di un computer virtuale istantaneo su Nutanix AHV.

Creazione di un piano Assured Recovery per proteggere Nutanix AHV per un nodo Linux

Per creare un piano Assured Recovery per proteggere Nutanix AHV per un nodo Linux, fare riferimento alla sezione Creazione di un piano Assured Recovery per proteggere Nutanix AHV per un nodo Linux.

Backup del volume cluster condiviso

Arcserve UDP supporta il backup del volume cluster condiviso (CSV) creato dalla versione 6.5 Aggiornamento 4. I volumi CSV vengono creati in caso di spazio di archiviazione e sono trasparenti per l'agente Arcserve UDP (Windows). CSV viene sempre considerato per il backup completo a livello di volume, indipendentemente dal tipo di processo di backup (completo o incrementale). Il backup CSV protegge i dati di tutti i file system popolari come NTFS, la deduplicazione NTFS, ReFS e CSVFS.

È possibile creare o aggiornare un piano basato sull'agente dalla Console Arcserve UDP per l'esecuzione del backup del volume CSV specificato.

Effettuare le operazioni seguenti:

1. Selezionare il volume cluster condiviso nel computer dell'agente. Per ulteriori informazioni, consultare la sezione Modifica delle impostazioni del computer dell'agente per il backup del volume CSV.

   Nota: è inoltre possibile eseguire il processo di backup dal computer dell'agente Windows. Per ulteriori informazioni, consultare la sezione Esecuzione del backup dal computer dell'agente Windows.

2. Per eseguire il backup dalla Console Arcserve UDP, accedere alla scheda **Risorse**.
3. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

4. Nel riquadro centrale, fare clic su **Aggiungi un piano** e specificare il nome del piano.
5. Dall'elenco a discesa **Tipo di attività**, selezionare **Backup, Windows basato su agente**.
6. Dalla scheda **Origine** del piano, selezionare la casella di controllo **Backup di tutti i volumi** come **Tipo di protezione**.
7. Specificare i dettagli Destinazione, Pianificazione e Avanzate. Per ulteriori informazioni, consultare la sezione Creazione di un piano di backup di Windows.

   A questo punto, dopo aver salvato il piano con l'esecuzione del processo di backup, viene eseguito il backup del volume CSV specificato per l'agente Windows.
8. Verificare lo stato dei processi sottoposti a backup. Per ulteriori informazioni, consultare la sezione Verifica del backup.

   Note:

   - il registro attività del nodo proprietario visualizza l'avanzamento del processo di backup e registra il messaggio di completamento al termine dell'operazione. Il registro attività del nodo membro (che non è il proprietario) visualizza un messaggio di avviso simile al seguente, ma lo stato di backup risulta corretto.

     Avviso: impossibile recuperare percorso fisico del volume cluster condiviso [C:\ClusterStorage\Volume1]. Il volume verrà escluso dal backup.
   - Se si desidera escludere il volume CSV durante il backup, procedere come segue:

     a. Sul nodo dell'agente UDP, aprire la chiave di registro nel percorso seguente:

        HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

     b. Creare il valore DWORD "BackupCSV".

     c. Impostare il valore su 0.

        In questo modo il volume CSV verrà escluso dal backup.

Modifica delle impostazioni del computer dell'agente sul volume CSV di backup

Prima di eseguire il primo backup, è necessario configurare le impostazioni di backup che si applicano a tutti i processi di backup. Queste impostazioni possono essere memorizzate per i backup futuri oppure modificate in qualsiasi momento dalla pagina principale dell'agente Arcserve UDP (Windows).

Effettuare le operazioni seguenti:

1. Dalla pagina principale dell'agente Arcserve UDP (Windows) (o dal monitoraggio dell'agente Arcserve UDP (Windows), fare clic su **Impostazioni**.

   Verrà visualizzata la finestra Impostazioni.

2. Fare clic sulla scheda **Impostazioni di backup**.

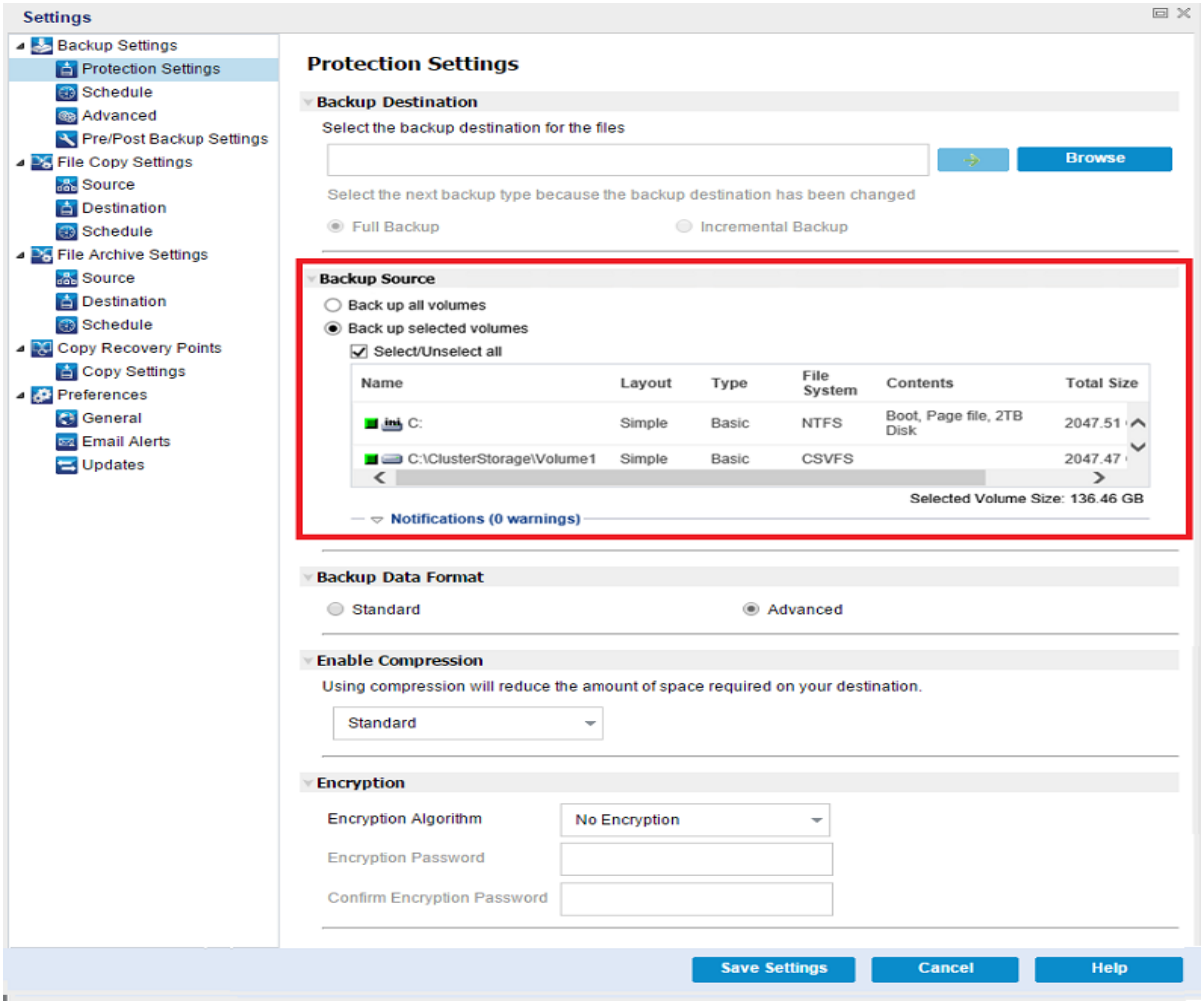
   Viene visualizzata la finestra Impostazioni di backup.

3. Fare clic su Impostazioni di protezione.

4. Viene visualizzata la finestra di dialogo Impostazioni di protezione.

   Note:

   - Se l'agente Arcserve UDP (Windows) viene gestito dalla Console, non tutte le impostazioni saranno disponibili e verranno visualizzate come informazioni di sola lettura.
   - Quando l'agente è gestito dalla console e non è protetto in un piano, tutte le impostazioni sono ancora disponibili, ad eccezione del riquadro Preferenze > Aggiornamenti.



5. Dal gruppo **Origine di backup**, selezionare **Esegui backup dei volumi selezionati**.

   Viene visualizzato l'elenco dei volumi disponibili nel computer dell'agente.

6. Selezionare il volume CSV di cui si desidera eseguire il backup e fare clic su **Salva impostazioni**.

   Le impostazioni di protezione per il backup vengono salvate.

Backup di volumi senza lettera di unità

A partire da Arcserve UDP v6.5 Aggiornamento 4, è possibile proteggere i volumi senza lettera di unità mediante l'opzione **di montaggio dei volumi nella cartella NTFS** sui **volumi di backup selezionati**. Prima di selezionare l'opzione **di montaggio nei volumi nella cartella NTFS** dalla Console Arcserve UDP, è necessario montare il volume della cartella NTFS. È inoltre possibile eseguire ulteriori personalizzazioni ed eseguire il backup soltanto di alcuni volumi sprovvisti di lettera di unità invece di eseguire il backup di tutti i volumi.

Per ulteriori informazioni, consultare le seguenti sezioni:

- Verifica dei prerequisiti
- Montaggio del volume senza lettera di unità nella cartella NTFS
- Definizione del volume senza lettera di unità nel Registro di sistema

Verifica dei prerequisiti

Verificare quanto segue:

- Affinché l'archivio dati sia in esecuzione tra i riavvii RPS, abilitare il montaggio automatico sul server RPS. È possibile attivare il montaggio automatico utilizzando il comando diskpart - automount.

  Effettuare le operazioni seguenti:

  1. Aprire un prompt dei comandi con privilegi elevati.
  2. Nel prompt dei comandi con privilegi elevati eseguire le seguenti operazioni:
  3. Digitare *diskpart*, quindi premere **Invio**.
  4. Digitare *automount enable* e premere **Invio**.
  5. Chiudere il prompt dei comandi con privilegi elevati.
  6. Per applicare le modifiche, riavviare il computer.

Montaggio del volume senza lettera di unità nella cartella NTFS

È necessario montare il volume senza lettera di unità nella cartella NTFS per eseguire il backup del volume e dei contenuti del punto di montaggio.

Effettuare le operazioni seguenti:

1. Dalla **Gestione dei dischi Windows**, selezionare un nuovo disco per cui non è stata assegnata una lettera di unità.
2. Dalle opzioni disponibili facendo clic con il tasto destro del mouse, selezionare **Modifica lettera di unità e percorsi**.

   Viene visualizzata la finestra di dialogo Aggiungi lettera di unità.
3. Fare clic su **Modifica**.

   Viene visualizzata la finestra di dialogo Modifica lettera di unità.

4. Selezionare l'opzione di **montaggio nella cartella NTFS vuota successiva**, specificare il percorso seguente e fare clic su **OK**.

   C:\MountPoint

   Il punto di montaggio viene visualizzato in Windows Explorer. Il volume è stato montato correttamente senza la lettera di unità.

Definizione di un volume senza lettera di unità nel Registro di sistema.

È necessario specificare il volume senza lettera di unità nel Registro di sistema per proteggere il volume e i contenuti corrispondenti nel punto di montaggio.

Effettuare le operazioni seguenti:

1. Dalla **Gestione dei dischi Windows**, selezionare un nuovo disco per cui non è stata assegnata una lettera di unità.
2. Fare clic con il tasto destro del mouse e selezionare **Proprietà**.

   Viene visualizzata la finestra Proprietà disco.
3. Dalla scheda **Protezione** copiare il **nome dell'oggetto**.
4. Nel computer dell'**agente Windows**, accedere al **nodo dell'agente** corrispondente e aprire il **Registro di sistema**.

   Verrà visualizzata la finestra del Registro di sistema.
5. Accedere al percorso seguente e fare clic su **BackupVolumesWIthMountedVolumes**.

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Verrà visualizzata la finestra di dialogo di modifica di più stringhe.
6. Nel campo **Dati valore**, aggiungere il nome dell'oggetto copiato.
7. Fare clic su **OK**.

   Il volume senza lettera di unità è specificato nel Registro di sistema.

   Quando si esegue backup dalla Console Arcserve UDP, vengono tenuti in considerazione soltanto i volumi specificati nel Registro di sistema.

Esecuzione del backup del volume selezionato

Il presente argomento descrive la modalità di esecuzione del backup dei volumi selezionati e non di un backup completo. Per eseguire il backup di un volume

specifico, è necessario selezionare la casella di controllo **Backup dei volumi selezionati** dall'opzione Origine durante la creazione di un piano.

Effettuare le operazioni seguenti:

1. Durante la creazione o la modifica di un piano, selezionare la scheda Origine.
2. Selezionare la casella di controllo Backup dei volumi selezionati con Tipo protetto.

   Verranno visualizzati diversi campi per la selezione dell'unità e delle altre opzioni relative al volume.
3. Selezionare uno o più unità dall'elenco delle unità disponibili.
4. Selezionare una o più opzioni dall'elenco dei volumi seguente:

   Volume di sistema riservato

   Indica il volume richiesto per l'avvio del sistema operativo. Selezionare l'opzione se si desidera eseguire il ripristino bare metal per il nodo di backup oppure per un'unità specifica.

   Volume di ripristino

   Indica il volume richiesto per l'ambiente di ripristino Windows. Selezionare l'opzione se si desidera eseguire il backup del volume di ripristino.

   Volume di avvio

   Indica il volume richiesto per l'avvio del sistema operativo Windows. Selezionare l'opzione se si desidera eseguire il ripristino bare metal per il nodo di backup oppure per un'unità specifica.

   Montaggio nei volumi della cartella NTFS

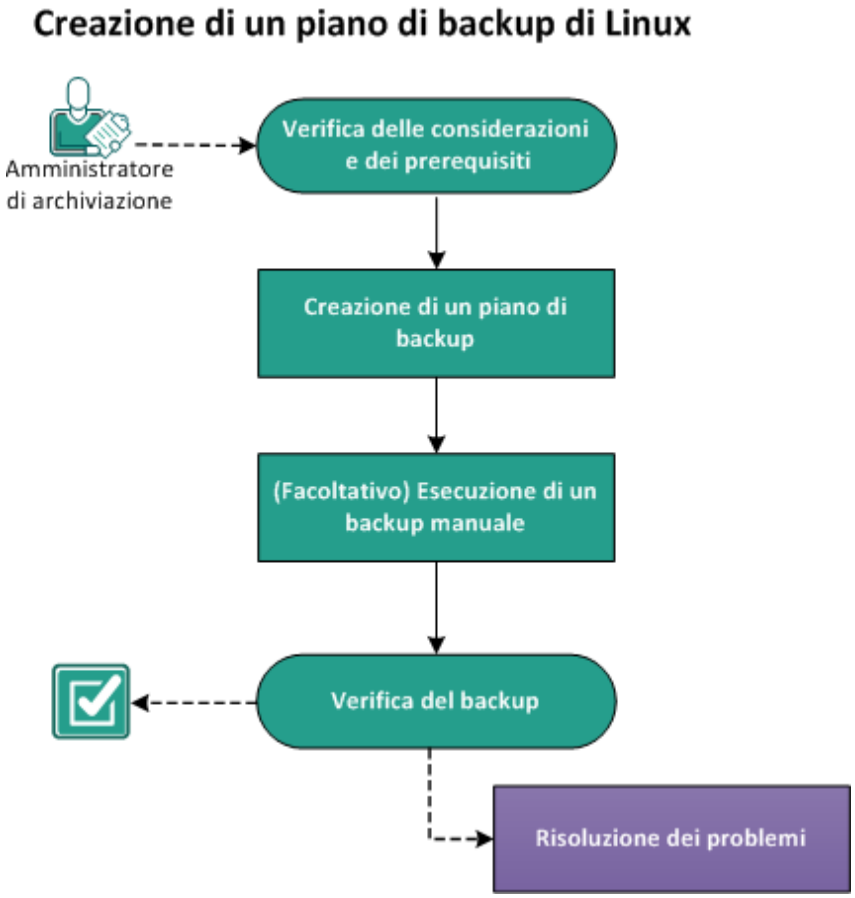
   Indica l'opzione di montaggio dei volumi nella cartella NTFS. Selezionare questa opzione se è possibile eseguire il backup di volumi senza lettera di unità. Prima di selezionare l'opzione nel piano, è necessario montare un volume nella cartella NTFS. È inoltre possibile eseguire ulteriori personalizzazioni ed eseguire il backup soltanto di alcuni volumi sprovvisti di lettera di unità invece di eseguire il backup di tutti i volumi. Per ulteriori informazioni, consultare la sezione Backup di volumi senza lettera di unità
5. Immettere i dettagli nelle altre schede del piano e salvare il piano.

   È stata specificata l'unità o il volume. Durante l'esecuzione del processo di backup, verrà eseguito il backup soltanto del volume o dell'unità selezionati.

Creazione di un piano di backup di Linux

Per proteggere i nodi di Linux, è necessario creare un piano. Un piano di backup per i nodi di Linux consiste in un'attività di backup. Questa attività di backup consente di specificare i nodi che si desidera proteggere, la destinazione di backup e la pianificazione dei backup. La destinazione di backup può essere una destinazione locale, una cartella di condivisione remota o un archivio dati in un Recovery Point Server.

Nel diagramma seguente viene illustrato il processo di protezione dei nodi di Linux:



Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di un piano di backup
3. (Facoltativo) Esecuzione di un backup manuale
4. Verifica del backup
5. Risoluzione dei problemi

Verifica delle considerazioni e dei prerequisiti

Completare i prerequisiti seguenti:

- Accedere alla console.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Creazione di un piano di backup

Un piano di backup include un'attività di backup che esegue un backup del nodo fisico o virtuale e archivia i dati nella destinazione specificata.

Effettuare le operazioni seguenti:

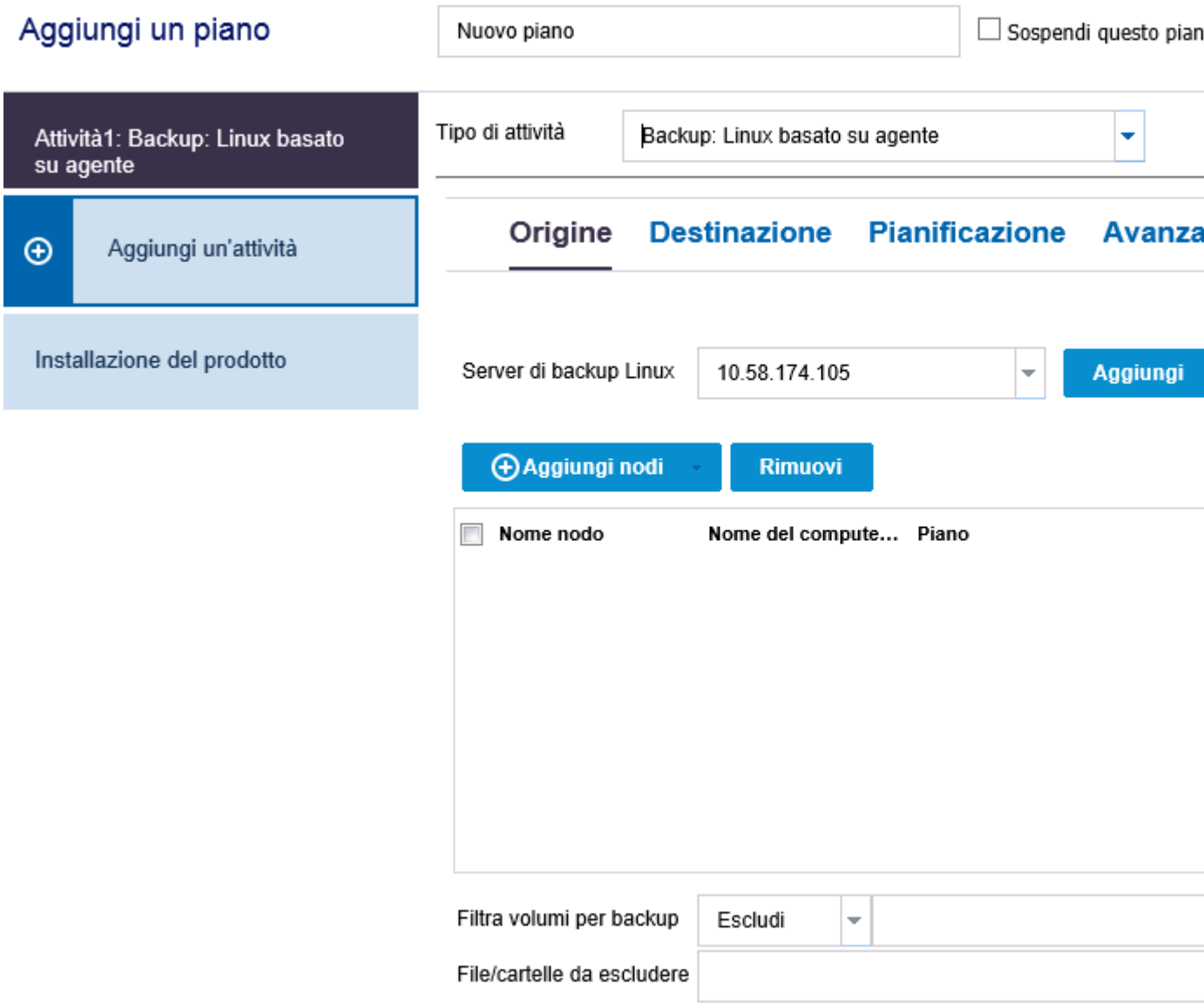
1. Accedere alla console Arcserve UDP.
2. Accedere alla scheda **Risorse** > **Piano** > **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina Aggiungi un piano.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa Tipo di attività, selezionare **Backup: Linux basato su agente**.



Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine che si desidera proteggere. È possibile selezionare più di un nodo per un piano. Se non sono stati aggiunti nodi alla Console, è possibile aggiungerli dalla pagina Origine. È possibile salvare un piano senza aggiungere i nodi di origine. Il piano non verrà comunque distribuito a meno che vengano aggiunti altri nodi.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda Origine.
2. Dall'elenco a discesa Server di backup Linux, selezionare il server di backup Linux.



3. (Facoltativo) Fare clic su **Aggiungi** per aggiungere un nuovo server di backup Linux all'elenco.
4. Fare clic su **+Aggiungi** e selezionare una delle opzioni seguenti:

   Selezionare i nodi da proteggere in Arcserve UDP

   Viene visualizzata la finestra di dialogo Selezionare i nodi da proteggere. Selezionare i nodi dall'elenco visualizzato. Selezionare questa opzione se sono stati già aggiunti nodi alla Console.

   Aggiungi nodo Linux

   Viene visualizzata la finestra di dialogo Aggiungi nodi Linux alla Console di Arcserve UDP. Selezionare questa opzione se non sono stati aggiunti nodi e si desidera aggiungere manualmente i nodi da proteggere.

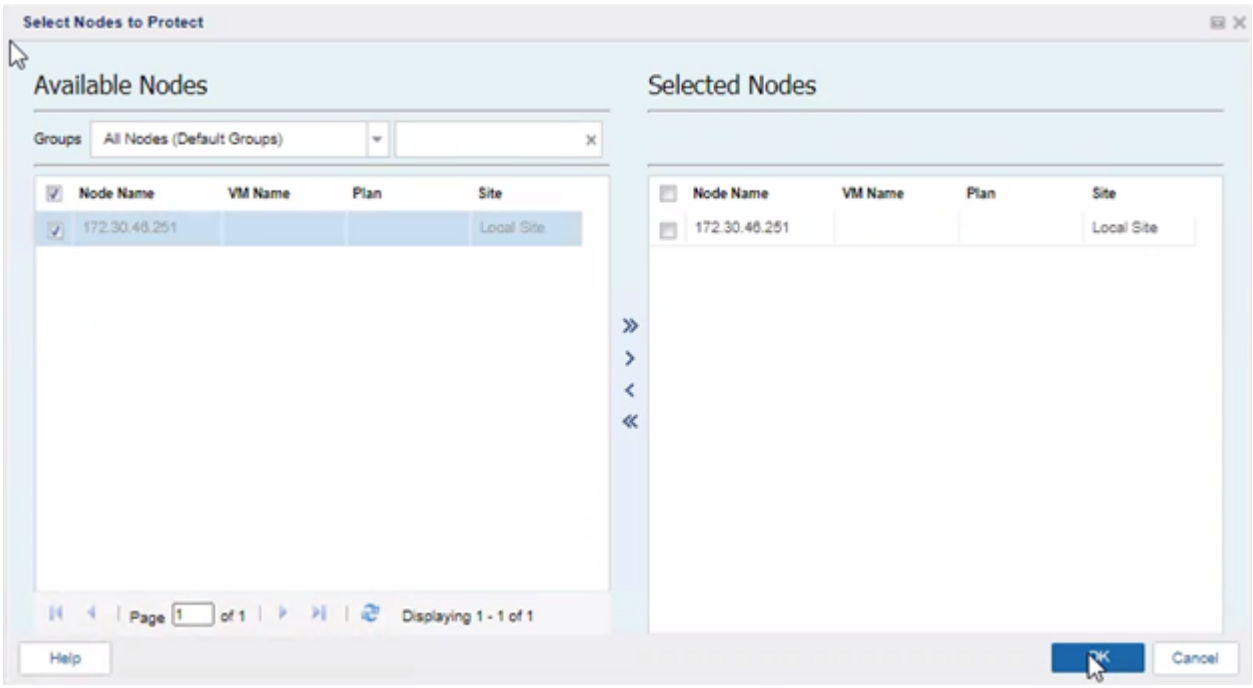
   Se selezionata, il backup del nodo di archiviazione UDP viene eseguito dal Server di backup Linux installato sul nodo stesso, anche se si seleziona manualmente un altro Server di backup Linux. Per eseguire il backup del nodo da un altro Server di backup Linux, è possibile aggiungere il nodo come nodo Linux invece di aggiungerlo come nodo di archiviazione UDP. Per ulteriori informazioni, consultare la sezione aggiunta di nodi.
5. Nella finestra di dialogo Seleziona nodi da proteggere, procedere come segue:

a. (Facoltativo) Selezionare un filtro dall'elenco a discesa Gruppi per filtrare i nodi. Immettere parole chiave per applicare ulteriori filtri ai nodi.

   I nodi vengono visualizzati nella colonna Nodi disponibili.

b. Selezionare i nodi dalla colonna Nodi disponibili, quindi fare clic sulla freccia destra e selezionare **OK**.

   I nodi selezionati vengono visualizzati nella colonna Nodi selezionati.



6. (Facoltativo) Fornire i dettagli per le opzioni seguenti:

   Filtra volumi per il backup

   Selezionare **Includi** o **Escludi** dall'elenco a discesa. L'opzione Includi consente indica che solo i volumi specificati saranno inclusi nel backup. Non verrà eseguito il backup di tutti i volumi non specificati. L'opzione Escludi specifica che i volumi verranno esclusi dal backup.

   File/cartelle da escludere

   Specificare i file e le cartelle dei nodi elencati di cui non si desidera eseguire il backup. Se non si desidera eseguire il backup di più file e cartelle, separare ciascun file e cartella mediante due punti (:). Fornire il percorso completo del file e della cartella che si desidera escludere.

7. Per la rete di backup designata, selezionare la rete tra il server di backup Linux (LBS) e il Recovery Point Server (RPS), fare clic sulla casella di controllo **Usa rete selezionata per il traffico di backup**, quindi selezionare la rete dall'elenco a discesa.

Nota: se la rete di backup selezionata non è accessibile e si desidera continuare il processo con la rete disponibile o con la rete predefinita, fare clic sulla casella di controllo **Procedere con l'esecuzione del processo anche nel caso in cui sia impossibile stabilire la connessione al CIDR selezionato**.

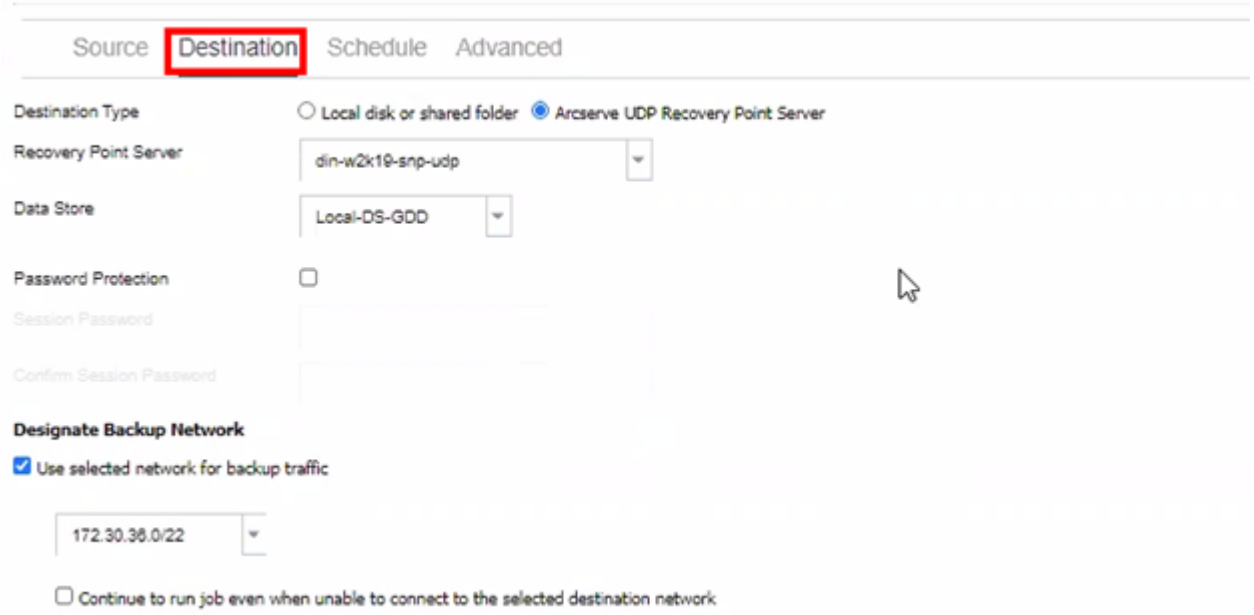
L'origine viene specificata.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Destinazione**.



2. Selezionare un tipo di destinazione tra quelli elencati di seguito:

   Disco locale o cartella condivisa

   Specifica che i dati di backup verranno archiviati in un disco locale o in una cartella condivisa.

   Recovery Point Server di Arcserve UDP

   Specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono memorizzati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.

3. Se si seleziona il **disco locale o la cartella condivisa** come tipo di destinazione, fornire i seguenti dettagli:

   - Se è stata selezionata la **condivisione NFS**, specificare i dettagli relativi alla destinazione di backup nel seguente formato:

     Indirizzo IP della condivisione NFS:/percorso completo della posizione di archiviazione

- Fare clic sul pulsante di freccia per convalidare le informazioni relative alla destinazione di backup.

  Se la destinazione di backup non è valida, verrà visualizzato un messaggio di errore.

Nota: alcune versioni di Data Domain NAS non supportano il meccanismo di blocco di file di NFS. Di conseguenza, non è possibile utilizzare la condivisione NFS come destinazione di backup. Per ulteriori informazioni su questo problema, consultare la sezione Problemi di compatibilità con Agente Arcserve Unified Data Protection per Linux.

- Se è stata selezionata la condivisione CIFS, specificare i dettagli relativi alla destinazione di backup nel seguente formato:

  //hostname/share_folder

  - Fare clic sul pulsante di freccia per convalidare le informazioni relative alla destinazione di backup.

    Se la destinazione di backup non è valida, verrà visualizzato un messaggio di errore.

  Nota: assicurarsi che il nome della cartella condivisa non contenga spazi.

- Se è stata selezionata l'opzione **Origine locale**, procedere come segue:

  a. Fornire il percorso della destinazione locale.

     Ad esempio: /root

  b. Selezionare un livello di compressione dall'elenco a discesa Compressione per specificare un tipo di compressione utilizzato per il backup.

     Le opzioni disponibili per la Compressione sono:

     Compressione standard

     Specifica un livello di compressione dall'elenco a discesa Compressione per specificare un tipo di compressione utilizzato per il backup.

     Compressione massima

     L'opzione implica un utilizzo massimo di CPU (velocità minima) ma utilizza anche una quantità minore di spazio su disco per l'immagine di backup.

  c. Selezionare un algoritmo dall'elenco a discesa Algoritmo di crittografia, quindi specificare la password di crittografia, se necessario.

d. Selezionare il tipo di algoritmo di crittografia da utilizzare per i backup.

   La crittografia dei dati corrisponde alla conversione di dati in un modulo incomprensibile senza un meccanismo di decifratura. La soluzione di protezione dei dati dell'agente Arcserve UDP (Linux) utilizza algoritmi di crittografia AES (Advanced Encryption Standard) per ottenere la massima protezione e riservatezza dei dati specificati.

   Per le opzioni del formato di crittografia disponibili, consultare la sezione Impostazioni di crittografia.

   - Il backup completo e i backup incrementali correlati devono utilizzare lo stesso algoritmo di crittografia.
   - Se l'algoritmo di crittografia per un backup incrementale è stato modificato, sarà necessario eseguire un backup completo.

   Ad esempio, se si modifica il formato dell'algoritmo e viene eseguito un backup incrementale, il tipo di backup verrà convertito automaticamente in un backup completo.

e. Nel caso in cui venga selezionato un algoritmo di crittografia, è necessario specificare e confermare una password di crittografia.

   - La password di crittografia può contenere un massimo di 23 caratteri.
   - Il backup completo e i relativi backup incrementali devono utilizzare la stessa password di crittografia.

- Se si desidera eseguire il backup su Amazon S3, procedere come segue:

  a. Selezionare la **condivisione CIFS**, quindi immettere l'archiviazione Amazon S3 nel seguente formato:

     s3://S3 Region/S3 bucket name

  b. Fare clic sulla freccia e fornire le informazioni di accesso di Amazon S3.

4. Se si seleziona il **Recovery Point Server di Arcserve UDP** come tipo di destinazione, procedere come segue:

   - Recovery Point Server: dall'elenco a discesa, selezionare il Recovery Point Server di destinazione.
   - Archivio dati: dall'elenco a discesa, selezionare l'archivio dati di destinazione.
   - Protezione password: selezionare la casella di controllo **Protezione password**, fornire la password di sessione, quindi digitare nuovamente la password per confermarla.

Nota: la password di sessione è facoltativa se la destinazione di backup è un archivio di dati RPS non crittografato.

- Per la rete di backup designata, selezionare la rete tra il server di backup Linux (LBS) e il Recovery Point Server (RPS), fare clic sulla casella di controllo **Usa rete selezionata per il traffico di backup**, quindi selezionare la rete dall'elenco a discesa.

  Nota: se la rete di backup selezionata non è accessibile e si desidera continuare il processo con la rete disponibile o con la rete predefinita, fare clic sulla casella di controllo **Procedere con l'esecuzione del processo anche nel caso in cui sia impossibile stabilire la connessione al CIDR selezionato**.

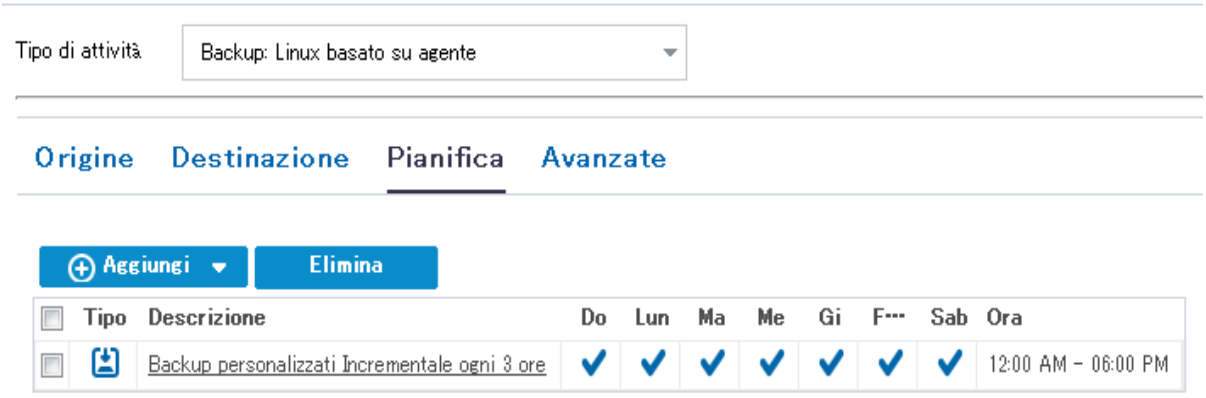
  Quando la destinazione di backup è un archivio dati di deduplicazione, il traffico riguarda direttamente il server di origine Linux e il Recovery Point Server (RPS) anche se l'opzione Specifica rete è configurata tra l'origine Linux e il server di backup Linux (LBS). Tuttavia, quando la destinazione di backup è un archivio dati non di deduplicazione, il traffico passa attraverso il server di backup Linux (LBS).

La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione di backup da ripetere a intervalli specifici. Dopo aver definito una pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione. Se la destinazione di backup corrisponde a un disco locale o una cartella condivisa, il valore predefinito è un backup incrementale personalizzato alle 22:00 ogni giorno. Se il server RPS è la destinazione di backup, il valore predefinito è un backup incrementale giornaliero alle 22:00 ogni giorno.

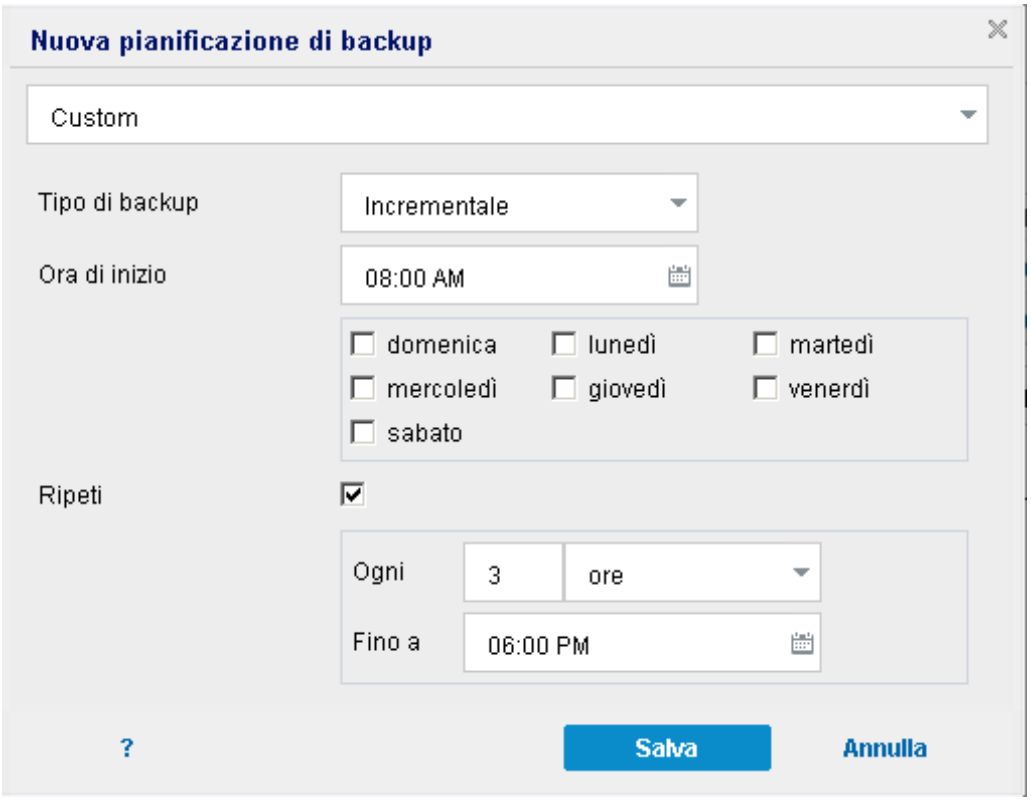
È possibile modificare o eliminare una pianificazione del processo di backup.



Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Pianificazione**.
2. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

   Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



a. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

b. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base

alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni del backup.

Verifica

Specifica la pianificazione dei backup di verifica.

Arcserve UDP controlla che i dati protetti siano validi e completi eseguendo una verifica di affidabilità dell'immagine di backup archiviata sull'origine di backup. Se necessario esegue la risincronizzazione dell'immagine. Un backup di verifica controlla il backup più recente di ogni blocco e lo confronta con il contenuto e le informazioni di origine. Questo confronto consente di verificare che il blocco di backup più recente rappresenti le informazioni corrispondenti all'origine. Se l'immagine di backup di un blocco non corrisponde all'origine (probabilmente a causa di modifiche apportate al sistema dall'ultimo backup), Arcserve UDP aggiorna (risincronizza) il backup del blocco non corrispondente. Sebbene si tratti di una procedura poco frequente, il backup di verifica può essere utilizzato per ottenere le stesse garanzie di un backup completo, ma senza occupare lo stesso spazio.

Vantaggi: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.

Svantaggi: il backup di verifica richiede tempi di esecuzione più lunghi, in quanto esegue il confronto di tutti i blocchi originali con i blocchi del backup più recente.

Incrementale

Specifica la pianificazione dei backup incrementali.

Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

c. Specificare l'ora di inizio del backup.

d. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

e. Fare clic su **Salva**.

La Pianificazione di backup viene specificata e viene visualizzata nella pagina **Pianificazione**.

3. Se la destinazione è condivisa o una cartella di rete, specificare le impostazioni di conservazione.

   Nota: per ulteriori informazioni sui set di ripristino, consultare la sezione Informazioni sui set di ripristino.

   Specificare il numero di set di ripristino da memorizzare

   Specifica il numero di set di ripristino conservati.

   Avvia un nuovo set di ripristino ad ogni:

   Giorno della settimana selezionato

   Specifica il giorno della settimana selezionato per avviare un nuovo set di ripristino.

   Giorno del mese selezionato

   Specifica il giorno del mese selezionato per avviare un nuovo set di ripristino. Specificare un valore da 1 a 31 oppure l'ultimo giorno del mese.

   Nota: Il server di backup Linux verifica ogni 15 minuti il numero di set di ripristino nell'archiviazione di backup configurata ed elimina eventuali set di ripristino aggiuntivi dal percorso di archiviazione del backup.

4. Se è stato selezionato il Recovery Point Server di Arcserve come destinazione, attenersi alla seguente procedura.

   Aggiunta di una pianificazione di unione

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di unione**.

      La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

   b. Specificare l'ora di inizio per l'avvio del processo di unione.

   c. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

   d. Fare clic su **Salva**.

      La Pianificazione di unione viene specificata e viene visualizzata nella pagina **Pianificazione**.

   Aggiungi pianificazione del limite delle risorse

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

      Viene visualizzata la finestra di dialogo Aggiungi nuova pianificazione del limite delle risorse.

   b. Specificare il limite di velocità effettiva in MB per unità di minuti.

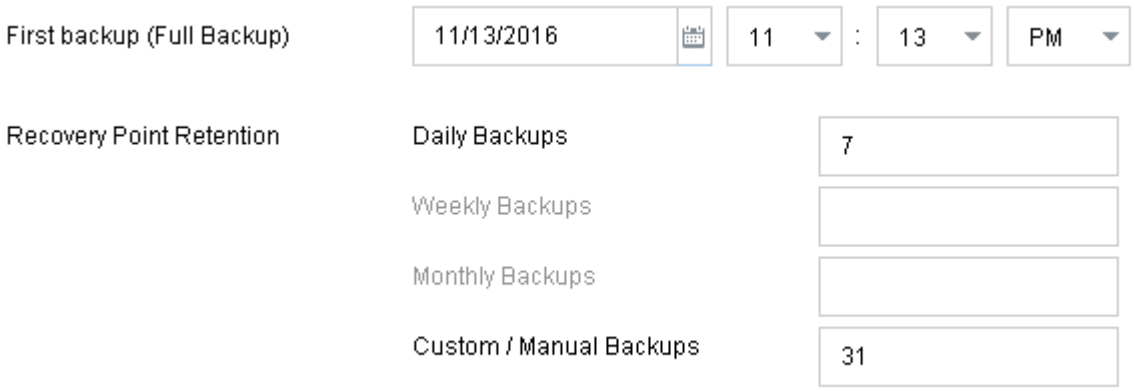
c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

La pianificazione del limite delle risorse viene specificata e viene visualizzata nella pagina **Pianificazione**.

5. Specificare l'ora di inizio per il backup pianificato.



6. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo Pianificazione di backup.

Viene specificata la pianificazione di backup.

Informazioni sui set di ripristino

Un set di ripristino è un'impostazione di archiviazione in cui un gruppo di punti di ripristino viene sottoposto a backup per un periodo di tempo specificato e memorizzato come un singolo set. Un set di ripristino contiene una serie di backup, a partire da un backup completo seguito da backup incrementali, di verifica o completi. È possibile specificare il numero di set di ripristino da memorizzare.

Le **Impostazioni del set di ripristino** garantiscono un mantenimento periodico dei set di ripristino. Quando il limite specificato viene superato, il set di ripristino meno recente viene eliminato. I valori seguenti definiscono i set di ripristino predefiniti, minimi e massimi nell'Agente Arcserve Unified Data Protection per Linux:

Impostazione predefinita: 2

Minimo: 1

Numero massimo di set di ripristino: 100

Nota: Per eliminare un set di ripristino e disporre di uno spazio di archiviazione maggiore per il backup, ridurre il numero di set memorizzati in modo che il server di backup elimini automaticamente il set di ripristino meno recente. Non tentare di eliminare il set di ripristino manualmente.

Set 1 di esempio:

- Completo
- Incrementale
- Incrementale
- Verifica
- Incrementale

Set 2 di esempio:

- Completo
- Incrementale
- Completo
- Incrementale

È necessario un backup completo per avviare un nuovo set di ripristino. Il backup di avvio del set verrà convertito automaticamente in un backup completo, incluso nel caso in cui l'esecuzione del backup completo non sia stata configurata né pianificata. Dopo aver modificato l'impostazione del set di ripristino (ad esempio, il punto di avvio del set di ripristino è stato modificato dal primo backup di lunedì al

primo backup di giovedì), il punto di avvio dei set di ripristino esistenti non verrà modificato.

Nota: I set di ripristino incompleti non vengono inclusi nel calcolo del set di ripristino esistente. Un set di ripristino viene considerato completo solo in seguito alla creazione del backup di avvio del set di ripristino successivo.

Esempio 1 - Memorizzazione di 1 set di ripristino:

- Specificare 1 come numero dei set di ripristino da memorizzare.

  Il server di backup memorizza sempre due set in modo da avere un set completo prima dell'avvio del set di ripristino successivo.

Esempio 2 - Memorizzazione di 2 set di ripristino:

- Specificare 2 come numero dei set di ripristino da memorizzare.

  Il server di backup elimina il primo set di ripristino quando il quarto set di ripristino sta per iniziare. In questo modo, quando il primo backup viene eliminato e il quarto è in fase di avvio, restano disponibili sul disco ancora due set di ripristino (il set di ripristino 2 e 3).

  Nota: Anche se si sceglie di memorizzare un solo set di ripristino, è necessario disporre di spazio sufficiente per almeno due backup completi.

Esempio 3 - Memorizzazione di 3 set di ripristino:

- La data/ora di inizio del backup è 06:00 del 20 agosto 2012.
- Ogni 12 ore viene eseguito un backup incrementale.
- Un nuovo set di ripristino verrà avviato venerdì. Per impostazione predefinita, il primo processo di backup del venerdì rappresenta l'inizio del nuovo set di ripristino.
- Si desidera memorizzare 3 set di ripristino.

  In base alla configurazione delineata, ogni giorno viene eseguito un backup incrementale alle 06:00 e alle 18:00. Il primo set di ripristino viene creato una volta eseguito il primo backup (deve essere un backup completo). Il primo backup completo viene quindi contrassegnato come backup di avvio del set di ripristino. Durante l'esecuzione del backup pianificato alle 06:00 di venerdì, questo viene convertito in un backup completo e contrassegnato come backup di avvio del set di ripristino.

  Nota: Se si desidera eseguire il processo di backup ripetutamente fino al termine della giornata, impostare la pianificazione fino alle 00:00. Ad esempio, per eseguire un processo di backup ogni 15 minuti per l'intera giornata, impostare la pianificazione dalle 00:00 alle 00:00 ogni 15 minuti.

Definizione delle impostazioni avanzate

Utilizzando la scheda Avanzate, specificare alcune impostazioni aggiuntive per il processo di backup comprese le impostazioni della velocità effettiva del backup e dello script pre/post backup.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Avanzate**.
2. Specificare il limite di velocità del backup.

   L'operazione può essere eseguita solo se la destinazione di backup è un disco locale o una cartella condivisa.

   È possibile specificare la velocità massima di scrittura (MB/min) del backup. e di limitare la velocità di backup per ridurre l'utilizzo della CPU o della rete. Tuttavia, la limitazione della velocità di backup potrebbe influire sul tempo di completamento del processo di backup. Con una velocità di backup inferiore, il tempo di completamento del backup aumenta.

   Nota: per impostazione predefinita, l'opzione Limite delle risorse di backup non è attivata e la velocità di backup non viene controllata.
3. Specificare le impostazioni di pre e post-backup in **Impostazioni script pre/post backup**.

   Questi script eseguono comandi di script per le azioni da eseguire prima dell'inizio del processo e/o al completamento del processo.

   Nota: i campi Impostazioni script pre/post backup vengono popolati solo se un file di script è già stato creato e posizionato nel percorso seguente del server di backup di Linux:

   /opt/Arcserve/d2dserver/usr/prepost

   Nota: per ulteriori informazioni sulla creazione di pre/post script, consultare la sezione *Gestione di pre/post script per l'automazione*.
4. Fare clic su Abilita avvisi di posta elettronica per specificare le impostazioni di posta elettronica, quindi fare clic su Avvisi sui processi.

   L'operazione può essere eseguita solo se la destinazione di backup corrisponde al Recovery Point Server di Arcserve.
5. Fare clic su **Salva**.

   Le modifiche vengono salvate.

   Il piano di backup viene creato e distribuito automaticamente al nodo di origine. Il backup viene eseguito in base alla pianificazione configurata nella scheda

Pianificazione. È possibile eseguire anche un backup manuale in qualsiasi momento.

A questo punto, è possibile aggiungere le seguenti attività al piano:

- Replica
- Replica in un Recovery Point Server gestito remotamente
- Copia su nastro

(Facoltativo) Gestione di pre/post script per l'automazione

Gli script di pre/post esecuzione consentono di eseguire regole di business in fasi specifiche di un processo in esecuzione. È possibile specificare quando eseguire gli script nelle **Impostazioni pre/post script** della **Procedura guidata di backup** e della **Procedura guidata di ripristino** nella console. È possibile eseguire gli script sul server di backup in base alle impostazioni dell'utente.

La gestione del pre/post script è un processo costituito da due passaggi: la creazione del pre/post script e la sua collocazione nella cartella prepost.

Creazione di pre/post script

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare un file di script mediante le variabili di ambiente nel linguaggio di scripting preferito.

Variabili di ambiente del pre/post script

Per creare lo script, utilizzare le variabili di ambiente seguenti:

D2D_JOBNAME

Indica il nome del processo.

D2D_JOBID

Identifica l'ID del processo. L'ID di processo è un numero attribuito al processo durante la sua esecuzione. Se si esegue lo stesso processo nuovamente, verrà fornito un nuovo numero di processo.

D2D_TARGETNODE

Identifica il nodo di cui viene eseguito il backup o il ripristino.

D2D_JOBTYPE

Identifica il tipo di processo in esecuzione. I valori seguenti identificano la variabile D2D_JOBTYPE:

backup.full

Identifica il processo come backup completo.

backup.incremental

Identifica il processo come backup incrementale.

backup.verify

Identifica il processo come backup di verifica.

restore.bmr

Identifica il processo come ripristino bare metal (BMR). Si tratta di un processo di ripristino.

restore.file

Identifica il processo come ripristino a livello di file. Si tratta di un processo di ripristino.

D2D_SESSIONLOCATION

Identifica la posizione in cui vengono archiviati i punti di ripristino.

D2D_PREPOST_OUTPUT

Identifica un file temp. Il contenuto della prima linea del file temp viene visualizzato nel registro attività.

D2D_JOBSTAGE

Indica la fase del processo. I valori seguenti identificano la variabile D2D_ JOBSTAGE:

pre-job-server

Identifica lo script eseguito sul server di backup prima dell'avvio del processo.

post-job-server

Identifica lo script eseguito sul server di backup dopo il completamento del processo.

pre-job-target

Identifica lo script eseguito sul computer di destinazione prima dell'avvio del processo.

post-job-target

Identifica lo script eseguito sul computer di destinazione dopo il completamento del processo.

pre-snapshot

Identifica lo script eseguito sul computer di destinazione prima dell'acquisizione della snapshot.

post-snapshot

Identifica lo script eseguito sul computer di destinazione dopo l'acquisizione della snapshot.

D2D_TARGETVOLUME

Identifica il volume di cui viene eseguito il backup durante un processo di backup. Questa variabile è adatta per gli script di snapshot di pre/post automazione per un processo di backup.

D2D_JOBRESULT

Identifica il risultato di uno script del processo di post-esecuzione. I valori seguenti identificano la variabile di D2D_JOBRESULT:

success

Identifica il risultato come corretto.

fail

Identifica il risultato come non corretto.

D2DSVR_HOME

Identifica la cartella in cui è installato il server di backup. È possibile applicare la variabile agli script in esecuzione sul server di backup.

Lo script viene creato.

Nota: per tutti gli script, un valore restituito pari a zero indica un'operazione riuscita, mentre un valore restituito diverso da zero indica la presenza di un errore.

Collocare lo script nella cartella prepost ed eseguire la verifica

Tutti gli script di pre/post per un server di backup sono gestiti centralmente dalla cartella prepost nella posizione seguente:

/opt/Arcserve/d2dserver/usr/prepost

Effettuare le operazioni seguenti:

1. Collocare il file nella posizione seguente del server di backup:

   /opt/Arcserve/d2dserver/usr/prepost

2. Fornire le autorizzazioni di esecuzione per il file di script.
3. Accedere all'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux.
4. Aprire la procedura guidata di **backup** o **ripristino** ed accedere alla scheda **Impostazioni avanzate**.
5. Selezionare il file di script nell'elenco del menu a discesa **Impostazioni di pre/post script**, quindi inviare il processo.
6. Fare clic sul **Registro attività** e verificare che lo script venga eseguito per il pro-

cesso di backup specificato.

Lo script viene eseguito.

I pre/post script vengono creati correttamente e inseriti nella cartella prevista.

(Facoltativo) Esecuzione di un backup manuale

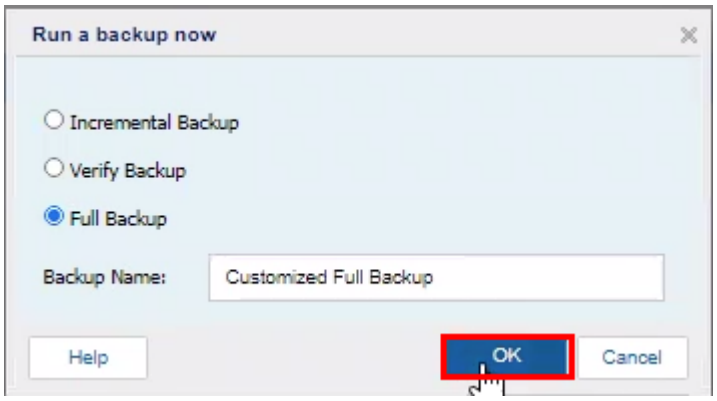
In genere, i backup vengono eseguiti automaticamente e vengono controllati attraverso le impostazioni di pianificazione. In aggiunta al backup pianificato, un backup manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze. Ad esempio, se si dispone di una pianificazione di ripetizione per backup completi, incrementali e di verifica e si desidera apportare modifiche sostanziali al computer, sarà necessario eseguire un backup manuale immediato senza attendere l'esecuzione del successivo backup pianificato.

Effettuare le operazioni seguenti:

1. Accedere alla console Arcserve UDP.
2. Accedere a **Risorse** > **Piano** > **Tutti i piani**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i piani.
3. Fare clic con il pulsante destro del mouse sul piano, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
4. Nella finestra di dialogo Esegui backup immediato, selezionare il tipo di backup che si desidera eseguire, quindi specificare il nome del backup, se necessario.



Le opzioni disponibili sono:

Backup incrementale

Avvia un backup incrementale del computer. Un backup incrementale esegue il backup solo dei blocchi modificati dopo l'ultimo backup.

Nota: se si esegue un backup per la prima volta, il backup completo viene avviato automaticamente anche se è stata selezionata l'opzione Backup incrementale.

I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup con dimensioni molto ridotte. Questa modalità di esecuzione backup è ottimale.

Backup di verifica

Avvia un backup di verifica individuando il backup più recente di ciascun blocco e ne confronta il contenuto e le informazioni con l'origine. Questo confronto consente di verificare che il blocco di backup più recente rappresenti le informazioni corrispondenti all'origine. Se l'immagine di backup di un blocco non corrisponde all'origine, l'agente Arcserve UDP (Windows) aggiornerà (risincronizzerà) il backup di tale blocco.

Vantaggi: viene prodotta un'immagine di backup di dimensioni molto ridotte rispetto al backup completo, poiché viene eseguito solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono all'ultimo backup.

Svantaggi: la velocità del backup è ridotta poiché tutti i blocchi del disco di origine vengono confrontati con i blocchi dell'ultimo backup.

Backup completo

Avvia un backup completo dell'intero computer o dei volumi selezionati.

Note:

- Se si aggiunge un nuovo volume all'origine di backup, il volume appena aggiunto verrà sottoposto a un backup completo, indipendentemente dal metodo di backup generale utilizzato.
- Se non viene specificato alcun nome di backup, per impostazione predefinita viene automaticamente denominato Backup completo personalizzato/Incrementale/Di verifica.

5. Fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.

6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.

7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Nota: è possibile eseguire un solo processo alla volta. Se si tenta di avviare manualmente un processo di backup durante l'esecuzione di un altro processo, verrà visualizzato un messaggio di avviso indicante che un altro processo è in esecuzione, per cui sarà necessario riprovare in un momento successivo.

   Il backup manuale è stato eseguito correttamente.

Verifica del backup

Per verificare il backup, confermare di avere creato correttamente il piano di backup. Dopo avere verificato che il piano è stato creato correttamente, confermare se il processo di backup è in esecuzione secondo quanto pianificato. È possibile verificare lo stato dei processi di backup dalla scheda Processi.

Effettuare le operazioni seguenti: per la verifica dei piani

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Attenersi a uno di questi metodi per verificare i processi di backup.

Metodo 1

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Tutti i Processi**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Metodo 2

1. Dalla console Arcserve UDP, accedere alla scheda **Processi** > **Processi completati correttamente**.

   L'elenco dei processi di backup completati viene visualizzato nel riquadro centrale.
2. Fare clic sul processo di replica inversa completato. Il riquadro destro viene aggiornato.
3. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
4. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Il processo di backup viene verificato.

Risoluzione dei problemi

Lo stato del processo, la cronologia del processo, e il Registro attività non sono visibili

Lo stato del processo, la cronologia del processo e il Registro attività non sono visibili

Sintomo

Non è possibile visualizzare lo stato del processo, la cronologia del processo e il registro attività per i nodi Linux della console Arcserve UDP.

Soluzione

Il server di backup Linux non è in grado di connettersi a Arcserve UDP mediante il nome host.

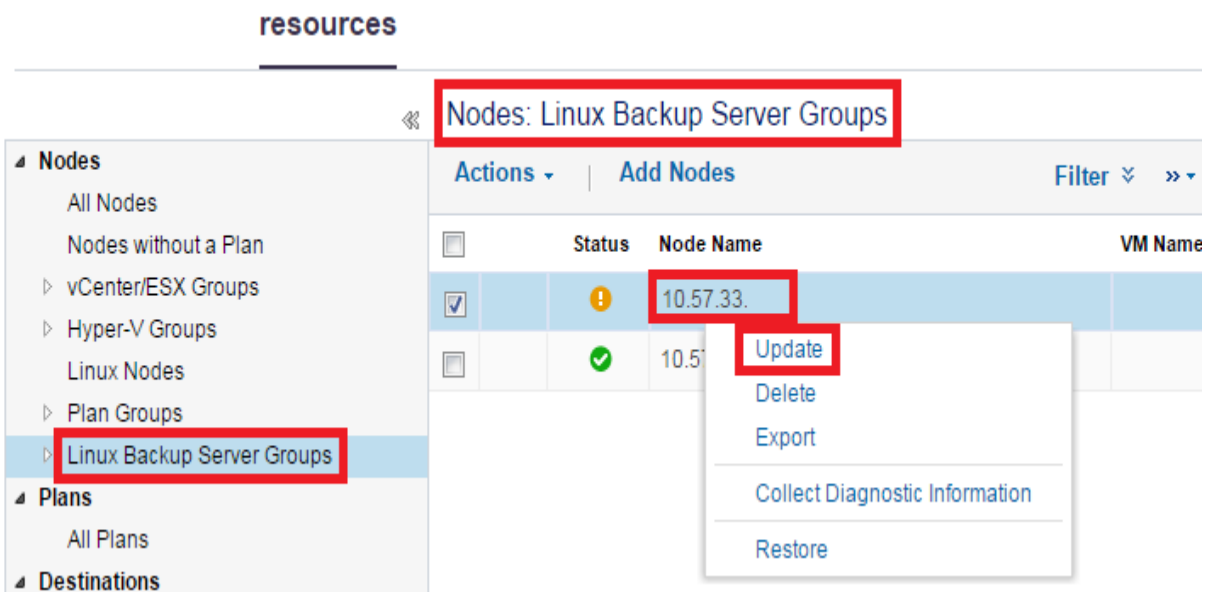
Effettuare le operazioni seguenti:

1. Creare il file server_ip.ini nel seguente percorso di Arcserve UDP:

   "UDP installation path"\Management\Configuration\server_ip.ini

2. Immettere l'indirizzo IP di Arcserve UDP nel file.
3. Accedere alla console Arcserve UDP e aggiornare il server di backup Linux e i nodi Linux.

   Nota: il server di backup Linux può essere aggiornato solamente da gruppi di server di backup Linux, in cui vengono elencati tutti i server di backup Linux.



Lo stato del processo, la cronologia del processo e il Registro attività sono visibili.

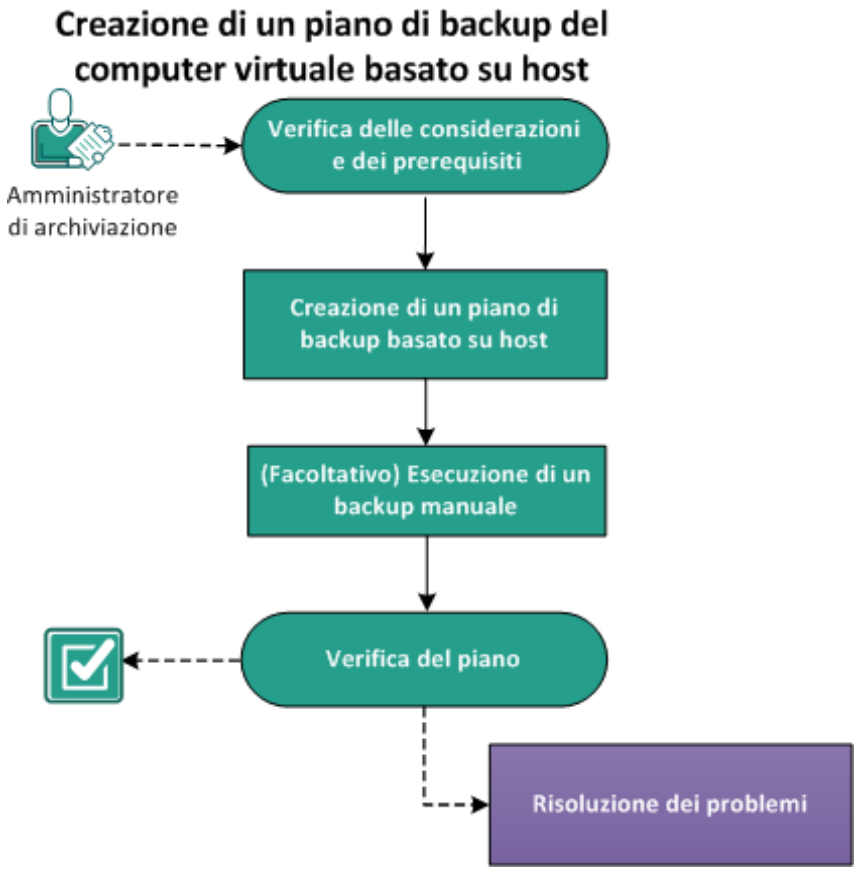
Creazione di un piano di backup del computer virtuale basato su host

Per proteggere i nodi di un computer virtuale basato su host, è necessario creare un piano di backup basato su host. Un piano di backup per i nodi di un computer virtuale basato su host consiste in un'attività di backup. Questa attività di backup consente di specificare i nodi che si desidera proteggere, la destinazione di backup e la pianificazione del backup. La destinazione di backup può essere una destinazione locale o una cartella di condivisione remota oppure il Recovery Point Server in cui archiviare i dati di backup.

È possibile eseguire anche il backup di database Oracle, SQL Server e Exchange Server. Per eseguire il backup dei database Oracle, devono essere soddisfatti requisiti specifici. Per eseguire il backup di SQL Server ed Exchange Server non è richiesto alcun prerequisito. Verificare i prerequisiti seguenti per eseguire un backup compatibile con le applicazioni di un database Oracle:

- Prerequisito per creare un backup compatibile con le applicazioni di un database Oracle

Il diagramma seguente illustra il processo di protezione dei nodi del computer virtuale basato su host.



Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di un piano di backup basato su host
3. (Facoltativo) Esecuzione di un backup manuale
4. Verifica del piano
5. Risoluzione dei problemi

Verifica delle considerazioni e dei prerequisiti

Verificare se i prerequisiti seguenti sono stati completati:

- Accedere alla console.
- Preparare un server proxy di backup basato su host dove è stato installato Agente Arcserve Unified Data Protection per Windows.
- Per eseguire funzioni come la verifica preliminare, i comandi pre/post script o l'eliminazione del registro dell'applicazione, aggiornare il computer virtuale nella visualizzazione dell'elenco dei nodi della Console di Arcserve UDP con una delle credenziali seguenti per il computer virtuale guest:
  - Credenziali dell'utente amministratore integrate.
  - Credenziali dell'utente amministratore di dominio integrate.
  - Per le altre credenziali di amministratore, disabilitare l'opzione di controllo dell'account utente (UAC) sul computer virtuale guest.
- Per poter eseguire un ripristino a livello di database (per Exchange e SQL Server) o un ripristino a livello granulare (Exchange) in seguito a un backup, è necessario soddisfare i prerequisiti seguenti:
  - Il computer virtuale deve supportare il backup coerente con le applicazioni. Per ulteriori informazioni sui backup coerenti con le applicazioni, consultare le sezioni Creazione di snapshot coerenti con l'applicazione per VMware o Creazione di snapshot coerenti con l'applicazione per Hyper-V.
  - Per i computer virtuali VMware VM, nel piano di backup è necessario utilizzare il metodo di disattivazione della snapshot di **Strumenti VMware**.
  - Per i computer virtuali Hyper-V, Arcserve UDP deve distribuire automaticamente un'utilità nel sistema operativo guest del computer virtuale per raccogliere i metadati dell'applicazione durante un backup. Il sistema operativo guest del computer virtuale deve essere accessibile dal server proxy di backup o dall'host Hyper-V mediante la rete. Allo stesso tempo, è necessario aggiornare il nodo del computer virtuale con le credenziali di amministratore appropriate nella visualizzazione dell'elenco dei nodi della Console di Arcserve UDP. Se per determinate ragioni il sistema operativo guest del computer virtuale non è accessibile dal server proxy di backup e dall'host Hyper-V, attenersi alla seguente procedura per installare manualmente l'utilità sul sistema operativo guest del computer virtuale:

a. Accedere al server proxy di backup e aprire la cartella seguente:

   <Arcserve UDP installation path>\Engine\BIN (Esempio: C:\P-rogrammi\Arcserve\Unified Data Protection\Engine\BIN)

b. Individuare il file eseguibile **VMICService_32.exe** o **VMICService_64.exe**.

c. Copiare il file eseguibile in una cartella qualsiasi nel sistema operativo guest del computer virtuale. (Per un sistema operativo a 32 bit, copiare **VMICService_32.exe**, in caso contrario copiare **VMICService_64.exe**).

   Ad esempio, è possibile creare un'immagine ISO includendo questo file eseguibile e montarla nella periferica DVD del computer virtuale.

d. Accedere al sistema operativo guest del computer virtuale ed eseguire **VMICService_32.exe-install** o **VMICService_64.exe-install**.

- Installare il componente server e creare gli archivi dati qualora si desideri archiviare i dati di backup nel Recovery Point Server.
- Verificare i prerequisiti per eseguire il backup di un database Oracle.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

I seguenti prerequisiti valgono per le snapshot hardware:

Per Hyper-V

- Installare un provider hardware VSS sui server Hyper-V e, per supportare la snapshot trasportabile, installare il provider hardware VSS sul server proxy di backup. La configurazione tipica di un provider hardware VSS include:
  - Definizione di un server che controlla la LUN.
  - Definizione delle credenziali dell'array di dischi per accedere all'array di dischi.

  Per ulteriori informazioni sulla configurazione del provider di hardware VSS, contattare il rivenditore del provider hardware.
- Il server Hyper-V e il server proxy devono disporre di una versione del sistema operativo simile.
- Se il server Hyper-V è compreso in un cluster, il server proxy non deve far parte del cluster Hyper-V.
- Disinstallare CBT di UDP da Programmi e funzionalità nel pannello di controllo dell'host Hyper-V.

Per VMware

- Arcserve UDP supporta le LUN NetApp iSCSI e NetApp NFS.
- Per creare una snapshot hardware per VMware, aggiungere l'array di archiviazione alla console. Per ulteriori informazioni sull'aggiunta di un array di archiviazione, consultare la sezione Aggiunta di un array di archiviazione.
- Per utilizzare la snapshot hardware, gli array di archiviazione NetApp in esecuzione con Data ONTAP in 7-Mode e in modalità cluster, necessitano della licenza FlexClone.

Considerazioni sul backup del computer virtuale:

- **Impatto della deframmentazione del volume sui backup continui**

  La deframmentazione del volume mediante lo strumento nativo di Windows influisce sulle dimensioni dei backup a livello di blocco poiché Arcserve UDP procede con il backup incrementale di tutti i blocchi modificati. Ciò significa che i blocchi spostati durante la deframmentazione sono inclusi nel backup, anche nel caso in cui non siano stati modificati dati nei file. Di conseguenza, le dimensioni del backup aumentano. Si tratta di un comportamento normale.

- **Protezione dei computer virtuali in Hyper-V 2016 mediante Windows Resilient Change Tracking**

  Per proteggere il computer virtuale in Hyper-V 2016, si consiglia di utilizzare Windows Resilient Change Tracking (RCT) per il backup incrementale. Arcserve UDP utilizza automaticamente Windows Resilient Change Tracking (RCT) durante il backup di computer virtuali con la configurazione della versione 8.0 (o versioni successive) in esecuzione sull'host/cluster Hyper-V 2016. Se l'Hyper-V viene aggiornato dalla versione precedente, aggiornare la configurazione del computer virtuale utilizzando anche la Documentazione di Microsoft. Al completamento dell'aggiornamento per tutti i computer virtuali protetti da Arcserve UDP, si consiglia di disinstallare il servizio CBT di Arcserve UDP dall'host Hyper-V.

Considerazioni sul backup di rete specifico:

- Hypervisor, Windows Proxy e RPS devono trovarsi nella stessa rete.
- Se ESXi viene aggiunto con il **nome host** a vCenter, la selezione della rete di backup deve essere la rete predefinita di ESXi.

  Nota: la rete predefinita corrisponde alla rete risolta da DNS.

- Se ESXi viene aggiunto con l'indirizzo IP a vCenter, la selezione della rete di backup deve corrispondere a quella utilizzata da ESXi per connettersi a vCenter.

Scenario #	Ha vCenter	Elementi utilizzati per l'aggiunta a vCenter	Potrebbe utilizzare la rete di backup?	La risoluzione temporanea di DNS o dei file host è funzionante?
1	No	N/D	Sì	N/D
2	Sì	Nome host di ESXi: l'indirizzo IP di produzione del nome host viene risolto	No	Sì. Aggiornare il DNS o i file host sul server proxy.
3	Sì	Nome host di ESXi: l'indirizzo IP della rete di backup del nome host viene risolto	Sì	N/D
4	Sì	IP di produzione di ESXi	No	No
5	Sì	IP di rete di backup di ESXi	Sì	N/D

Revisione dei prerequisiti per eseguire il backup compatibile con le applicazioni di un database Oracle

Per eseguire il backup di un database Oracle con dati coerenti, verificare che la modalità ARCHIVELOG sia abilitata per archiviare i registri Redo.

Nota: il volume di dati deve includere file di dati Oracle, file di controllo, file di parametro del server e registri di ripristino in linea. I registri di ripristino archiviati devono trovarsi fisicamente in un volume separato.

Attenersi alla seguente procedura per verificare che la modalità ARCHIVELOG sia abilitata:

a. Accedere come utente Oracle con privilegi SYSDBA al server Oracle.

b. Al prompt SQL*Plus, immettere il seguente comando:

   ARCHIVE LOG LIST;

   Vengono visualizzate le impostazioni Archive log per l'istanza corrente.

c. Configurare le impostazioni seguenti:

   Database log mode: Archive Mode

   Automatic archival: Enabled

d. Avviare la modalità ARCHIVELOG.

   Nota: se non è attivata la modalità ARCHIVELOG, avviare la modalità ARCHIVELOG per eseguire il backup del database.

Completare le operazioni seguenti per avviare la modalità ARCHIVELOG:

a. Chiudere Oracle Server.

b. Eseguire le istruzioni sotto riportate in Oracle:

   CONNECT SYS/SYS_PASSWORD AS SYSDBA

   STARTUP MOUNT;

   ALTER DATABASE ARCHIVELOG;

   ALTER DATABASE OPEN;

   Per impostazione predefinita, i registri di archivio verranno scritti nell'area di ripristino flash. Se non si desidera scrivere i registri di archivio nell'area di ripristino flash, è possibile impostare il parametro LOG_ARCHIVE_DEST_n nella posizione in cui scrivere i registri di archivio.

   SQL>ALTER SYSTEM SET LOG_ARCHIVE_DEST_
   1='LOCATION=e:\app\administrator\oradata\<oracle_database_name>\arch'
   SCOPE= BOTH;

Sistema modificato.

SQL> ARCHIVE LOG LIST;

Vengono visualizzate le impostazioni Archive log per l'istanza corrente.

c. Configurare le impostazioni seguenti:

Database log mode: Archive Mode

Automatic archival: Enabled

Archive destination: E:\app\oracle\oradata\<oracle_database_name>\arch

Oldest online log sequence: 21

Current log sequence: 23

Il servizio di scrittura Oracle VSS viene avviato correttamente.

Creazione di un piano di backup basato su host

Un piano di backup include un'attività di backup che esegue un backup del computer virtuale e archivia i dati nella destinazione specificata. Ciascuna attività consiste di parametri che definiscono l'origine, la destinazione, la pianificazione, e altri dettagli di backup.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

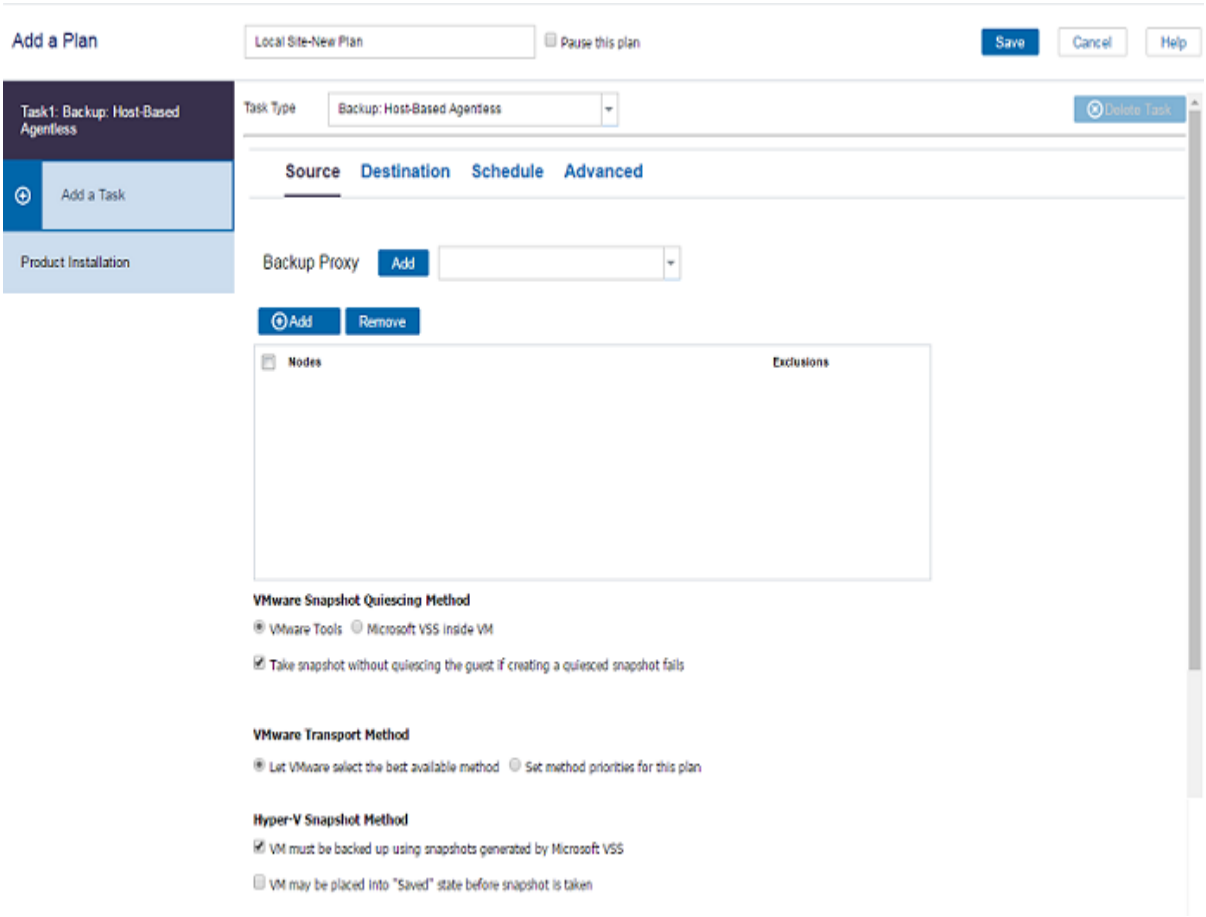
   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la finestra di dialogo **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa **Tipo di attività**, selezionare **Backup, basato su host senza**

agente.



Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine che si desidera proteggere. È possibile selezionare più di un nodo per un piano. Se non sono stati aggiunti nodi alla console, è possibile aggiungerli in fase di creazione o modifica di un piano dalla pagina Origine. È possibile salvare un piano senza aggiungere nessun nodo di origine. Il piano viene distribuito soltanto dopo l'aggiunta dei nodi di origine.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Origine** e aggiungere un server proxy di backup.

   Il server proxy è un nodo in cui si installa l'Agente Arcserve Unified Data Protection per Windows. Se l'agente non è installato su questo server proxy, l'agente viene distribuito al server proxy durante il salvataggio del piano. L'impostazione di distribuzione dell'agente si trova nell'attività Installazione agente nel piano.

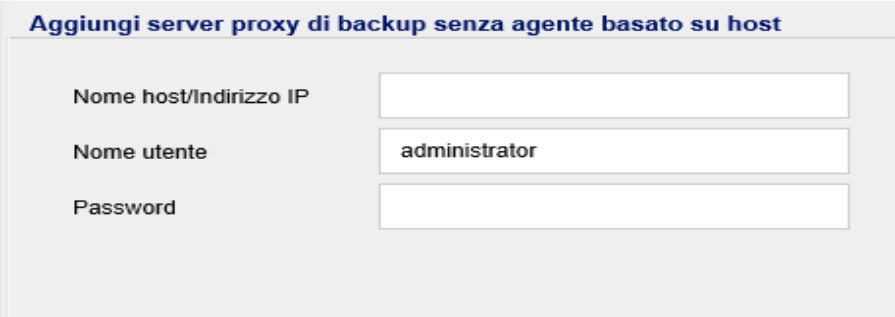
   - Se il proxy di backup è già stato aggiunto, selezionarlo dall'elenco a discesa.

   - In caso contrario, fare clic su **Aggiungi**.

     Viene visualizzata la finestra di dialogo **Aggiungi server proxy di backup senza agente basato su host**.

     Specificare i dettagli del server proxy, quindi fare clic su **OK**.

   Non è necessario aggiungere il numero di porta e il protocollo. Il numero di porta e il protocollo vengono configurati nella scheda delle **impostazioni** della console.

   Nota: la distribuzione del piano non riesce quando lo si modifica tramite il cambiamento del proxy di backup, ma sono presenti dei processi in esecuzione per i nodi inclusi nel piano. Attenersi alla procedura seguente per modificare il proxy di un piano:

a. Interrompere il piano.

b. Attendere finché tutti i nodi del piano non completino i processi di backup in esecuzione (in alternativa, è possibile annullare tali processi in esecuzione).

c. Modificare il proxy del piano e salvarlo.

d. Riprendere il piano.

2. Fare clic su **Aggiungi nodi** per selezionare una delle opzioni seguenti e aggiungere i nodi da sottoporre a backup:

Selezionare i nodi da proteggere

Consente di aprire la finestra di dialogo **Selezionare i nodi da proteggere** in cui è possibile scegliere i nodi dall'elenco visualizzato. Selezionare questa opzione se sono stati già aggiunti nodi alla Console.

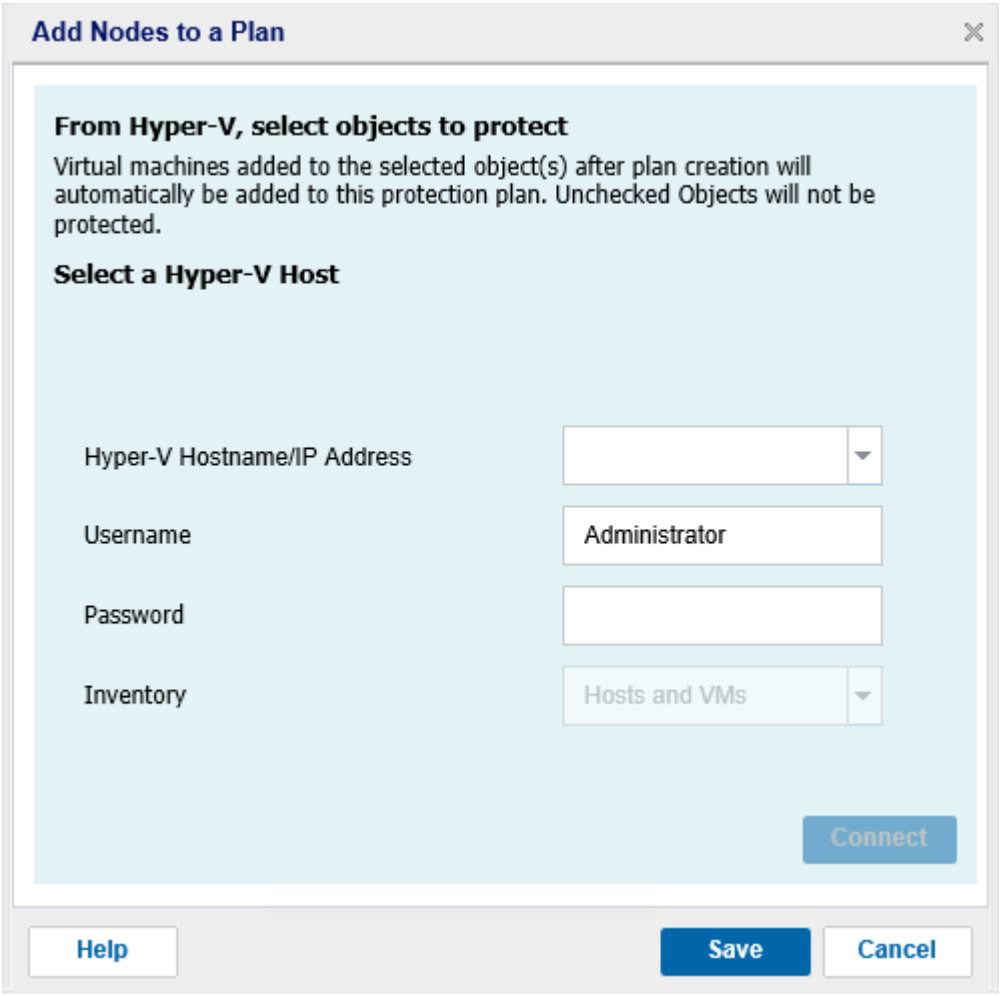
Aggiunta di nodi da un server Hyper-V

Consente di aprire la finestra di dialogo **Aggiungi nodi alla Console Arcserve UDP**. È possibile aggiungere a un piano singoli nodi del computer virtuale, oppure oggetti contenitore (compreso il cluster Hyper-V, l'host Hyper-V e la posizione di archiviazione). Dopo aver aggiunto un oggetto contenitore del computer virtuale al piano, il piano protegge automaticamente tutti i computer virtuali assegnati. Se viene creato un nuovo computer virtuale nell'oggetto contenitore del computer virtuale oppure viene spostato nell'oggetto contenitore del computer virtuale da un'altra posizione, Arcserve UDP protegge il computer virtuale senza intervento manuale. Se il computer virtuale viene eliminato dall'oggetto contenitore del computer virtuale (o spostato all'esterno dell'oggetto contenitore del computer virtuale), Arcserve UDP interrompe la protezione del computer virtuale.

Per aggiungere un oggetto contenitore del computer virtuale a un piano, procedere come segue:

a. Specificare i dettagli del server Hyper-V, selezionare la modalità di rilevamento dei computer virtuali nella casella di selezione a discesa (Host e computer virtuali, Archivi e computer virtuali), quindi fare clic su Connetti.

Viene visualizzata una struttura gerarchica Hyper-V.

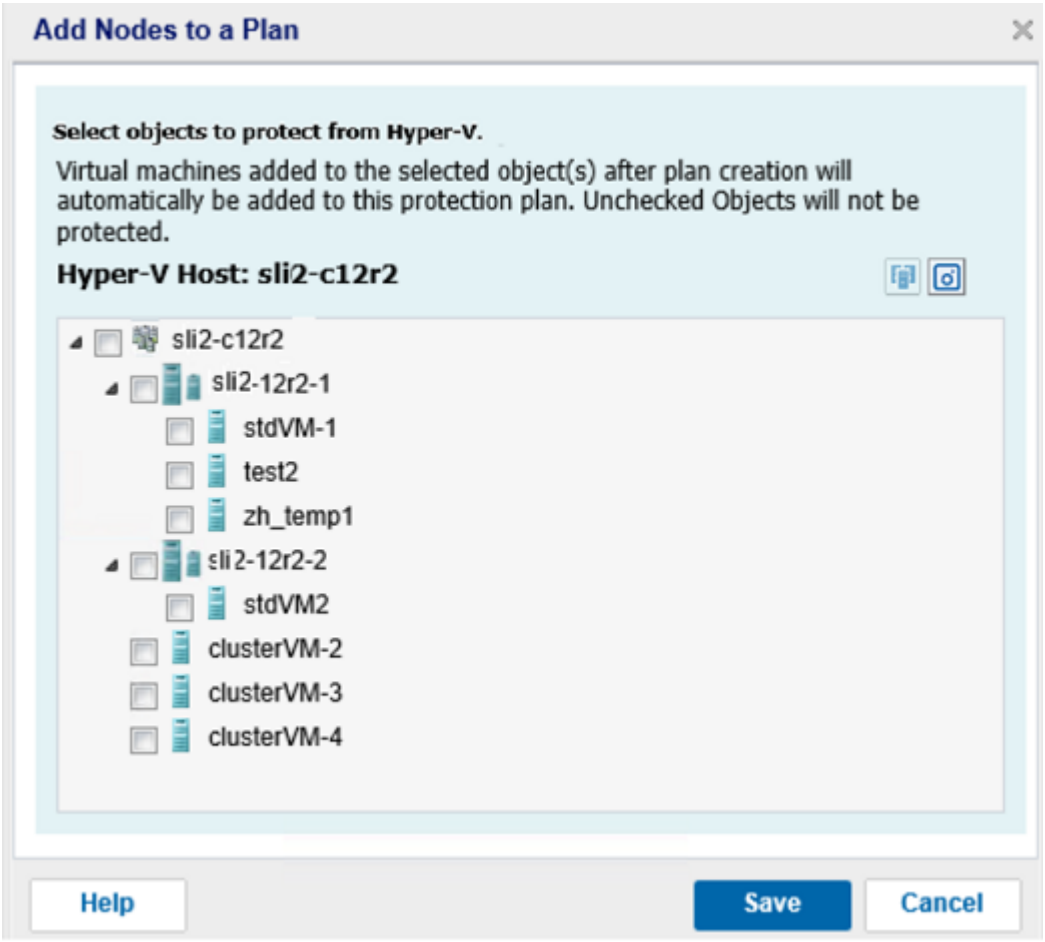


b. Espandere la struttura gerarchica di Hyper-V per eseguire le seguenti opzioni:

Nota: a seconda della selezione nell'elenco a discesa Inventario, vengono mostrate visualizzazioni di struttura gerarchica differenti, ovvero host e computer virtuali oppure archivi e computer virtuali. Per passare da una struttura ad albero all'altra, fare clic sui pulsanti nella parte superiore a destra della struttura.

i. **Aggiunta di un singolo computer virtuale**

Selezionare la casella di controllo corrispondente al computer virtuale che si desidera aggiungere e fare clic su **Salva**.



ii. **Aggiunta di un oggetto contenitore del computer virtuale**

Selezionare la casella di controllo corrispondente all'oggetto contenitore del computer virtuale che si desidera aggiungere dall'elenco, quindi fare clic su Salva. Mentre si seleziona l'oggetto contenitore del computer virtuale da proteggere, è inoltre possibile deselezionare la selezione di un computer virtuale figlio o di un oggetto contenitore del computer virtuale disponibili al di sotto dell'oggetto. Di conseguenza, il computer virtuale figlio o l'oggetto contenitore del computer virtuale vengono esclusi dalla protezione.

Nota: Arcserve UDP utilizza il nome dell'host/cluster Hyper-V, il nome del volume o della condivisione SMB per identificare in modo univoco l'oggetto contenitore nell'elenco di Hyper-V. Di conseguenza, è possibile aggiungere lo stesso oggetto contenitore ai piani più di una volta.

Ad esempio, aggiungere un host Hyper-V mediante il nome host, quindi aggiungere lo stesso host Hyper-V utilizzando l'indirizzo IP. Per fare un altro esempio, aggiungere una condivisione SMB utilizzando il nome

host del computer host, quindi aggiungere la stessa condivisione SMB utilizzando l'indirizzo IP del computer host.

Importante! Arcserve UDP non supporta l'aggiunta dello stesso oggetto contenitore a un piano due volte, in quanto potrebbero verificarsi comportamenti imprevisti.

Aggiunta di nodi da vCenter/ESX

Consente di aprire la finestra di dialogo **Aggiungi nodi alla Console Arcserve UDP**. È possibile aggiungere a un piano singoli nodi di computer virtuale, modelli di computer virtuale oppure oggetti contenitore del computer virtuale. Dopo aver aggiunto un oggetto contenitore del computer virtuale al piano, il piano protegge automaticamente tutti i computer virtuali assegnati. Quando un nuovo computer virtuale viene creato in un oggetto contenitore del computer virtuale o spostato nell'oggetto contenitore del computer virtuale da un'altra posizione, Arcserve UDP protegge il computer virtuale senza intervento manuale. Se il computer virtuale viene eliminato dall'oggetto contenitore del computer virtuale oppure viene spostato all'esterno dell'oggetto contenitore del computer virtuale, Arcserve UDP interrompe la protezione del computer virtuale stesso.

Nota: oltre agli oggetti contenitore di computer virtuale presenti in vSphere, Arcserve UDP considera anche i tag e le categorie di tag come oggetti contenitore, in modo da essere aggiunti al piano di backup senza agente. In tal caso, tutti i computer virtuali e i modelli a cui è assegnato quel tag specifico vengono protetti automaticamente. Inoltre, se a un oggetto contenitore del computer virtuale di livello superiore viene assegnato un tag, tutti i computer virtuali compresi in esso assumono praticamente lo stesso tag. Ad esempio, se si assegna un tag a un pool di risorse, automaticamente lo stesso tag è valido per i computer virtuali del pool anche se non presentano un tag assegnato in vCenter. Inoltre, la protezione automatica mediante tag è supportata solo per vCenter 6.0 e 6.5.

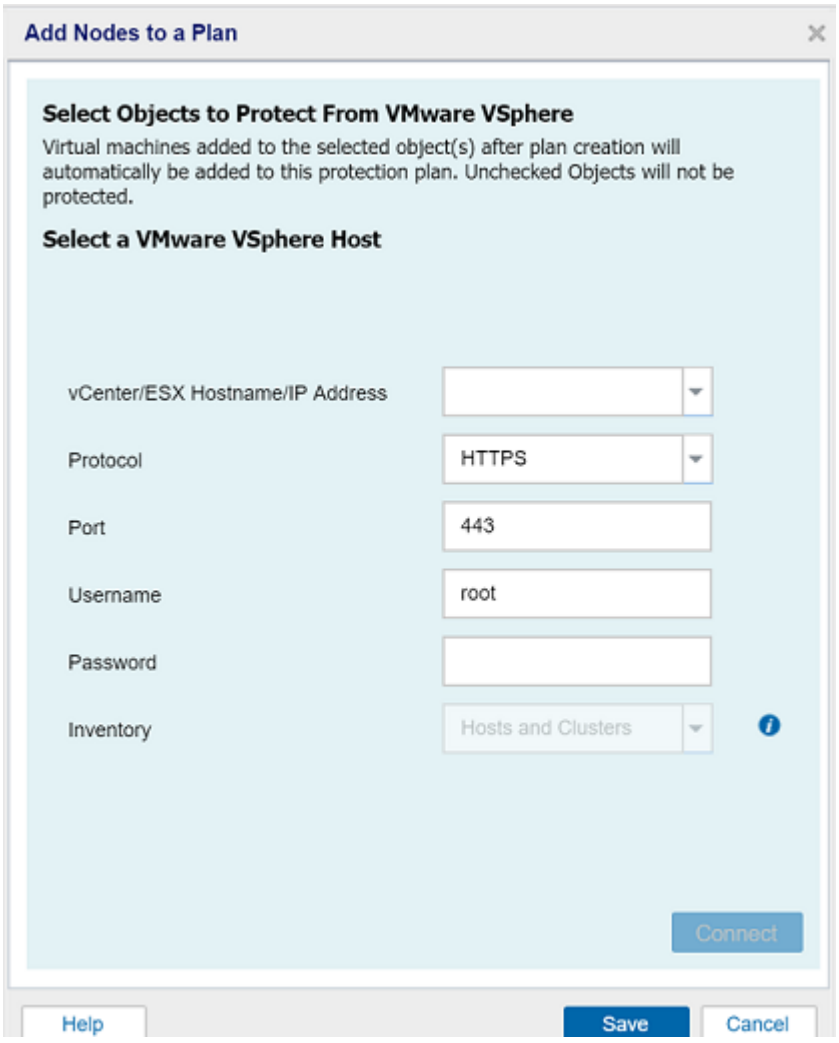
Per aggiungere un oggetto contenitore del computer virtuale a un piano, procedere come segue:

a. Specificare i dettagli del server vCenter/ESX, selezionare la modalità di esplorazione dei computer virtuali nella casella di riepilogo Inventario (Host e cluster, Modelli e computer virtuali, Computer virtuali e tag), quindi fare clic su **Connetti**.

   Viene visualizzata la struttura gerarchica di vSphere.

Nota: Considerare quanto segue:

- VMware Virtual Disk Development Kit (VDDK) 6.x.x è integrato in Arcserve UDP 7.0, ma non supporta il protocollo HTTP. Inoltre, vCenter e ESX in genere supportano la connessione HTTPS solo per impostazione predefinita.
- Selezionare il **protocollo HTTPS** se si desidera sostituire manualmente la versione VDDK 6.x.x integrata con un'altra e configurare vCenter/ESX per consentire la connessione HTTP manuale.

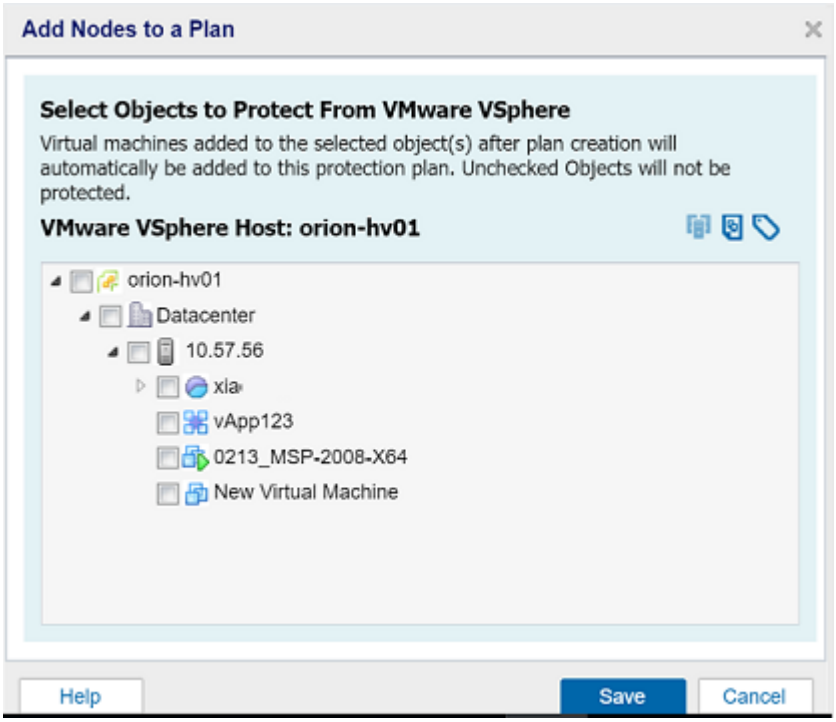


b. Espandere l'elenco vSphere per aggiungere le seguenti operazioni:

Nota: A seconda dell'opzione selezionata nell'elenco a discesa Inventario, vengono visualizzate diverse strutture ad albero gerarchiche: Host e cluster, Modelli e computer virtuali, Computer virtuali e tag. È possibile passare da una struttura ad albero all'altra utilizzando i pulsanti sul lato superiore destro.

i. **Add an individual VM**

Selezionare la casella di controllo corrispondente al computer virtuale che si desidera aggiungere e fare clic su **Salva**.



ii. **Aggiunta di un oggetto contenitore del computer virtuale**

Selezionare la casella di controllo corrispondente al contenitore che si desidera aggiungere e fare clic su **Salva**. Se si seleziona il contenitore da proteggere, è inoltre possibile deselezionare un computer virtuale figlio o un oggetto contenitore figlio del computer virtuale contenuto all'interno. Di conseguenza, il computer virtuale figlio o l'oggetto contenitore del computer virtuale vengono esclusi dalla protezione.

Nota: Arcserve UDP utilizza il nome vCenter/ESX e l'ID vSphere MoRef (ID di riferimento dell'oggetto gestito) per identificare in modo univoco l'oggetto contenitore di computer virtuale nell'elenco **vSphere**. L'operazione consente di aggiungere lo stesso oggetto contenitore del computer virtuale ai piani più di una volta.

Esempio:

a. Aggiungere un oggetto contenitore del computer virtuale a vCenter tramite la connessione a vCenter con il nome host, quindi aggiungere nuovamente lo stesso oggetto

contenitore del computer virtuale tramite la connessione con l'indirizzo IP vCenter.

b. Aggiungere un oggetto contenitore del computer virtuale a vCenter, quindi aggiungerlo nuovamente direttamente dall'host ESX.

Importante: Arcserve UDP non supporta l'aggiunta dello stesso oggetto contenitore del computer virtuale due volte, in quanto potrebbero verificarsi comportamenti imprevisti.

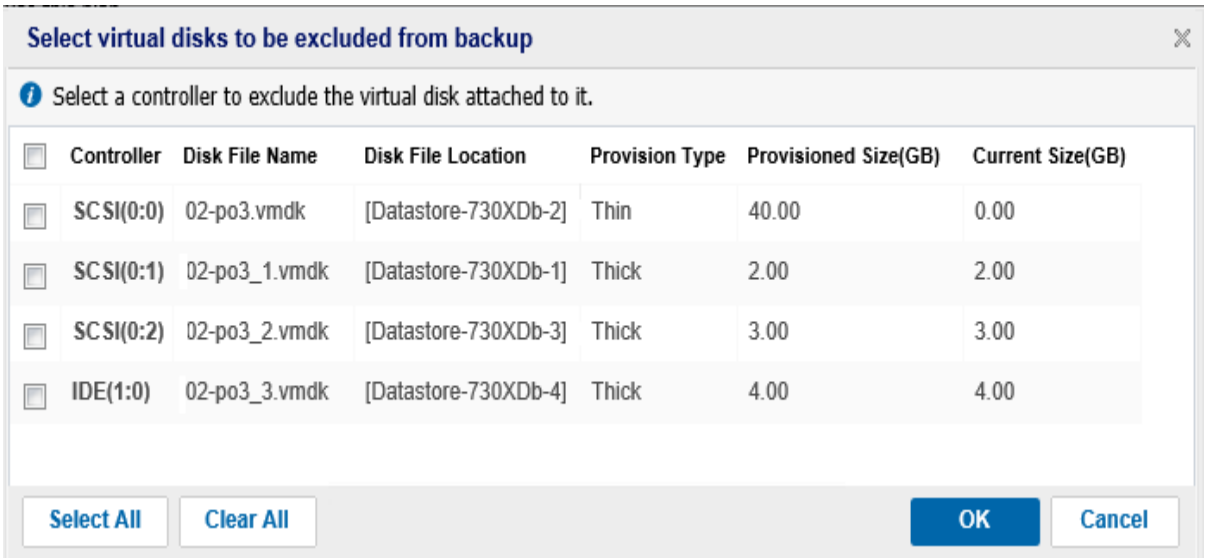
3. (Facoltativo) Selezionare il disco virtuale che si desidera escludere dal processo di backup.

   Per impostazione predefinita, il processo di backup senza agente esegue il backup dell'intero computer virtuale, compresi i dischi virtuali. Tuttavia, è possibile specificare uno o più dischi virtuali da ignorare durante il backup.

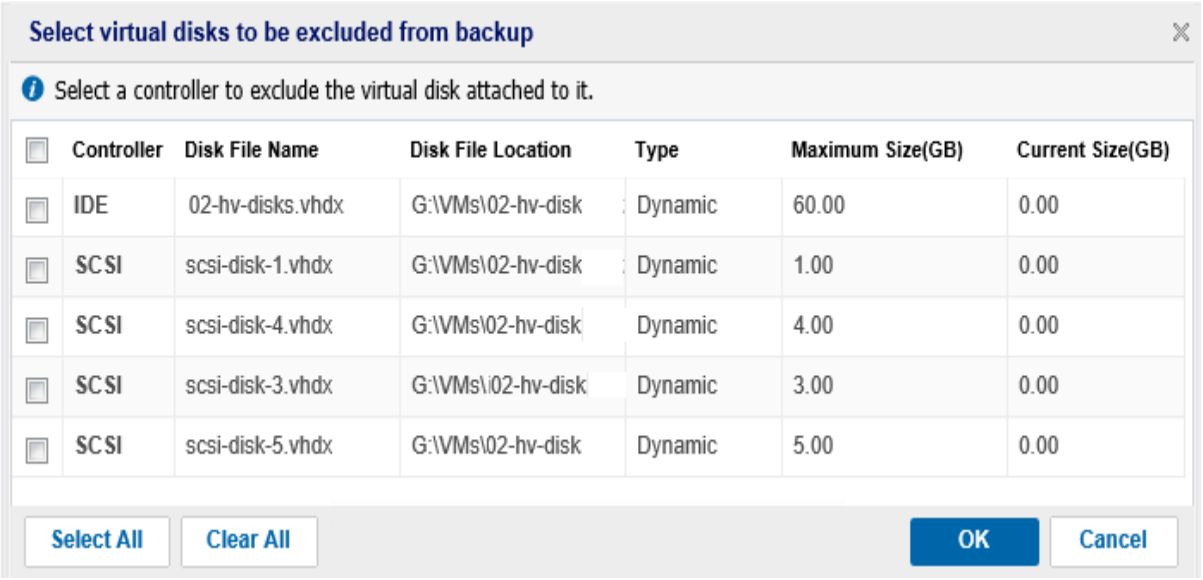
   a. Dopo aver aggiunto un nodo del computer virtuale al piano, fare clic sul pulsante Configura disponibile a destra del nodo.

      Viene visualizzata una finestra di dialogo.

      Finestra di dialogo per il computer virtuale VMware



Finestra di dialogo per il computer virtuale Hyper-V



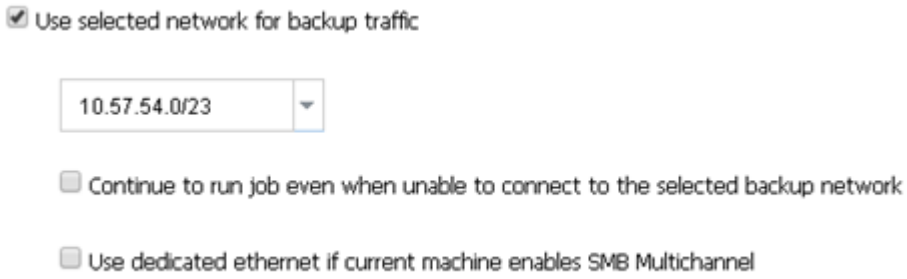
b. Selezionare la casella di controllo corrispondente al disco virtuale che si desidera escludere dal backup e fare clic su **OK** per salvare.

Note:

- Il disco virtuale viene escluso dal controller invece che dal nome del file di disco virtuale.
- Se il disco virtuale contenente il volume di sistema del sistema operativo guest viene escluso dal backup, non sarà possibile avviare il computer virtuale ripristinato.
- Se il computer virtuale dispone di un'applicazione installata (SQL Server o Exchange) e viene escluso un disco virtuale dal backup, il ripristino a livello di database non è consentito.

4. (Facoltativo) Selezionare la casella di controllo **Usa rete selezionata per il traffico di backup** e attenersi alla seguente procedura:

a. Per abilitare la comunicazione tra il proxy Windows e il server Hypervisor, selezionare la rete CIDR dall'elenco a discesa.



b. Se si desidera che l'attività di backup continui anche se la rete selezionata non è disponibile tra il server proxy e l'Hypervisor, selezionare la casella di controllo **Continua a eseguire il processo anche quando non è possibile connettersi alla rete di backup selezionata**.

c. Per definire i vincoli di SMB Multichannel in modo che i dati vengano trasferiti solo tramite la rete selezionata, selezionare la casella di controllo **Usa l'ethernet apposita se il computer corrente abilita SMB Multichannel**.

Note:

- Per impostazione predefinita, questa opzione non è disponibile. Per attivare questa opzione, accedere al seguente percorso nella cartella C:\Programmi\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. Impostare quindi il valore per useDedicatedEthernet su True.

```
- <SpecifyNetwork>
      <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

- La funzionalità SMB Multichannel è abilitata in Windows per impostazione predefinita.

5. Specificare le impostazioni di rete per il backup del computer virtuale Hyper-V di backup basato su host:

Impostazione del Registro di sistema: SMBSpecifiedIONetwork

Posizione: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll or HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\VMInstUUID

Tipo: Valore multistringa

Nome valore: SMBSpecifiedIONetwork

Dati valore: stringa nel formato CIDR (ip/maskBitCount)

Esempio: 192.168.10.0/24

Se Hyper-V o i dischi del computer virtuale cluster Hyper-V sono contenuti nella stessa condivisione SMB, l'utente potrà definire un'altra rete da utilizzare per il trasferimento dei dati tra il server SMB e il computer proxy.

Nota: il mapping tra l'indirizzo IP specificato e il nome host del server SMB devono essere registrati nel dominio.

6. (Facoltativo) Selezionare uno dei seguenti metodi di disattivazione. Queste opzioni sono adatte solo per VMware.

   Strumenti VMware

   Indica che Arcserve UDP utilizza gli strumenti VMware per la disattivazione del computer virtuale. Se nel processo di backup precedente è stata utilizzata l'opzione **Microsoft VSS in Computer virtuale**, il primo processo di backup successivo con questa opzione richiede le credenziali per accedere al computer virtuale. Questo avviene perché Arcserve UDP rimuove gli strumenti necessari dal computer virtuale. Inoltre, è necessario installare e aggiornare gli strumenti VMware nel computer virtuale.

   Microsoft VSS in Computer virtuale

   Indica che Arcserve UDP utilizza Microsoft VSS nel sistema operativo guest per disattivare il computer virtuale. È applicabile solo per i computer virtuali con sistema operativo guest di Windows. È necessario che gli strumenti VMware siano installati nel sistema operativo guest e aggiornati. Quando si utilizza questa opzione, è necessario che il computer virtuale sia acceso e aggiornato con le credenziali ingrate dell'amministratore. Per ulteriori informazioni sull'aggiornamento di un nodo, consultare Aggiornamento dei nodi.

   Nota: la snapshot fornita da VMware mediante questa opzione potrebbe non essere coerente con le applicazioni. In altre parole, il backup generato mediante questa opzione potrebbe non essere un backup coerente con le applicazioni. La soluzione alternativa consiste nell'utilizzare il metodo di disattivazione della snapshot di Strumenti VMware, con la disattivazione dei writer VSS *MSSearch Service Writer* e *Shadow Copy Optimization Writer*nel sistema operativo guest del computer virtuale in attesa della risoluzione del problema.

   Acquisire la snapshot senza disattivazione guest in caso di errore della snapshot di disattivazione

   Indica che, se il processo di backup non riesce ad acquisire la snapshot con l'opzione di disattivazione, Arcserve UDP continuerà il processo di backup acquisendo una snapshot senza disattivare il computer virtuale.

   Note:

   - L'opzione **Microsoft VSS in Computer virtuale** non supporta il livello database dell'applicazione e il livello granulare di ripristino.
   - Quando il computer virtuale è spento, nessuno dei due metodi di disattivazione è applicabile. Se quando il computer virtuale è spento viene avviato

un processo di backup, tale processo ignora entrambi i metodi di disattivazione.

- Per entrambi i metodi di disattivazione, se il processo di backup non può continuare per qualsiasi motivo (ad esempio le credenziali non sono corrette), il processo di backup di Arcserve UDP non riesce. Per ulteriori informazioni sull'errore del processo di backup, consultare l'argomento Risoluzione dei problemi.

7. (Facoltativo) Selezionare uno delle seguenti modalità di trasporto per VMware. Queste opzioni sono adatte per VMware.

   Consenti a VMware di selezionare il metodo migliore disponibile

   Indica che l'opzione di trasferimento dei dati viene selezionata da VMware. Non è necessario impostare manualmente nessuna opzione per il trasferimento dei dati.

   Imposta priorità di metodo per questo piano

   Indica che è possibile selezionare l'opzione di trasferimento dati e impostare la priorità per ogni opzione. Utilizzare la freccia per assegnare la priorità alla modalità di trasporto.

   - Modalità di trasporto HOTADD
   - Modalità di trasporto NBD
   - Modalità di trasporto NBDSSL
   - Modalità di trasporto SAN

   Nota: Se è stata specificata la modalità di trasporto sia nella Console, sia nella chiave di registro, il valore di priorità impostato dalla Console prevale su quello impostato nella chiave di registro. Per ulteriori informazioni sull'impostazione della priorità mediante la chiave di registro, consultare la sezione Definizione di una modalità di trasporto per il backup e il ripristino senza agente basati su host.

8. (Facoltativo) Selezionare il metodo snapshot Hyper-V. Queste opzioni sono adatte solo per Hyper-V.

   È necessario eseguire il backup del computer virtuale utilizzando snapshot generate dal metodo Microsoft VSS

   Indica che Arcserve UDP utilizza i metodi di snapshot nativi in linea e non in linea di Microsoft per il processo di backup. Questa è l'opzione predefinita. Quando questa casella di controllo non è selezionata e i due metodi in linea e non in linea di Microsoft non sono disponibili, il processo di backup utilizza il metodo di Arcserve UDP per eseguire il backup del computer virtuale.

Se viene utilizzato il metodo non in linea di Microsoft per il backup e il computer virtuale deve essere nello stato Salvato, selezionare anche la casella di controllo **Il computer virtuale deve essere in Stato "Salvato" prima dell'acquisizione di una snapshot**. Se questa casella di controllo non viene selezionata, il processo di backup non riesce.

Backup in linea è il metodo di backup consigliato poiché supporta il backup coerente dell'applicazione senza il tempo di inattività del computer virtuale. Il computer virtuale è accessibile durante il backup. Il metodo di backup online deve soddisfare alcuni prerequisiti, ad esempio i servizi di integrazione devono essere installati e in esecuzione. Se uno qualsiasi dei prerequisiti non viene soddisfatto, viene utilizzato solo il metodo di backup non in linea.

Il metodo di backup in linea di Microsoft ha due approcci: stato Salva e del punto di controllo. Se l'host Hyper-V dispone del sistema operativo Windows 2012R2 con 2919355 KB o successivi, viene utilizzato l'approccio del punto di controllo; in caso contrario, viene utilizzato l'approccio dello stato Salva.

La principale differenza tra questi due approcci è che l'approccio dello stato Salva richiede che il computer virtuale sia inaccessibile per un breve intervallo di tempo. Il computer virtuale deve essere impostato sullo stato Salvato per pochi minuti durante l'acquisizione della snapshot.

Oltre ai metodi snapshot nativi di Microsoft, Arcserve UDP dispone di un proprio metodo snapshot che può essere utilizzato quando non sono disponibili i primi.

Nota: sia il metodo non in linea di Microsoft, sia il metodo di Arcserve UDP sono metodi di backup crash-consistent. Nessuno dei metodi può garantire l'integrità dei dati. La principale differenza tra i metodi è che il metodo non in linea di Microsoft può essere paragonato allo stato di un computer virtuale spento bruscamente, mentre il metodo di Arcserve UDP può essere paragonato allo stato di un host Hyper-V spento bruscamente.

Il computer virtuale deve essere in Stato "Salvato" prima dell'acquisizione di una snapshot

Indica che il computer virtuale è impostato sullo stato Salvato, se necessario, prima di acquisire la snapshot VSS. Selezionare questa opzione quando il computer virtuale non supporta il backup in linea. Se il computer virtuale supporta il backup in linea, anche se si abilita questa opzione, il computer virtuale non sarà nello stato Salvato.

L'origine viene specificata.

Definizione di una modalità di trasporto nel registro per il backup e il ripristino senza agente basati su host

È possibile definire la modalità di trasporto (trasferimento dei dati) per l'agente UDP come proxy che esegue il backup senza agente basato su host o come processo di ripristino per i computer virtuali presenti su un server VMware ESX. Per impostazione predefinita, il backup e il ripristino senza agente basati su host si servono di una modalità che consente al backup e al ripristino senza agente di migliorare le prestazioni (aumento della velocità) del trasferimento dati. Tuttavia, se si desidera specificare una determinata modalità di trasporto per le operazioni di backup o ripristino, è possibile configurare la chiave di registro descritta nella presente sezione.

Nota: per il backup, la modalità di trasporto definita nel piano ha la precedenza su quella definita nel Registro di sistema.

Il backup dei computer virtuali basati su host può essere eseguito utilizzando le modalità di trasporto seguenti:

- Modalità di trasporto HOTADD
- Modalità di trasporto NBD
- Modalità di trasporto NBDSSL
- Modalità di trasporto SAN

Tenere presenti le seguenti considerazioni:

- Si tratta di un'attività di configurazione facoltativa. Per impostazione predefinita, il backup dei computer virtuali basati su host viene eseguito mediante la modalità di trasporto in grado di ottimizzare la prestazioni dell'operazione di backup.
- Quando si configura questa chiave di registro per utilizzare una modalità di trasporto specifica e tale modalità non è disponibile, il backup del computer basato su host utilizza una modalità di trasporto predefinita disponibile per il backup.
- È possibile definire la modalità di trasporto per tutti i computer virtuali utilizzati per il backup mediante il server proxy (livello di proxy) o definire un computer virtuale specifico (livello del computer virtuale). Se vengono configurati sia il server proxy che il computer virtuale, il Registro di sistema a livello di computer virtuale ha la precedenza sul Registro di sistema a livello di proxy.

Attenersi alla seguente procedura per definire la modalità di trasporto a livello di server proxy (adatto per il backup e per il ripristino):

1. Accedere al server proxy di backup dell'Agente Arcserve Unified Data Protection per Windows.
2. Aprire l'editor del Registro di sistema di Windows e cercare la seguente chiave:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine]
3. Fare clic con il pulsante destro del mouse su VDDKEnforceTransport e selezionare Modifica dal menu di scelta rapida per aprire la finestra di dialogo Modifica stringa.
4. Nel campo Dati del valore, specificare la modalità di trasporto che si desidera utilizzare durante il processo di backup. Specificare uno o più dei valori seguenti, separati da ":". (Ad esempio nbd o san:nbd:nbdssl:)

   hotadd

   Modalità di trasporto HOTADD

   nbd

   Modalità di trasporto NBD

   nbdssl

   Modalità di trasporto NBDSSL

   san

   Modalità di trasporto SAN
5. Fare clic su OK per applicare il valore e chiudere la finestra di dialogo di modifica della stringa.

   La modalità di trasporto viene definita e viene utilizzata all'esecuzione successiva del processo.

   Nota: per ripristinare dischi di computer virtuali (VMDK) di piccole dimensioni, per impostazione predefinita viene utilizzata la modalità di trasporto non avanzata (modalità di trasporto LAN). Per abilitare la modalità di trasporto avanzata per dischi di computer virtuali (VMDK) di piccole dimensioni, aggiornare la chiave di registro come nell'esempio seguente:

   a. Aprire l'editor del Registro di sistema di Windows e cercare la seguente chiave:

      ```
      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine]
      ```

   b. Creare una chiave denominata AFRestoreDll

c. Creare un valore stringa denominato EnforceTransportForRecovery all'interno della chiave AFRestoreDll.

d. Specificare la modalità di trasporto che si desidera utilizzare durante il processo di ripristino. (Ad esempio: "san:nbd:nbdssl")

Esempio

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFRestoreDll]

"EnforceTransportForRecovery"="san:hotadd:nbd:nbdssl"

Per definire la modalità di trasporto a livello di computer virtuale, procedere come segue (solo per backup):

1. Accedere al server proxy di backup dell'Agente Arcserve Unified Data Protection per Windows per i computer virtuali.
2. Aprire l'editor del Registro di sistema di Windows e cercare la seguente chiave:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\{VM-InstanceUUID}
3. Fare clic con il pulsante destro del mouse su VM-InstanceUUID e scegliere Nuovo.
4. Fare clic su Valore stringa nel menu di scelta rapida.
5. Nominare il nuovo valore della stringa come segue.

   EnforceTransport
6. Fare clic con il pulsante destro del mouse su EnforceTransport e selezionare Modifica dal menu di scelta rapida per aprire la finestra di dialogo Modifica stringa.
7. Nel campo Dati del valore, specificare la modalità di trasporto che si desidera utilizzare durante il processo di backup. Specificare uno dei seguenti valori:

   hotadd

   Modalità di trasporto HOTADD

   nbd

   Modalità di trasporto NBD

   nbdssl

   Modalità di trasporto NBDSSL

   san

   Modalità di trasporto SAN
8. Fare clic su OK per applicare il valore e chiudere la finestra di dialogo di modifica della stringa.

La modalità di trasporto viene definita e viene utilizzata all'esecuzione successiva del processo.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Selezionare un **Tipo di destinazione** tra quelli elencati di seguito:

   Disco locale o cartella condivisa

   Specifica che la destinazione di backup è una destinazione locale o una cartella condivisa. Se si seleziona questa opzione, è possibile salvare i dati come punti di ripristino o set di ripristino. Le opzioni dei punti di ripristino e dei set di ripristino sono disponibili nella scheda **Pianificazione.**

   Recovery Point Server di Arcserve UDP

   Specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono memorizzati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.

2. Se è stato selezionato il **Recovery Point Server di Arcserve UDP**, immettere i seguenti dettagli:

   a. Selezionare un Recovery Point Server.

   b. Selezionare un archivio dati. L'elenco mostra tutti gli archivi dati creati sul Recovery Point Server specificato.

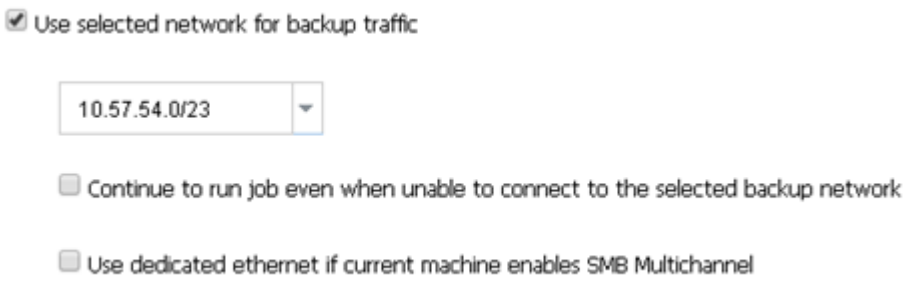
   c. Fornire una password di sessione.

      Nota: la password di sessione è facoltativa se la destinazione di backup è un archivio di dati RPS non crittografato.

   d. Confermare la password di sessione.

   e. (Facoltativo) Selezionare la casella di controllo **Usa rete selezionata per il traffico di backup** e attenersi alla seguente procedura:

      1. Per abilitare la comunicazione tra il proxy Windows e il Recovery Point Server, selezionare la rete CIDR dall'elenco a discesa.



2. Se si desidera che l'attività di backup continui anche se la rete selezionata non è disponibile tra il server proxy e il Recovery Point Server, selezionare la casella di controllo **Continua a eseguire il processo anche quando non è possibile connettersi alla rete di backup selezionata**.
3. Per disabilitare SMB Multichannel in modo che i dati vengano trasferiti solo tramite la rete selezionata, selezionare la casella di controllo **Usa l'ethernet apposita se il computer corrente abilita SMB Multichannel**.

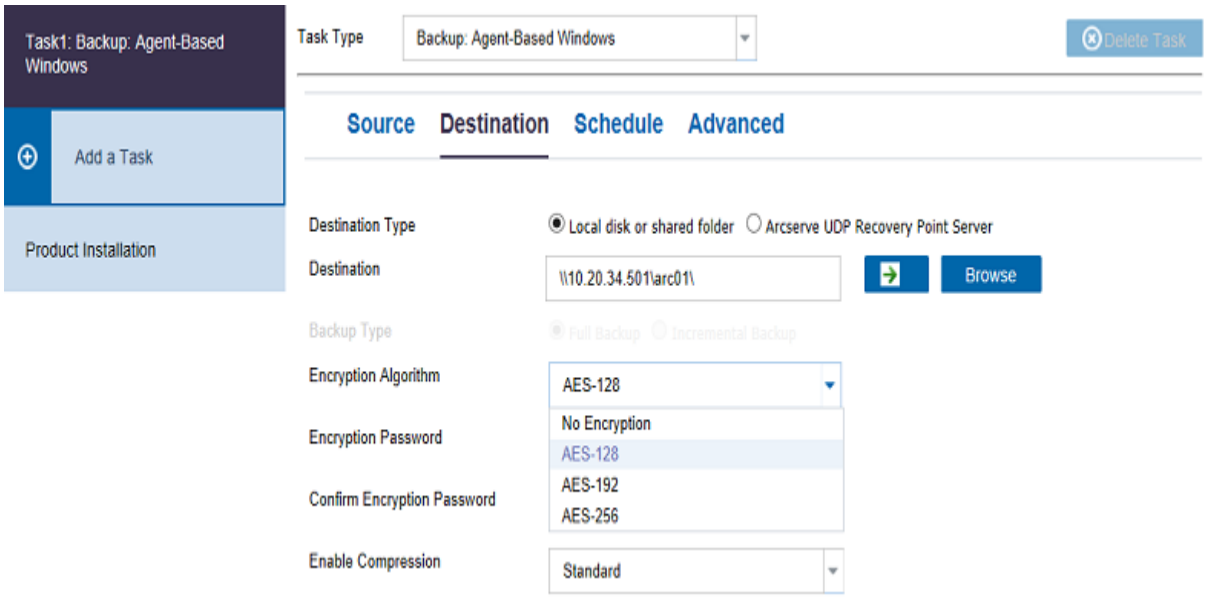
Note:

- Per impostazione predefinita, questa opzione non è disponibile. Per attivare questa opzione, accedere al seguente percorso nella cartella C:\Programmi\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. Impostare quindi il valore per *useDedicatedEthernet* su True.

```
- <SpecifyNetwork>
      <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

  La funzione Definisci rete viene disabilitata nel caso di un archivio dati remoto che utilizza la cartella di rete condivisa come destinazione.
- La funzionalità SMB Multichannel è abilitata in Windows per impostazione predefinita.

3. Se è stata selezionata l'opzione **Utilizza il disco locale o la cartella condivisa**, fornire i dettagli seguenti:



a. Fornire il percorso completo della destinazione locale o di rete. Per la destinazione di rete, specificare le credenziali con l'accesso di scrittura. È possibile fare clic su Sfoglia per individuare la destinazione oppure fare clic sull'icona della freccia avanti per eseguire il test della connessione e fornire le credenziali per la cartella di destinazione fornita.

b. Dall'elenco a discesa delle opzioni disponibili, selezionare l'algoritmo di crittografia. Per ulteriori informazioni, consultare la sezione Impostazioni di crittografia.

c. Facoltativamente, fornire una password di crittografia.

d. Immettere la password di crittografia per confermarla.

e. Selezionare un tipo di compressione. Per ulteriori informazioni, consultare la sezione Tipo di compressione.

Nota: Se si archiviano i dati in un disco locale o in una cartella condivisa, non è possibile replicare i dati in un altro Recovery Point Server. La replica è supportata solo se si archiviano i dati in un Recovery Point Server.

La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

Effettuare le operazioni seguenti:

1. (Facoltativo) Selezionare l'opzione per la gestione dei punti di ripristino. Questa opzione è visibile solamente se sono state selezionate le cartelle Locale o Condivisa come destinazione di backup.

   Conserva per punti di ripristino

   I dati di backup vengono archiviati come punti di ripristino.

   Conserva per set di ripristino

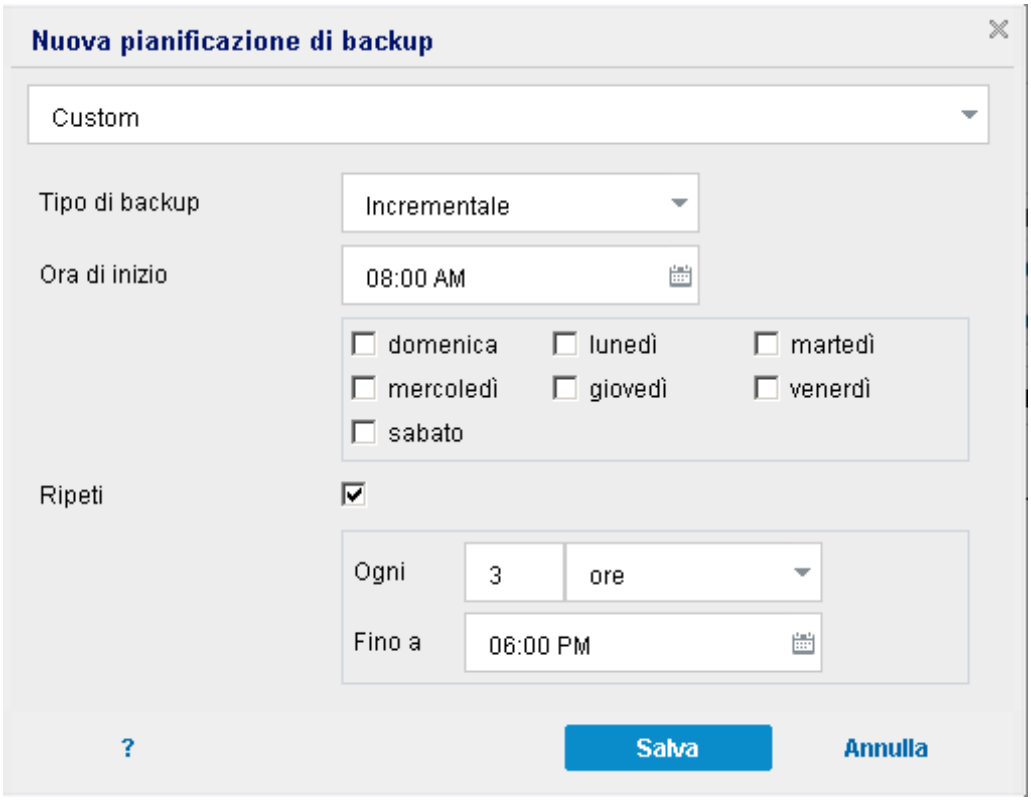
   I dati di backup vengono archiviati come set di ripristino.

2. Aggiungere le pianificazioni di backup, di unione e di definizione del limite di velocità

   Aggiunta di una pianificazione di backup

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base

alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni del backup.

Verifica

Specifica la pianificazione dei backup di verifica.

In base alla pianificazione specificata, Arcserve UDP controlla che i dati protetti siano validi e completi eseguendo una verifica di affidabilità dell'immagine di backup archiviata sull'origine di backup originale. Se necessario esegue la risincronizzazione dell'immagine. Un backup di verifica controlla il backup più recente di ogni blocco e lo confronta con il contenuto e le informazioni di origine. Questo confronto consente di verificare che il blocco di backup più recente rappresenti le informazioni corrispondenti all'origine. Se l'immagine di backup di un blocco non corrisponde all'origine (probabilmente a causa di modifiche apportate al sistema dall'ultimo backup), Arcserve UDP aggiorna (risincronizza) il backup del blocco non corrispondente. Sebbene si tratti di una procedura poco frequente, il backup di verifica può essere utilizzato per ottenere le stesse garanzie di un backup completo, senza occupare lo spazio richiesto da questo tipo di backup.

Vantaggi: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.

Svantaggi: il backup di verifica richiede tempi di esecuzione più lunghi, in quanto esegue il confronto di tutti i blocchi originali con i blocchi del backup più recente.

Incrementale

Specifica la pianificazione dei backup incrementali.

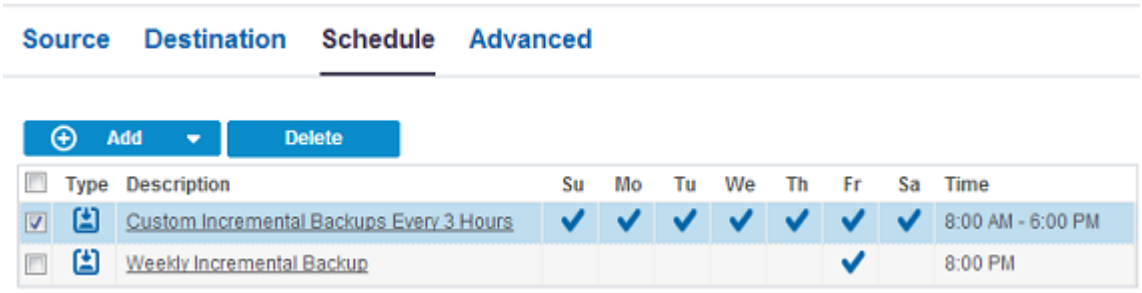
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Si tratta della modalità di backup ottimale e si consiglia di utilizzarla come modalità predefinita.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La Pianificazione di backup viene specificata e viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di unione**.

b. La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

c. Specificare l'ora di inizio per l'avvio del processo di unione.

d. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

e. Fare clic su **Salva**.

La Pianificazione di unione viene specificata e viene visualizzata nella pagina **Pianificazione**.

Aggiungi pianificazione del limite delle risorse

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

b. Viene visualizzata la finestra di dialogo Aggiungi nuova pianificazione del limite delle risorse.

c. Specificare il limite di velocità effettiva in MB per unità di minuti.

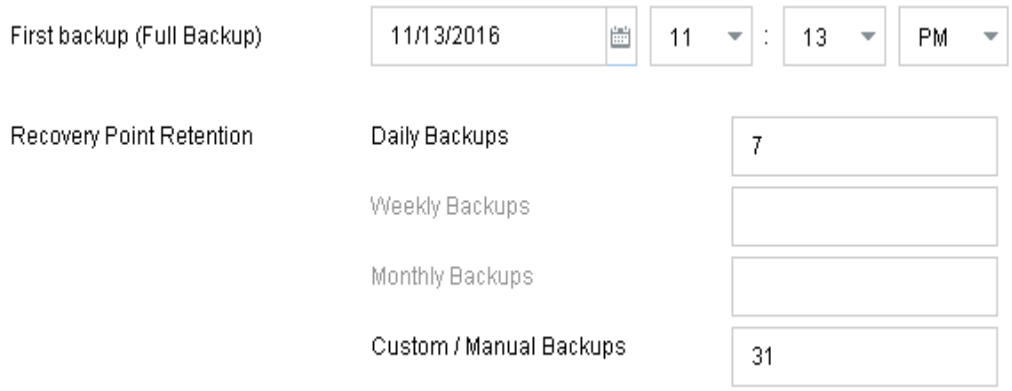
d. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

e. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

f. Fare clic su **Salva**.

La pianificazione della velocità effettiva viene specificata e viene visualizzata nella pagina **Pianificazione**.

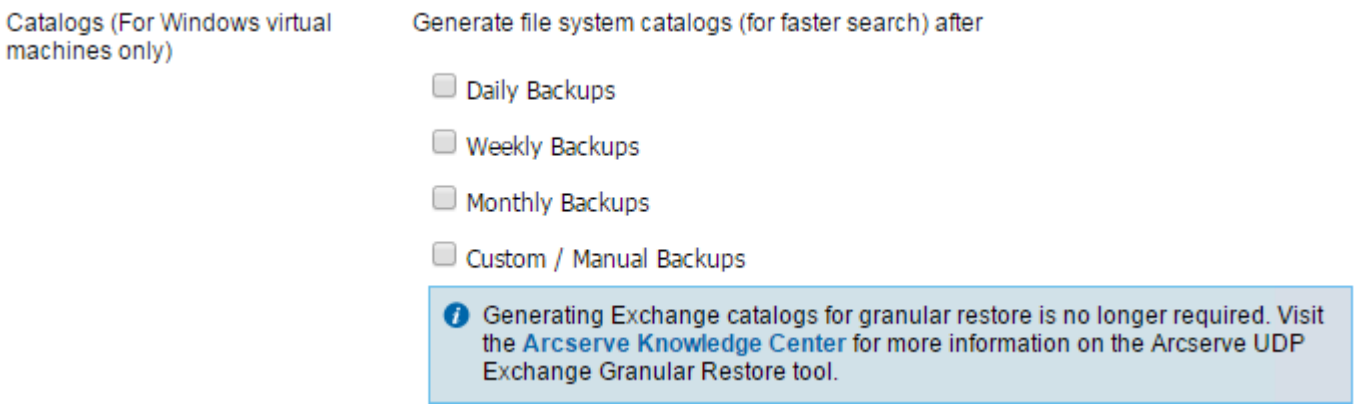
3. Specificare l'ora di inizio per il backup pianificato.



4. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo Pianificazione di backup.

5. Specificare i dettagli relativi al catalogo.



   I cataloghi permettono di generare il catalogo file system. Il catalogo file system è necessario per semplificare e velocizzare la ricerca. I cataloghi vengono abilitati in base al tipo di backup specificato.

   Viene specificata la pianificazione.

Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione

L'opzione di pianificazione consente di specificare una pianificazione personalizzata o una pianificazione giornaliera/settimanale/mensile o entrambe. Nella pianificazione personalizzata è possibile configurare la pianificazione del backup per ciascun giorno della settimana e aggiungere fino a quattro pianificazioni di backup ogni giorno. È possibile selezionare un giorno specifico di una settimana e creare un intervallo di tempo per definire quando eseguire il backup e la frequenza.

Pianificazione	Processo supportato	Commenti
Backup	Processo di backup	Definire gli intervalli di tempo per eseguire i processi di backup.
Limitazione della velocità di backup	Processo di backup	Definire gli intervalli di tempo per controllare la velocità di backup.
Unione	Processo di unione	Definire quando unire i processi.
Pianificazione quotidiana	Processo di backup	Definire quando eseguire processi di backup quotidiani.
Pianificazione settimanale	Processo di backup	Definire quando eseguire processi di backup settimanali.
Pianificazione mensile	Processo di backup	Definire quando eseguire processi di backup mensili.

È inoltre possibile specificare le impostazioni di memorizzazione per i punti di ripristino.

Nota: All'interno di ogni piano è necessario configurare le impostazioni di conservazione per controllare il modo in cui i nodi assegnati a tale piano vengono memorizzati nell'archivio dati di destinazione.

Le pianificazioni per i backup giornalieri/settimanali/mensili sono indipendenti dalla pianificazione personalizzata e gli uni dagli altri. È possibile configurare di eseguire solo il backup giornaliero, il backup settimanale o il backup mensile senza configurare la pianificazione personalizzata.

Pianificazione del processo di backup

È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del backup. Un intervallo di tempo valido è dalle 00:00 alle 23:59. Non è possibile specificare un intervallo di tempo come ad esempio dalle 18:00 alle 06:00. In tali casi, si devono specificare manualmente due intervalli di tempo diversi.

Per ogni intervallo di tempo l'ora di inizio è inclusa e l'ora di fine è esclusa. Ad esempio, si è configurato il backup incrementale da eseguire ogni ora tra le 06:00 e le 09:00 e il backup inizierà alle 06:00. Ciò significa che il backup verrà eseguito alle 06:00, alle 07:00 e 08:00, ma NON alle 09:00.

Nota: Se si desidera eseguire il processo di backup ripetutamente fino al termine della giornata, impostare la pianificazione fino alle 00:00. Ad esempio, per eseguire un processo di backup ogni 15 minuti per l'intera giornata, impostare la pianificazione dalle 00:00 alle 00:00 ogni 15 minuti.

Pianificazione del limite delle risorse di backup

La pianificazione del limite delle risorse di backup consente di controllare la velocità effettiva di backup, che a sua volta controlla l'utilizzo delle risorse (I/O del disco, CPU, larghezza di banda della rete) del server di cui si esegue il backup. Questo è utile se non si desidera influire sulle prestazioni del server durante i normali orari di ufficio. È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del limite delle risorse di backup. Per ogni intervallo di tempo è possibile specificare un valore, in MB per minuto. Questo valore viene utilizzato per controllare la velocità effettiva di backup. I valori validi sono compresi tra 1 MB/minuto a 99999 MB/minuto.

Se un processo di backup si estende oltre il tempo specificato, il limite della velocità cambia in conformità all'intervallo di tempo specificato. Ad esempio, il limite delle risorse di backup definito è 500 MB/minuto dalle 08:00 alle 20:00 e 2500 MB/minuto dalle 20:00 alle 22:00. Se un processo di backup inizia alle 19:00 e viene eseguito per tre ore, dalle 19:00 alle 20:00 il limite della velocità è pari a 500 MB/minuto e dalle 20:00 alle 22:00 a 2500 MB/minuto.

Se non si definisce alcuna pianificazione del backup e della sua velocità effettiva, il backup viene eseguito il più rapidamente possibile.

Pianificazione di unione

Consente di unire i punti di ripristino in base alla pianificazione fornita.

Considerare i punti seguenti per il processo di unione:

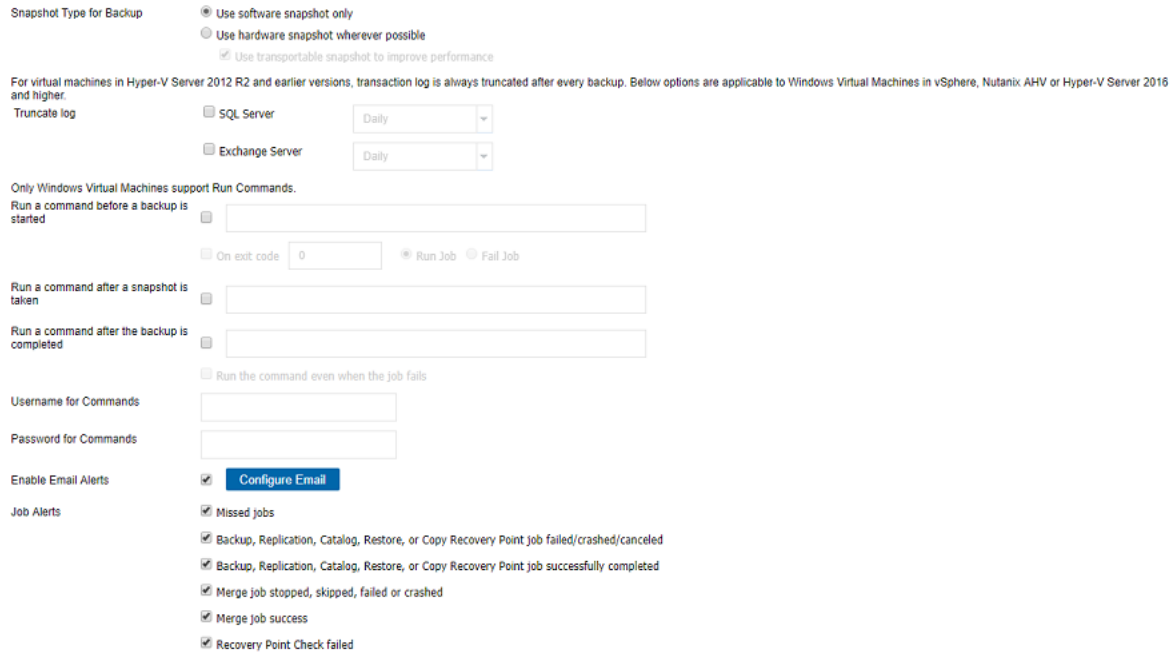
- In qualsiasi momento è possibile eseguire solo un processo di unione per un nodo.
- Se un processo di unione inizia, esso deve essere completato prima di poter avviare il processo di unione successivo. Ciò significa che se uno o più set di punti di ripristino vengono uniti, non è possibile aggiungere nuovi punti di ripristino a questo processo di unione finché il processo di unione dell'insieme corrente dei punti di ripristino non viene completato.

- Se un processo di unione sta elaborando più di un set di punti di ripristino (ad esempio set [1~4], set [5~11] e set [12~14] sono tre set distinti), il Recovery Point Server elabora tali set uno alla volta.
- Se un processo di unione viene ripreso dopo una pausa, il processo individua in quale punto era stato interrotto e riprende l'unione da tale punto.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione del tipo di snapshot per il backup, delle impostazioni per troncare i registri, l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica. Verificare i prerequisiti prima di selezionare il tipo di snapshot hardware.

La seguente immagine mostra la scheda Avanzate:



Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

Tipo di snapshot per il backup

Selezionare una delle seguenti opzioni per la snapshot del backup:

Utilizza solo snapshot software

Specifica che il tipo di backup utilizza solo la snapshot software. Arcserve UDP non cercherà la snapshot hardware. La snapshot software utilizza un numero minore di risorse sui computer virtuali. È possibile utilizzare questa opzione se il server presenta configurazioni e velocità di elaborazione inferiori.

Utilizza snapshot hardware se possibile

Specificare che il tipo di backup verifica innanzitutto una la presenza di una snapshot hardware. Se tutti i criteri vengono soddisfatti, il tipo di backup utilizza la snapshot hardware.

Nota: Per ulteriori informazioni sui criteri della snapshot hardware, consultare la sezione dedicata ai prerequisiti.

Per Hyper-V, Arcserve UDP utilizza il provider hardware per acquisire una snapshot VSS dei volumi sull'host Hyper-V e importare la snapshot hardware per il server proxy. Sul server proxy deve essere installato un provider hardware adatto. Per VMware, Arcserve UDP crea la snapshot software vSphere per un breve periodo di tempo, quindi crea la snapshot hardware. Questo snapshot hardware viene montato sul server ESX VMware e la snapshot software viene eliminata. Quindi Arcserve UDP utilizza i contenuti nella snapshot hardware per eseguire il backup dei file relativi al computer virtuale.

Use transportable snapshots to improve performance (Utilizza snapshot trasportabili per migliorare le prestazioni)

Specifica che la snapshot hardware utilizza una snapshot trasportabile. Le snapshot trasportabili consentono di aumentare la velocità effettiva del backup. Questa opzione è adatta solo per i server Hyper-V.

Tronca registro

Consente di specificare la pianificazione per troncare i registri per SQL Server ed Exchange Server. È possibile specificare la pianificazione come **Giornaliero**, **Settimanale** o **Mensile**. Questa opzione è applicabile solo a VMware.

Esegui un comando prima dell'avvio di un backup

Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script all'interno del sistema operativo guest del computer virtuale. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Esegui processo** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita. Questa opzione è applicabile solo ai computer virtuali Windows.

Note: (Valido anche per i comandi In seguito all'acquisizione della snapshot e In seguito al completamento del backup).

- Si consiglia di specificare il percorso completo dello script o del comando. Ad esempio, è possibile utilizzare C:\Windows\System32\Ping.exe invece di solo Ping.exe.

- Per fare in modo che il processo di backup non si blocchi a causa dell'interruzione del comando o dello script, essi verranno interrotti per impostazione predefinita se il processo non può essere completato entro 3 minuti. Se si desidera modificare l'impostazione di timeout predefinito, procedere come segue a livello di server proxy o del computer virtuale:

  A livello di server proxy (adatto per tutti i processi di backup in esecuzione sul server proxy)

  a. Aprire la chiave del Registro di sistema dal percorso seguente:

     [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

  b. Aggiungere il valore DWORD denominato PrePostCMDTimeoutInMinute e specificarne il valore con il tempo di timeout in minuti.

  A livello di computer virtuale

  a. Aprire la chiave del Registro di sistema dal percorso seguente:

     [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

  b. Aggiungere il valore DWORD denominato PrePostCMDTimeoutInMinute e specificarne il valore con il tempo di timeout in minuti.

     Nota: Se si aggiunge il valore del Registro di sistema nel Registro di sistema a livello del computer virtuale e del proxy, l'impostazione nel Registro di sistema a livello del computer virtuale avrà la priorità sull'impostazione nel Registro di sistema a livello del proxy.

Esegui comando dopo l'acquisizione della snapshot

Consente di eseguire uno script dopo l'acquisizione della snapshot del backup. Specificare il percorso di archiviazione dello script all'interno del sistema operativo guest del computer virtuale. Questa opzione è applicabile solo ai computer virtuali Windows.

Esegui un comando al completamento di un backup

Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso di archiviazione dello script all'interno del sistema operativo guest del computer virtuale. Questa opzione è applicabile solo ai computer virtuali Windows.

Esegui un comando anche quando il processo non riesce

Se questa casella di controllo è selezionata, lo script specificato in Esegui un comando al completamento di un backup viene eseguito anche quando si verifica un errore di completamento del processo di backup. In caso contrario, lo script viene eseguito solo quando il processo di backup viene completato correttamente.

Nome utente comandi

Consente di specificare il nome utente per eseguire i comandi.

Password comandi

Consente di specificare la password per eseguire i comandi.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere in un messaggio di posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

2. Fare clic su **Salva**.

Gli aggiornamenti vengono salvati e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota:

- Se si deve aggiungere un'altra attività, selezionare il piano dalla scheda Risorse e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo.
- Quando si seleziona un nodo che non ha installato l'agente Arcserve UDP, come proxy di backup la console UDP distribuisce automaticamente un agente in tale nodo dopo aver salvato il piano.

Viene creato il piano di backup basato su host senza agente per il computer virtuale. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

Esecuzione di uno script o un comando e troncamento del registro con un account di amministratore aggiuntivo

L'account di amministratore aggiuntivo fa riferimento agli account che non utilizzano amministratori predefiniti. I due account seguenti sono coinvolti durante l'esecuzione di comandi o script:

1. Account impostato con Aggiorna nodo
2. Account impostato nella scheda Avanzata di un piano

I computer virtuali VMware e Hyper-V presentano condizioni distinte per l'utilizzo degli account di amministratore aggiuntivi.

Computer virtuali VMware

Se sono impostati entrambi gli account, utilizzare il primo per accedere al computer virtuale (viene utilizzato l'SDK di vSphere per comunicare con il computer virtuale, in modo che non sia necessario l'accesso alla rete tra il server proxy e il computer virtuale). Utilizzare quindi il secondo account per eseguire il comando o lo script nel computer virtuale.

Se uno dei due account non è impostato, utilizzare l'account disponibile per accedere al computer virtuale ed eseguire il comando o lo script.

Si consiglia di utilizzare l'account di amministratore integrato o l'account di amministratore di dominio integrato per entrambi.

Se si utilizza un account di amministratore aggiuntivo (non integrato), la procedura cambia.

Effettuare le operazioni seguenti:

1. Per accedere al computer virtuale con l'account di amministratore aggiuntivo, attenersi alla procedura descritta nella sezione Aggiornamento dei nodi per verificare che l'account disponga delle autorizzazioni richieste.
2. Per eseguire il comando o lo script con l'account di amministratore aggiuntivo, verificare che questo disponga delle autorizzazioni richieste. Accedere al computer virtuale guest con l'account di amministratore aggiuntivo, eseguire il comando o lo script e confermare il corretto completamento.

Computer virtuali Hyper-V

È necessario un solo account per i computer virtuali Hyper-V. Se sono impostati entrambi gli account, utilizzare il secondo account, indicato nella scheda Avanzata di un piano, per connettersi al computer virtuale ed eseguire il comando o lo script. Strumentazione gestione Windows (WMI) si utilizza per comunicare con il

computer virtuale in modo che sia necessario l'accesso alla rete tra il server proxy e il computer virtuale.

Se uno dei due account non è impostato, utilizzare l'account di amministratore disponibile per connettersi al computer virtuale ed eseguire il comando o lo script.

Effettuare le operazioni seguenti:

1. Accedere al computer virtuale con WMI remoto. Verificare di disporre delle autorizzazioni richieste con l'account di amministratore aggiuntivo. Consultare la sezione Aggiornamento dei nodi per i requisiti dell'account.
2. Per eseguire il comando o lo script con l'account di amministratore aggiuntivo, verificare che questo disponga delle autorizzazioni richieste. Accedere al computer virtuale guest con l'account di amministratore aggiuntivo, eseguire il comando o lo script e confermare il corretto completamento.

   Inoltre, verificare se WMI è autorizzato dal firewall sul computer virtuale ospite. Se non è abilitato, procedere come segue:

1. Accedere al computer virtuale guest.
2. Aprire il Pannello di controllo.
3. Aprire Windows Firewall.
4. Fare clic su Consenti app o funzionalità attraverso Windows Firewall.
5. Abilitare Strumentazione gestione Windows (WMI).
6. Fare clic su OK.

Definizione di un limite per il numero di backup simultanei

L'applicazione consente di definire un limite per il numero di processi di backup eseguiti simultaneamente. Questa funzionalità consente di ottimizzare le prestazioni del server proxy di backup del computer virtuale nell'ambiente di backup. Per impostazione predefinita, il backup del computer virtuale basato su host può eseguire fino a quattro processi di backup di computer virtuali VMware, dieci processi di backup di computer virtuali Hyper-V e quattro processi di backup di computer virtuali Nutanix AHV contemporaneamente. Negli ambienti che contengono molti computer virtuali associati a un server proxy, una quantità elevata di backup simultanei può compromettere le prestazioni del backup e della rete.

Nota: se il numero di processi simultanei supera il limite specificato, i processi oltre il limite vengono messi in coda.

Nota: se il numero massimo di processi di backup VMware simultanei supera il limite di connessioni del server ESX, potrebbe verificarsi un errore di comunicazione tra il server ESX e il proxy di backup. Inoltre, il file system dell'archivio dati del server ESX potrebbe rimanere bloccato. In tali casi, riavviare il server ESX o eseguire la migrazione del computer virtuale bloccato in un altro archivio dati per sbloccare il computer virtuale. Per ulteriori informazioni, fare riferimento al documento VMware (VMware KB:1022543).

Effettuare le operazioni seguenti:

1. Accedere al sistema proxy del computer virtuale Arcserve UDP.
2. Aprire l'editor del Registro di sistema di Windows e cercare la seguente chiave:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
   ```

3. Individuare le chiavi seguenti:

   ```
   VMwareMaxJobNum
   ```

   ```
   HyperVMaxJobNum
   ```

   ```
   AHVMaxJobNum
   ```

   Nota: entrambe le chiavi sono state già create e i valori predefiniti sono rispettivamente 4 e 10.

4. Fare clic con il pulsante destro del mouse su VMMaxJobNum, HyperVMaxJobNum o AHVMaxJobNum, quindi selezionare Modifica dal menu di scelta rapida.

   Viene visualizzata la finestra di dialogo di modifica della stringa.

5. Nel campo Dati valore specificare il numero di processi di backup che si desidera eseguire simultaneamente.
   - **Limite massimo** - 1
   - **Limite massimo** - nessuno
   - **Valore predefinito**: 10 per Hyper-V e 4 per VMware e Nutanix AHV
6. Fare clic su OK.

   Il limite è definito.

   Il limite dei processi di backup simultanei è stato definito.

(Facoltativo) Esecuzione di un backup manuale

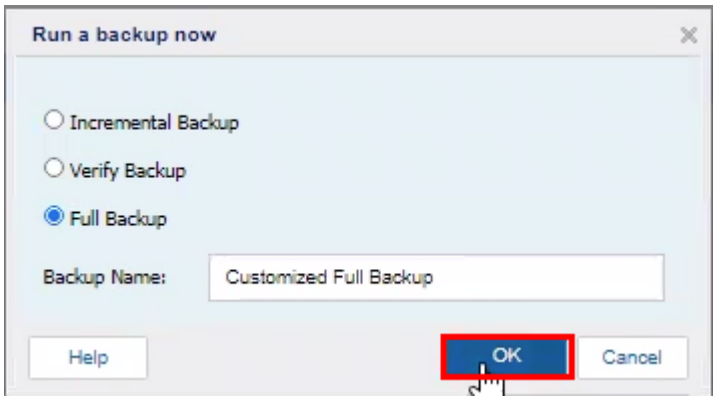
In genere, i backup vengono eseguiti automaticamente e vengono controllati attraverso le impostazioni di pianificazione. In aggiunta al backup pianificato, un backup manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze. Ad esempio, se si dispone di una pianificazione di ripetizione per backup completi, incrementali e di verifica e si desidera apportare modifiche sostanziali al computer, sarà necessario eseguire un backup manuale immediato senza attendere l'esecuzione del successivo backup pianificato.

Effettuare le operazioni seguenti:

1. Accedere alla console Arcserve UDP.
2. Accedere a **Risorse** > **Piano** > **Tutti i piani**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i piani.
3. Fare clic con il pulsante destro del mouse sul piano, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
4. Nella finestra di dialogo Esegui backup immediato, selezionare il tipo di backup che si desidera eseguire, quindi specificare il nome del backup, se necessario.



Le opzioni disponibili sono:

Backup incrementale

Avvia un backup incrementale del computer. Un backup incrementale esegue il backup solo dei blocchi modificati dopo l'ultimo backup.

Nota: se si esegue un backup per la prima volta, il backup completo viene avviato automaticamente anche se è stata selezionata l'opzione Backup incrementale.

I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup con dimensioni molto ridotte. Questa modalità di esecuzione backup è ottimale.

Backup di verifica

Avvia un backup di verifica individuando il backup più recente di ciascun blocco e ne confronta il contenuto e le informazioni con l'origine. Questo confronto consente di verificare che il blocco di backup più recente rappresenti le informazioni corrispondenti all'origine. Se l'immagine di backup di un blocco non corrisponde all'origine, l'agente Arcserve UDP (Windows) aggiornerà (risincronizzerà) il backup di tale blocco.

Vantaggi: viene prodotta un'immagine di backup di dimensioni molto ridotte rispetto al backup completo, poiché viene eseguito solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono all'ultimo backup.

Svantaggi: la velocità del backup è ridotta poiché tutti i blocchi del disco di origine vengono confrontati con i blocchi dell'ultimo backup.

Backup completo

Avvia un backup completo dell'intero computer o dei volumi selezionati.

Note:

- Se si aggiunge un nuovo volume all'origine di backup, il volume appena aggiunto verrà sottoposto a un backup completo, indipendentemente dal metodo di backup generale utilizzato.
- Se non viene specificato alcun nome di backup, per impostazione predefinita viene automaticamente denominato Backup completo personalizzato/Incrementale/Di verifica.

5. Fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.

6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.

7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Nota: è possibile eseguire un solo processo alla volta. Se si tenta di avviare manualmente un processo di backup durante l'esecuzione di un altro processo, verrà visualizzato un messaggio di avviso indicante che un altro processo è in esecuzione, per cui sarà necessario riprovare in un momento successivo.

   Il backup manuale è stato eseguito correttamente.

Nota: È inoltre possibile attivare il backup manuale. Fare clic con il pulsante destro del mouse su un piano e selezionare **Esegui backup** tra le opzioni disponibili. In questo caso, se il piano protegge oggetti contenitore di vSphere, UDP attiverà il backup per tutti i computer virtuali presenti nel contenitore.

Verifica del piano

Per verificare il backup, confermare di avere creato correttamente il piano di backup. Dopo avere verificato che il piano è stato creato correttamente, confermare se il processo di backup è in esecuzione secondo quanto pianificato. È possibile verificare lo stato dei processi di backup dalla scheda Processi.

Effettuare le operazioni seguenti: per la verifica dei piani

1. Fare clic sulla scheda Risorse.
2. Dal riquadro sinistro, accedere a Nodi, quindi fare clic su Tutti i nodi.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Effettuare le operazioni seguenti: per la verifica dei processi di backup

1. Fare clic sulla scheda Jobs (Processi).
2. Dal riquadro sinistro, fare clic su Tutti i Processi.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Creazione di un piano di Virtual Standby su AWS EC2

Lo standby virtuale converte i punti di ripristino in formati di computer virtuale su un cloud specifico e prepara una snapshot per recuperare facilmente i dati qualora necessario. Questa funzionalità fornisce anche la capacità High Availability e garantisce che il computer virtuale possa intervenire immediatamente quando si verifica un errore nel computer di origine. Il computer virtuale di standby viene creato mediante la conversione dei punti di ripristino in un formato del computer virtuale AWS EC2 di Amazon.

Nota: L'attività Virtual Standby viene eseguita solo se l'attività di backup crea una snapshot valida del punto di ripristino. Se l'attività di backup non riesce, l'attività Virtual Standby viene ignorata.

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di un piano con un'attività di backup
3. Aggiunta al piano di un'attività Virtual Standby su EC2
4. (Facoltativo) Esecuzione manuale dell'attività Virtual Standby su EC2
5. Sospensione e riattivazione del processo Virtual Standby.
6. Verifica del piano
7. Interruzione delle risorse EC2

Verifica delle considerazioni e dei prerequisiti

Verificare se i prerequisiti seguenti sono stati completati:

- Accedere alla console.
- Installare il componente server e creare gli archivi dati qualora si desideri archiviare i dati di backup nei Recovery Point Server.
- Si dispone di un punto di ripristino valido per creare un computer Virtual Standby. I punti di ripristino possono provenire da una delle attività seguenti:
  - Backup di Windows basato su agente
  - Backup senza agente basato su host
  - Replica
  - Replica da un Recovery Point Server
- Eseguire il backup del computer completo per abilitare l'attività Virtual Standby. Non è possibile creare un'attività Virtual Standby se il backup non è completo.
- Installare il volume di sistema sul primo disco. Verificare che il volume di sistema e il volume di avvio del computer di origine si trovino sullo stesso disco.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.
- Configurare l'impostazione Gruppo di protezione su EC2 per aprire le porte corrispondenti per l'accesso in entrata, inclusi TCP 8014 e TCP 4091.
- Verificare che l'account AWS di Amazon possa accedere a AWS S3 e AWS EC2. Arcserve UDP non fornisce l'account.
- È necessario installare il volume di sistema sul primo disco. Verificare che il volume di sistema e il volume di avvio del computer di origine si trovino sullo stesso disco.
- Sono necessarie autorizzazioni specifiche dell'API AWS affinché gli utenti Amazon IAM possano ottenere il controllo e interagire con le API AWS per VSB su EC2. Per ulteriori informazioni, consultare la sezione Configurazione delle autorizzazioni granulari IAM per gli utenti IAM con VSB su EC2.

Considerazioni:

- Virtual Standby per l'attività EC2 non supporta l'avvio del computer di origine dal firmware UEFI a causa di una limitazione AWS EC2 di Amazon.

- .NET framework 4.5 è necessario sul computer di origine per installare il driver PV di Amazon per Virtual Standby sull'attività EC2.
- Il volume di sistema e quello di avvio sul nodo di origine nel piano da VSB a EC2 devono trovarsi sul primo disco a causa delle limitazioni di AWS.
- Non è possibile applicare la personalizzazione dell'impostazione TCP/IP alla prima interfaccia di rete nell'istanza EC2 a causa delle limitazioni di AWS.
- L'assegnazione dell'indirizzo IP elastico è disponibile solo per la prima interfaccia di rete nell'istanza EC2.
- La personalizzazione dell'impostazione TCP/IP è applicabile allo scenario solo quando è configurato l'accesso diretto o VPN tra il sito principale e la rete AWS. In caso contrario, la personalizzazione rende l'istanza EC2 inaccessibile.
- Non è possibile modificare la proprietà per abilitare o disabilitare l'indirizzo IP pubblico con assegnazione automatica nel piano per i nodi esistenti, per cui l'aggiornamento interessa solo i nuovi nodi aggiunti al piano.
- È necessario installare PowerShell versione 3.0 (o versioni successive) sul computer di origine prima di configurare VSB su EC2 per i tipi di istanza seguenti:

  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, and z1d

Configurazione delle autorizzazioni granulari IAM per gli utenti IAM con VSB su EC2

In questa sezione sono illustrati i passaggi e i criteri di autorizzazione API richiesti per l'agente Arcserve UDP installato sul proxy VSB Cloud nei servizi Amazon Web Services EC2. Le autorizzazioni consentono di eseguire le azioni richieste per il trasferimento dei dati e di Virtual Standby al cloud AWS EC2.

La procedura descritta permette a un utente Amazon IAM di ottenere il controllo ed interagire con l'API AWS. Il criterio di autorizzazione viene applicato non solo direttamente all'utente, ma anche al ruolo e al gruppo nell'interfaccia IAM Security di Amazon Web Services.

Effettuare le operazioni seguenti:

1. Accedere come amministratore ad Amazon Web Services.
2. Selezionare My Security Credentials, fare clic su **Users** a sinistra, quindi fare clic sul pulsante **Create New Users**.
3. Inserire il nome utente desiderato.

   Nota: verificare che l'opzione per la **generazione di una chiave d'accesso per ogni utente** sia selezionata.
4. Fare clic sul pulsante **Create**.
5. Fare clic su **Download Credentials**.

   Le credenziali contengono il codice di accesso e la chiave privata necessaria in seguito per la Console UDP.
6. Dalla visualizzazione Users, selezionare l'utente dall'elenco e fare clic sulla scheda Permissions, disponibile nella parte inferiore.
7. Dall'opzione Custom Policy creare un criterio personalizzato in linea per l'utente.
8. Immettere un nome per il criterio e incollare il contenuto seguente in Document Policy.

```
{
"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. Fare clic su **Apply Policy**.
10. Nella Console UDP, utilizzare il codice di accesso dell'utente IAM e il codice di accesso di protezione per creare un piano da VSB a EC2.

Creazione di un piano con un'attività di backup

Un piano include diversi tipi di attività da eseguire. Per creare un computer Virtual Standby, creare un piano che include un'attività di backup e un'attività Virtual Standby. Un'attività di backup esegue un backup dei nodi di origine e archivia i dati nella destinazione specificata. Questi dati di backup vengono quindi utilizzati dalla funzionalità Virtual Standby e convertiti in un formato di computer virtuale.

È possibile creare un computer Virtual Standby da un backup Windows basato su agente e da un backup basato su host senza agente. Inoltre, è possibile creare un computer Virtual Standby dai dati replicati mediante l'attività **Replica**. La procedura seguente è un esempio di come creare un backup Windows basato su agente.

Note:

- Per ulteriori informazioni sul backup senza agente basato su host, consultare la sezione Creazione di un piano di backup di un computer virtuale basato su host.
- Per ulteriori informazioni sulla replica dei dati di backup, consultare la sezione Replica dei dati tra archivi dati gestiti da una console UDP e gestiti da console UPD diverse.
- Virtual Standby su EC2 NON supporta l'avvio del computer di origine dal firmware UEFI a causa delle limitazioni Amazon AWS EC2.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

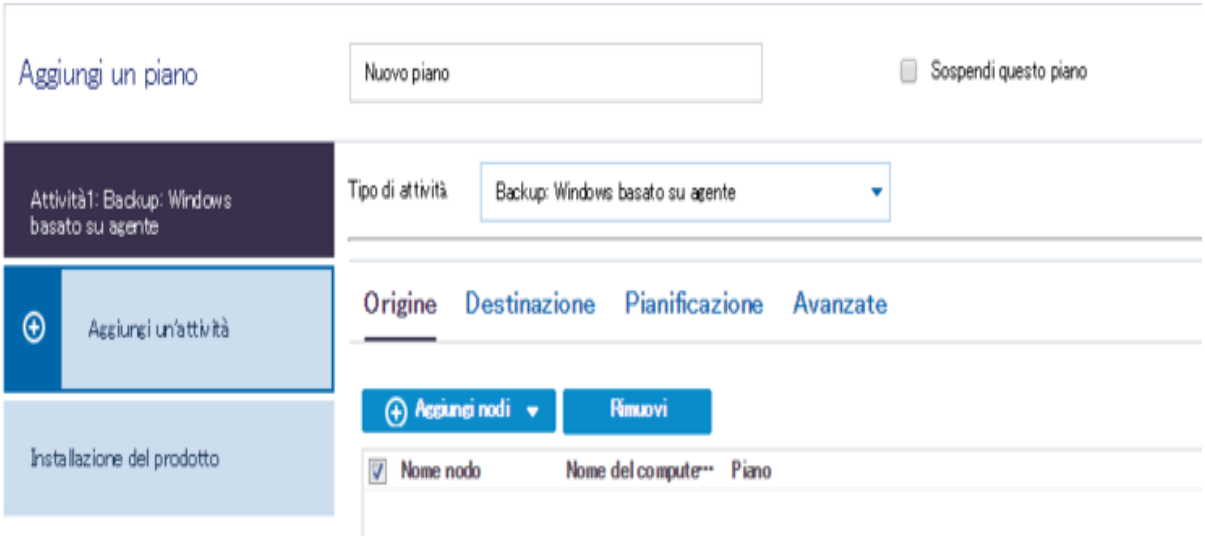
   Viene visualizzata la finestra di dialogo **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile

eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.

6. Dall'elenco a discesa **Tipo di attività**, selezionare **Backup, Windows basato su agente**.



Specificare quindi i dettagli per i campi Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine che si desidera proteggere. È possibile selezionare più di un nodo per un piano. Se non sono stati aggiunti nodi alla console, è possibile aggiungerli in fase di creazione o modifica di un piano dalla pagina Origine. È inoltre possibile salvare un piano senza aggiungere nessun nodo di origine. Il piano viene distribuito soltanto dopo l'aggiunta dei nodi di origine.

Effettuare le operazioni seguenti:

1. Nella scheda Origine, fare clic su **Aggiungi**.
2. Selezionare una delle seguenti opzioni:

   Selezionare i nodi da proteggere in Arcserve UDP

   Consente di visualizzare la finestra di dialogo Selezionare i nodi da proteggere in Arcserve UDP. Selezionare i nodi dall'elenco visualizzato. Selezionare questa opzione se sono stati già aggiunti nodi alla Console.

   Aggiungi nodo Windows

   Viene visualizzata la finestra di dialogo Aggiungi nodi a un piano. Selezionare questa opzione se non sono stati aggiunti nodi e si desidera aggiungere manualmente i nodi da proteggere.

   Rileva nodi da Active Directory

   Consente di aprire la finestra di dialogo Aggiungi nodi alla Console Arcserve UDP. Selezionare questa opzione se si desidera rilevare e aggiungere nodi da Active Directory.
3. Se è stata selezionata l'opzione **Selezionare i nodi da proteggere in Arcserve UDP**, nella finestra di dialogo Selezionare i nodi da proteggere, procedere come segue:
   a. (Facoltativo) Selezionare un filtro dall'elenco a discesa Gruppi per filtrare i nodi. Immettere parole chiave per applicare ulteriori filtri ai nodi.

      I nodi vengono visualizzati nella colonna Nodi disponibili.

   b. Selezionare i nodi dalla colonna Nodi disponibili, quindi fare clic sulla freccia destra singola (>) o sulla freccia destra doppia (>>) per spostare rispettivamente i nodi selezionati o tutti i nodi nella colonna Nodi selezionati.

      I nodi vengono visualizzati nella colonna Nodi selezionati.

   c. Fare clic su **OK** per chiudere la finestra di dialogo.



4. Per scegliere il Tipo di protezione, selezionare una delle seguenti opzioni:

   Backup di tutti i volumi

   Prepara una snapshot del backup di tutti i volumi.

   Backup dei volumi selezionati

   Prepara una snapshot del backup del volume selezionato.

   L'origine viene specificata.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Selezionare un **Tipo di destinazione** tra quelli elencati di seguito:

   Disco locale o cartella condivisa

   Specifica che la destinazione di backup è una destinazione locale o una cartella condivisa. Se si seleziona questa opzione, è possibile salvare i dati come punti di ripristino o set di ripristino. Le opzioni dei punti di ripristino e dei set di ripristino sono disponibili nella scheda **Pianificazione.**

   Recovery Point Server di Arcserve UDP

   Specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono memorizzati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.

2. Se è stato selezionato il **Recovery Point Server di Arcserve UDP**, immettere i seguenti dettagli:
   a. Selezionare un Recovery Point Server.
   b. Selezionare un archivio dati. L'elenco mostra tutti gli archivi dati creati sul Recovery Point Server specificato.
   c. Fornire una password di sessione.
   d. Confermare la password di sessione.
3. Se è stata selezionata l'opzione **Utilizza il disco locale o la cartella condivisa**, fornire i dettagli seguenti:
   a. Fornire il percorso completo della destinazione locale o di rete. Per la destinazione di rete, specificare le credenziali con l'accesso di scrittura.
   b. Selezionare l'algoritmo di crittografia. Per ulteriori informazioni, consultare la sezione Impostazioni di crittografia.
   c. Facoltativamente, fornire una password di crittografia.
   d. Confermare la password di crittografia.
   e. Selezionare un tipo di compressione. Per ulteriori informazioni, consultare la sezione Tipo di compressione.

Nota: Se si archiviano i dati in un disco locale o in una cartella condivisa, non è possibile replicare i dati in un altro Recovery Point Server. La replica è supportata solo se si archiviano i dati in un Recovery Point Server.

La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

Effettuare le operazioni seguenti:

1. (Facoltativo) Selezionare l'opzione per la gestione dei punti di ripristino. Questa opzione è visibile solamente se sono state selezionate le cartelle Locale o Condivisa come destinazione di backup.

   Conserva per punti di ripristino

   I dati di backup vengono archiviati come punti di ripristino.

   Conserva per set di ripristino

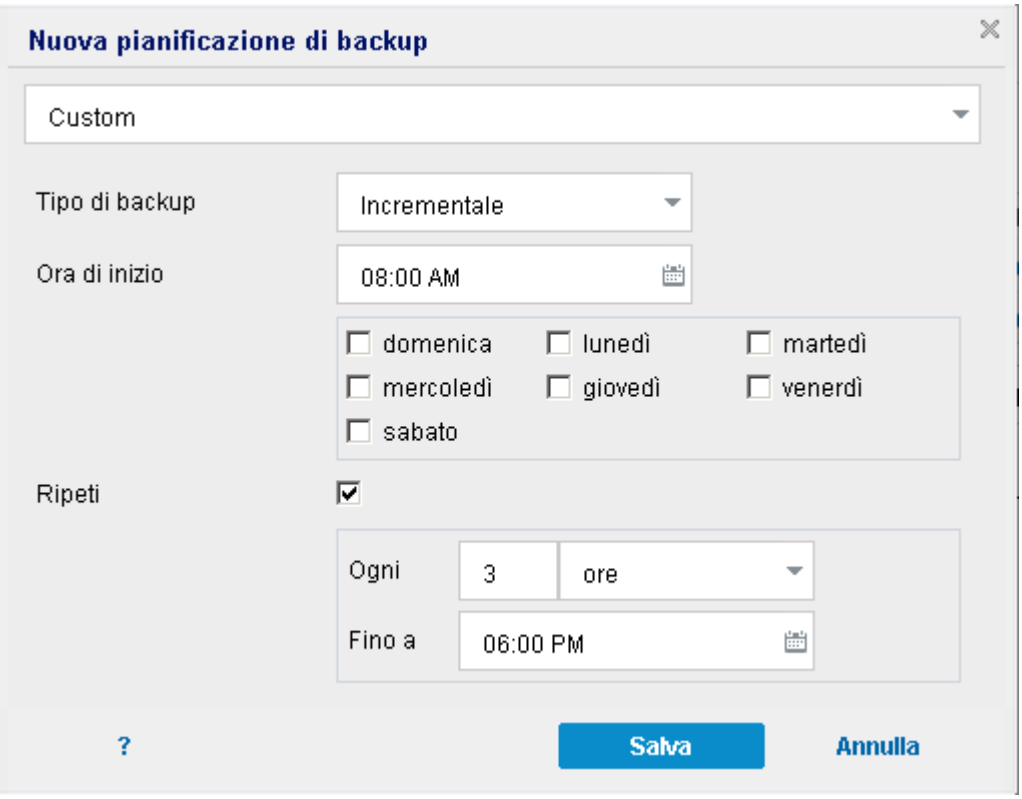
   I dati di backup vengono archiviati come set di ripristino.

2. Aggiungere le pianificazioni di backup, di unione e di definizione del limite di velocità

   Aggiunta di una pianificazione di backup

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base

alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni di backup.

Verifica

Specifica la pianificazione dei backup di verifica.

Arcserve UDP controlla che i dati protetti siano validi e completi eseguendo una verifica di affidabilità dell'immagine di backup archiviata sull'origine di backup. Se necessario esegue la risincronizzazione dell'immagine. Un backup di verifica controlla il backup più recente di ogni blocco e lo confronta con il contenuto e le informazioni di origine. Questo confronto consente di verificare che le informazioni corrispondenti all'origine siano contenute nel blocco di backup più recente. Se l'immagine di backup di un blocco non corrisponde all'origine (probabilmente a causa di modifiche apportate al sistema dall'ultimo backup), Arcserve UDP aggiorna (risincronizza) il backup del blocco non corrispondente. Sebbene si tratti di una procedura poco frequente, il backup di verifica può essere utilizzato per ottenere le stesse garanzie di un backup completo, ma senza occupare lo stesso spazio.

Vantaggi: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.

Svantaggi: il backup di verifica richiede tempi di esecuzione più lunghi, in quanto esegue il confronto di tutti i blocchi originali con i blocchi del backup più recente.

Incrementale

Specifica la pianificazione dei backup incrementali.

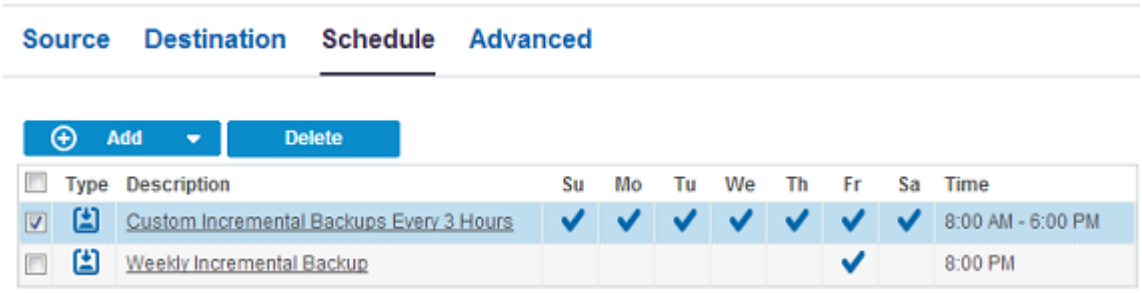
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su Aggiungi e selezionare Aggiungi pianificazione di unione.

   La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

b. Specificare l'ora di inizio per l'avvio del processo di unione.

c. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

d. Fare clic su **Salva**.

   La Pianificazione di unione viene specificata e visualizzata nella pagina **Pianificazione.**

Aggiungi pianificazione del limite delle risorse

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

   Viene visualizzata la finestra di dialogo Aggiungi nuova pianificazione del limite delle risorse.

b. Specificare il limite di velocità effettiva in MB per unità di minuti.

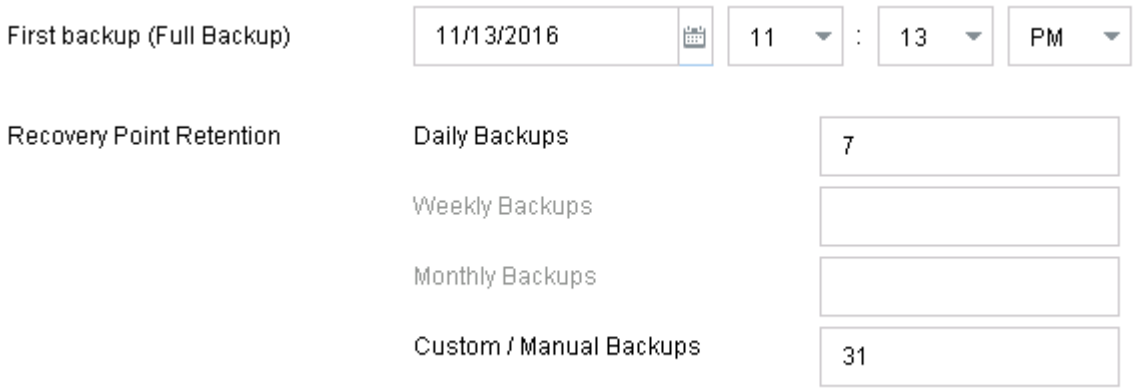
c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

   La pianificazione del limite delle risorse specificata viene visualizzata nella pagina **Pianificazione**.

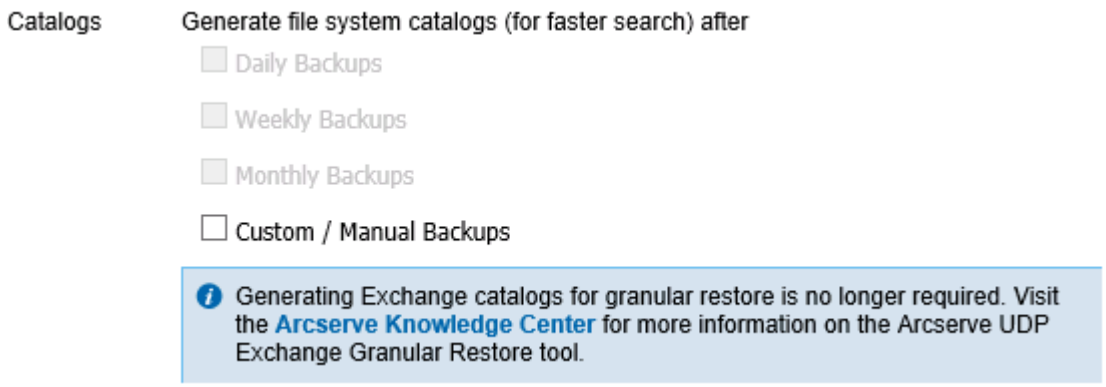
3. Specificare l'ora di inizio per il backup pianificato.



4. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo Pianificazione di backup.

5. Specificare i dettagli relativi al catalogo.



   I cataloghi permettono di generare il catalogo file system. Il catalogo file system è necessario per migliorare e velocizzare la ricerca. Se si selezionano le caselle di controllo del catalogo, i cataloghi verranno abilitati in base al tipo di backup specificato. Deselezionare una casella di controllo per disattivare la generazione del catalogo.

   Viene specificata la pianificazione.

Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione

L'opzione di pianificazione consente di specificare una pianificazione personalizzata o una pianificazione giornaliera/settimanale/mensile o entrambe. Nella pianificazione personalizzata è possibile configurare la pianificazione del backup per ciascun giorno della settimana e aggiungere fino a quattro pianificazioni di backup ogni giorno. È possibile selezionare un giorno specifico di una settimana e creare un intervallo di tempo per definire quando eseguire il backup e la frequenza.

Pianificazione	Processo supportato	Commenti
Backup	Processo di backup	Definire gli intervalli di tempo per eseguire i processi di backup.
Limitazione della velocità di backup	Processo di backup	Definire gli intervalli di tempo per controllare la velocità di backup.
Unione	Processo di unione	Definire quando unire i processi.
Pianificazione quotidiana	Processo di backup	Definire quando eseguire processi di backup quotidiani.
Pianificazione settimanale	Processo di backup	Definire quando eseguire processi di backup settimanali.
Pianificazione mensile	Processo di backup	Definire quando eseguire processi di backup mensili.

È inoltre possibile specificare le impostazioni di memorizzazione per i punti di ripristino.

Nota: All'interno di ogni piano è necessario configurare le impostazioni di conservazione per controllare il modo in cui i nodi assegnati a tale piano vengono memorizzati nell'archivio dati di destinazione.

Le pianificazioni per i backup giornalieri/settimanali/mensili sono indipendenti dalla pianificazione personalizzata e gli uni dagli altri. È possibile configurare di eseguire solo il backup giornaliero, il backup settimanale o il backup mensile senza configurare la pianificazione personalizzata.

Pianificazione del processo di backup

È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del backup. Un intervallo di tempo valido è dalle 00:00 alle 23:59. Non è possibile specificare un intervallo di tempo come ad esempio dalle 18:00 alle 06:00. In tali casi, si devono specificare manualmente due intervalli di tempo diversi.

Per ogni intervallo di tempo l'ora di inizio è inclusa e l'ora di fine è esclusa. Ad esempio, si è configurato il backup incrementale da eseguire ogni ora tra le 06:00 e le 09:00 e il backup inizierà alle 06:00. Ciò significa che il backup verrà eseguito alle 06:00, alle 07:00 e 08:00, ma NON alle 09:00.

Nota: Se si desidera eseguire il processo di backup ripetutamente fino al termine della giornata, impostare la pianificazione fino alle 00:00. Ad esempio, per eseguire un processo di backup ogni 15 minuti per l'intera giornata, impostare la pianificazione dalle 00:00 alle 00:00 ogni 15 minuti.

Pianificazione del limite delle risorse di backup

La pianificazione del limite delle risorse di backup consente di controllare la velocità effettiva di backup, che a sua volta controlla l'utilizzo delle risorse (I/O del disco, CPU, larghezza di banda della rete) del server di cui si esegue il backup. Questo è utile se non si desidera influire sulle prestazioni del server durante i normali orari di ufficio. È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del limite delle risorse di backup. Per ogni intervallo di tempo è possibile specificare un valore, in MB per minuto. Questo valore viene utilizzato per controllare la velocità effettiva di backup. I valori validi sono compresi tra 1 MB/minuto a 99999 MB/minuto.

Se un processo di backup si estende oltre il tempo specificato, il limite della velocità cambia in conformità all'intervallo di tempo specificato. Ad esempio, il limite delle risorse di backup definito è 500 MB/minuto dalle 08:00 alle 20:00 e 2500 MB/minuto dalle 20:00 alle 22:00. Se un processo di backup inizia alle 19:00 e viene eseguito per tre ore, dalle 19:00 alle 20:00 il limite della velocità è pari a 500 MB/minuto e dalle 20:00 alle 22:00 a 2500 MB/minuto.

Se non si definisce alcuna pianificazione del backup e della sua velocità effettiva, il backup viene eseguito il più rapidamente possibile.

Pianificazione di unione

Consente di unire i punti di ripristino in base alla pianificazione fornita.

Considerare i punti seguenti per il processo di unione:

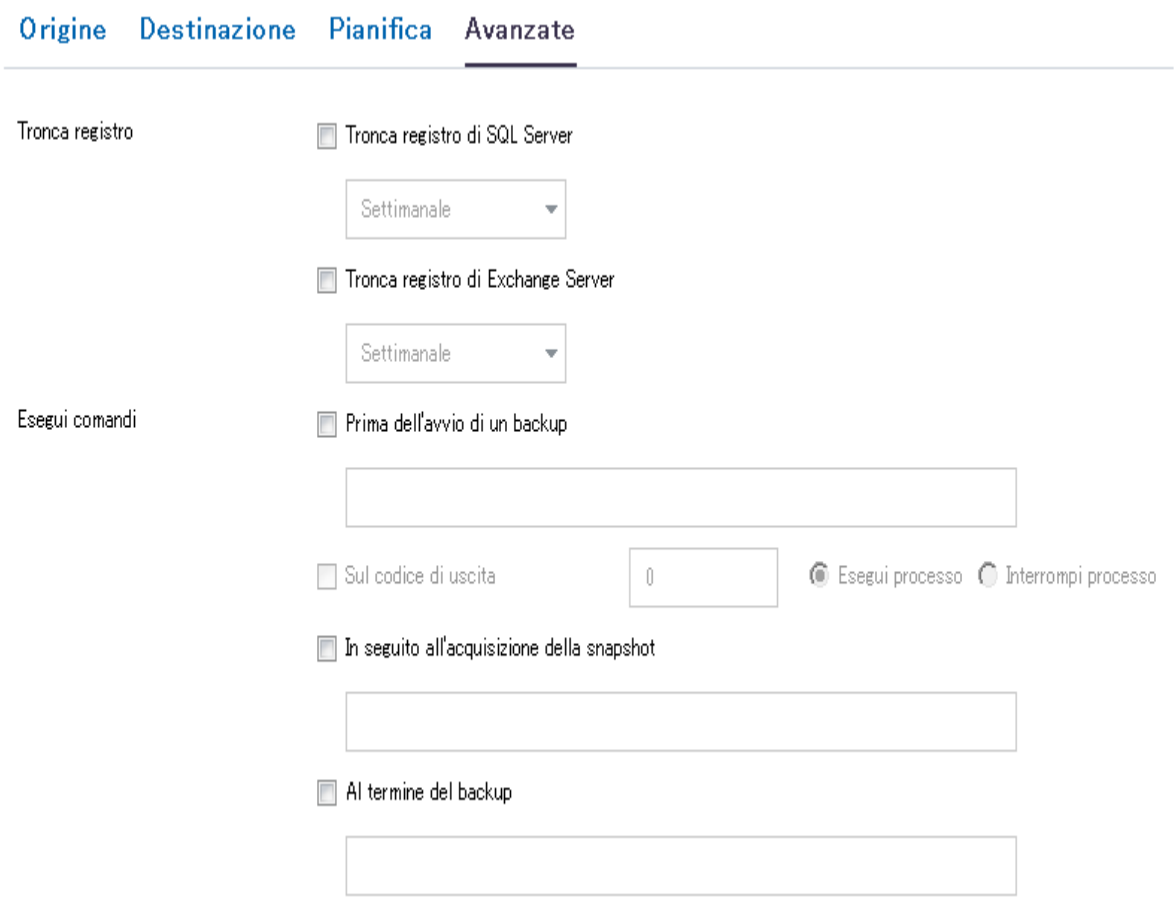
- In qualsiasi momento è possibile eseguire solo un processo di unione per un nodo.
- Se un processo di unione inizia, esso deve essere completato prima di poter avviare il processo di unione successivo. Ciò significa che se uno o più set di punti di ripristino vengono uniti, non è possibile aggiungere nuovi punti di ripristino a questo processo di unione finché il processo di unione dell'insieme corrente dei punti di ripristino non viene completato.

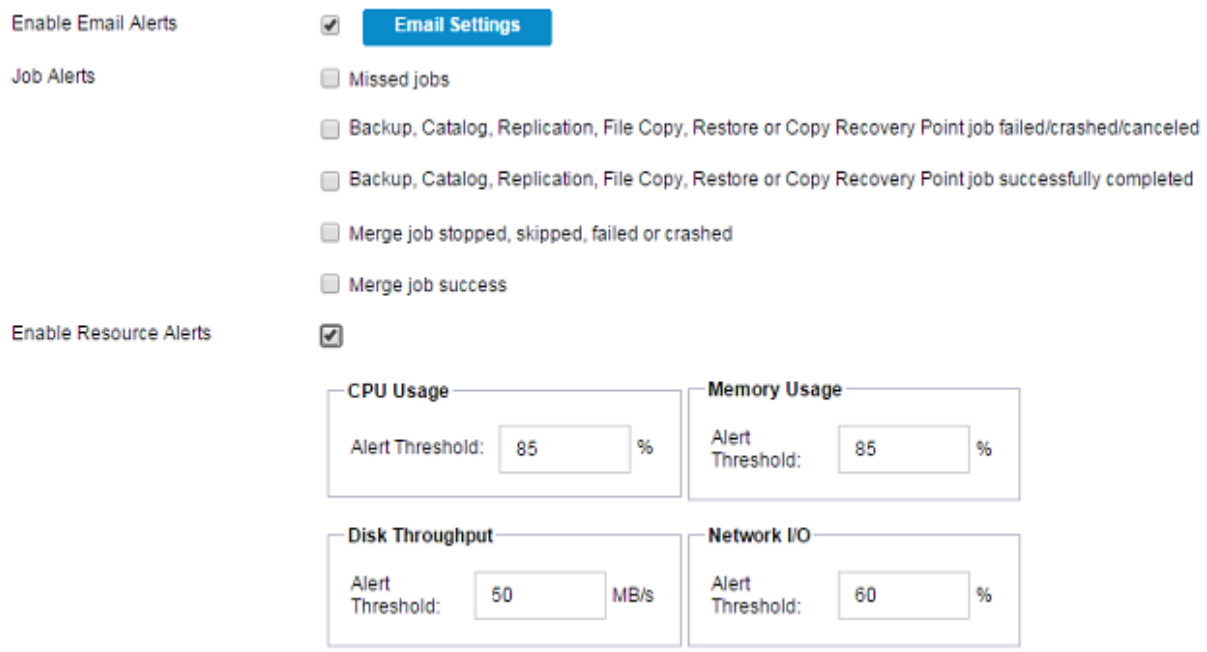
- Se un processo di unione sta elaborando più di un set di punti di ripristino (ad esempio set [1~4], set [5~11] e set [12~14] sono tre set distinti), il Recovery Point Server elabora tali set uno alla volta.
- Se un processo di unione viene ripreso dopo una pausa, il processo individua in quale punto era stato interrotto e riprende l'unione da tale punto.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione delle impostazioni per troncare i registri, l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda Avanzate:





Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

Tronca registro

Consente di specificare la pianificazione per troncare i registri per SQL Server ed Exchange Server. È possibile specificare la pianificazione come **Giornaliero**, **Settimanale** o **Mensile**.

Nome utente

Consente di specificare l'utente autorizzato per l'esecuzione di uno script.

Password

Consente di specificare la password dell'utente autorizzato all'esecuzione dello script.

Esegui un comando prima dell'avvio del backup

Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Esegui processo** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

Esegui un comando dopo l'acquisizione della snapshot

Consente di eseguire uno script dopo l'acquisizione della snapshot del backup. Specificare il percorso di archiviazione dello script.

Esegui un comando al completamento del backup

Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso di archiviazione dello script.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere mediante posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

Abilita avvisi sulle risorse

Consente di specificare una soglia per Utilizzo CPU, Memoria, Velocità del disco, I/O di rete. È possibile fornire il valore in percentuale. Si riceve un messaggio di posta elettronica al superamento del valore Soglia di avviso.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su Salva.

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: Se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo.

Il piano di backup viene creato e distribuito automaticamente al nodo di origine. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

Aggiunta al piano di un'attività Virtual Standby su EC2

Creare un'attività Virtual Standby su EC2 in modo che i dati di backup vengano convertiti in un formato di computer virtuale e venga creato un computer virtuale.

Note:

- Virtual Standby su EC2 non supporta l'avvio automatico del computer virtuale.
- Se il piano viene interrotto, il processo Virtual Standby non verrà avviato. Quando il piano viene ripreso, il processo di Virtual Standby non viene ripreso automaticamente. Per avviare il processo Virtual Standby è necessario eseguire un altro processo di backup manualmente. Pertanto, se il piano viene interrotto, l'opzione Sospendi/Riprendi Virtual Standby non sarà disponibile. Se non si desidera che il computer virtuale venga avviato automaticamente dopo l'interruzione del piano, è necessario interrompere manualmente l'heartbeat per i nodi.

Effettuare le operazioni seguenti:

1. Fare clic su **Aggiungi un'attività** dal riquadro sinistro.

   Viene aggiunta una nuova attività al riquadro sinistro.

2. Dal menu a discesa **Tipo di attività**, selezionare **Virtual Standby**.

   Viene aggiunta l'attività Virtual Standby.

3. Dalla scheda **Origine**, selezionare un'origine per l'attività Virtual Standby.
4. Fare clic sulla scheda **Server di virtualizzazione**.
5. Selezionare il tipo di virtualizzazione EC2 e immettere i dettagli corrispondenti.

   Tipo di virtualizzazione: EC2

   Nome account

   Selezionare l'account Amazon AWS esistente per accedere ad AWS EC2. È inoltre possibile aggiungere un nuovo account facendo clic su **Aggiungi**. Per ulteriori informazioni, consultare la sezione Aggiunta di un account cloud per Amazon EC2.

   Area EC2

   Selezionare l'area EC2 in cui si trova il proxy cloud. Arcserve UDP supporta tutte le aree globali EC2 e l'area cinese EC2.

   Nota: l'account specificato deve essere un account amministratore o un account con privilegi di amministratore sul sistema EC2.

Proxy cloud VSB

Specificare un'istanza EC2 selezionata per l'area come proxy cloud.

Nota: nell'istanza EC2 deve essere installato l'agente Arcserve UDP.

Nome utente e Password

Specificare le credenziali per accedere al proxy cloud VSB.

Protocollo

Specificare HTTP o HTTPS come protocollo da utilizzare per la comunicazione tra l'agente Arcserve Unified Data Protection di origine e il proxy cloud VSB.

Porta

Specificare la porta che si desidera utilizzare per il trasferimento dei dati tra il server di origine e il proxy cloud VSB.

Nota: poiché il proxy cloud viene utilizzato per il trasferimento dei dati, le porte corrispondenti devono essere abilitate per l'accesso in entrata al gruppo di protezione AWS EC2, comprese le porte TCP 8014 e 4091.

6. Fare clic sulla scheda **Computer virtuale** e immettere i dettagli per l'impostazione di base, l'impostazione dell'archiviazione cloud e le impostazioni di rete.

   Amazon AWS EC2

   Per sistemi Amazon AWS EC2, applicare le opzioni seguenti al computer virtuale:

   Prefisso nome del computer virtuale

   Specificare il prefisso che si desidera aggiungere al nome visualizzato per il computer virtuale sul sistema AWS EC2.

   Valore predefinito: UDPVM_

   Snapshot del punto di ripristino

   Specificare il numero di snapshot del punto di ripristino (punti di ripristino) per il computer Virtual Standby. Il numero massimo di snapshot del punto di ripristino è 29 per AWS EC2.

   Combina tutte le sessioni non convertite in una snapshot del singolo punto di ripristino

   Consente di specificare se si desidera combinare tutte le sessioni convertite in una singola snapshot del punto di ripristino con l'esecuzione del processo VSB successivo.

   Impostazione predefinita: opzione selezionata

   Tipo di istanza

Amazon EC2 fornisce un'ampia scelta di tipi di istanze ottimizzate per l'utilizzo in diversi casi. Le istanze sono server virtuali che eseguono applicazioni. Dispongono di combinazioni diverse di memoria CPU, di archiviazione e di capacità di rete. Forniscono inoltre la flessibilità di poter scegliere le risorse adeguate per le proprie applicazioni. Per ulteriori informazioni sui tipi di istanze e sulle diverse esigenze di elaborazione corrispondenti, fare clic sul seguente collegamento.

Tipo di volume EBS

I volumi generici (SSD) possono essere suddivisi in 3000 IOP e fornire una previsione costante di 3 IOP/GiB. I volumi IOP forniti possono fornire un massimo di 20000 IOP e rappresentano la soluzione ideale per le istanze ottimizzate per EBS. I volumi magnetici, precedentemente noti come volumi standard, forniscono una media di 100 IOP e possono essere suddivisi in centinaia di IOP. Per ulteriori informazioni sui tipi di volume EBS, visualizzare il seguente collegamento.

Rete

Consente di definire le subnet VCP, le NIC e i gruppi di protezione per il computer virtuale Virtual Standby su AWS EC2.

Nota: quando l'indirizzo IP pubblico di assegnazione automatica è attivato, a causa delle limitazioni di AWS EC2 viene eseguito soltanto il mapping su AWS EC2. Gli altri elementi vengono invece scartati.

Stesso numero di schede di rete dell'origine all'ultimo backup

Selezionare questa opzione per definire come eseguire il mapping della NIC virtuale sulla rete virtuale EC2. Specificare questa opzione quando il computer virtuale contiene NIC virtuali e una rete virtuale.

Nota: tali impostazioni sono disponibili per la configurazione solo se l'indirizzo IP pubblico di assegnazione automatica è disattivato.

7. Fare clic su **Salva**.

Le modifiche vengono salvate e l'attività Virtual Standby viene distribuita automaticamente al server Virtual Standby.

Il piano Virtual Standby è stato creato e distribuito correttamente.

Aggiunta della pianificazione del limite di risorse per il trasferimento di dati su cloud

La pianificazione del limite delle risorse consente di controllare la velocità effettiva di trasferimento dei dati su cloud, che a sua volta controlla l'utilizzo delle risorse (larghezza di banda della rete) del server in corso di trasferimento su cloud. Questo è utile se non si desidera influire sulle prestazioni del server durante i normali orari di ufficio. È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del limite delle risorse per il trasferimento di dati su cloud. Per ogni intervallo di tempo è possibile specificare un valore, espresso in Mbps/Kbps. Questo valore viene utilizzato per controllare la velocità effettiva di trasferimento su cloud. I valori validi sono compresi tra 1 Mbps/Kbps e 99999 Mbps/Kbps.

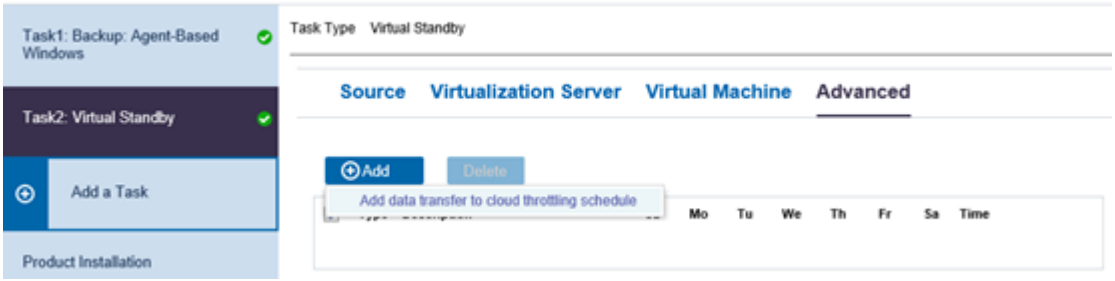
Se il processo di trasferimento dati si estende oltre il tempo specificato, il limite della velocità cambia in conformità all'intervallo di tempo specificato. Ad esempio, il limite di velocità per il trasferimento dati definito è 500 Mbps dalle 08:00 alle 20:00 e 2500 Mbps dalle 20:00 alle 22:00. Se un processo di trasferimento dati inizia alle 19:00 e viene eseguito per tre ore, dalle 19:00 alle 20:00 il limite di velocità è pari a 500 Mbps e dalle 20:00 alle 22:00 a 2500 Mbps.

Se sono presenti più nodi di origine nell'attività di backup con Virtual Standby per l'ambiente cloud, il limite di velocità verrà suddiviso in modo uniforme. Ad esempio, è stato definito il limite di velocità per il trasferimento dati di 500 Mbps e sono presenti due nodi di origine nel piano. Se il trasferimento dati su cloud viene eseguito contemporaneamente, il limite di velocità è pari a 250 Mbps per ogni nodo. Una volta completato il trasferimento di un nodo, il limite di velocità dell'altro nodo in esecuzione diventa 500 Mbps.

Se non si definisce alcuna pianificazione del limite di risorse, il processo di trasferimento dati su cloud viene eseguito il più rapidamente possibile.

Effettuare le operazioni seguenti:

1. Fare clic su Aggiungi pianificazione limite delle risorse per trasferimento dati su cloud.



Viene visualizzata la finestra di dialogo Aggiungi nuova pianificazione del limite delle risorse.

2. Specificare il limite di velocità effettiva in Mbps/Kbps.

   Viene visualizzata la pagina Configurazione di rete del computer virtuale di standby - <node name>.

3. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.
4. Compilare il campo Fino a per specificare un'ora di fine per il processo del limite di velocità effettiva.
5. Fare clic su Salva.

   La pianificazione del limite delle risorse specificata viene visualizzata nella pagina Pianificazione.

Configurazione della rete del computer virtuale Virtual Standby

È possibile attivare il computer virtuale Virtual Standby su AWS EC2 mediante impostazioni di rete personalizzate. È possibile configurare le impostazioni di rete seguenti sul computer virtuale Virtual Standby:

- Specificare la rete virtuale, la scheda di interfaccia di rete e le impostazioni TCP/IP per ciascuna scheda di rete nella scheda **Impostazioni della scheda di rete**.
- Aggiornare i server DNS per reindirizzare i client dal computer di origine ai computer virtuali Virtual Standby in base alle impostazioni TCP/IP della scheda **Impostazioni di aggiornamento DNS**.

Effettuare le operazioni seguenti:

1. Dalla scheda **Risorse**, accedere al gruppo nodi **Virtual Standby**.

   I nodi Virtual Standby vengono mostrati nel riquadro centrale.

2. Nel riquadro centrale selezionare il nodo e fare clic su **Configurazione di rete del computer virtuale di standby**.

   Viene visualizzata la pagina Configurazione di rete del computer virtuale di standby - <node name>.

3. Nella scheda **Impostazioni della scheda di rete** selezionare la rete virtuale dall'elenco **Computer virtuale di standby - Rete virtuale**.
4. Selezionare la subnet dall'elenco a discesa.
5. Selezionare l'indirizzo IP elastico dall'elenco **Elastic IP (Elastic IP)**.
6. Selezionare **Personalizza le impostazioni TCP/IP**.
7. Fare clic sul pulsante **Aggiungi indirizzo** e aggiungere **Indirizzi IP**, **Indirizzi gateway**, **Indirizzi DNS** e **Indirizzi WINS**.

   Nota: Se si aggiungono **Indirizzi DNS**, configurare i server DNS nella scheda **Impostazioni di aggiornamento DNS**.

8. Fare clic su **Salva**.

   La pagina Configurazione di rete del computer virtuale di standby - <node name> viene chiusa.

   La rete del computer virtuale Virtual Standby è configurata.

(Facoltativo) Esecuzione manuale dell'attività Virtual Standby su EC2

Per eseguire manualmente un processo Virtual Standby, occorre prima eseguire un backup manuale. L'attività Virtual Standby sull'attività EC2 è associata a un'attività di backup. Se un piano include un'attività di backup e un'attività Virtual Standby su un'attività EC2, quando si esegue manualmente il processo di backup, il processo Virtual Standby viene eseguito automaticamente dopo il completamento del processo di backup.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Se sono stati aggiunti, questi piani verranno mostrati nel riquadro centrale.
3. Selezionare i nodi di cui si desidera eseguire il backup e ai quali è stato assegnato un piano.
4. Nel riquadro centrale, fare clic su **Azioni**, **Esegui backup**.

   Verrà visualizzata la finestra di dialogo **Esegui un backup immediato**.
5. Selezionare il tipo di backup e fornire un nome al processo di backup.
6. Fare clic su **OK**.

   Il processo di backup viene eseguito.

   Il processo Virtual Standby sul processo EC2 viene eseguito immediatamente dopo la conclusione del processo di backup.

   Il processo Virtual Standby sul processo EC2 viene eseguito manualmente.

Sospensione e riattivazione del processo Virtual Standby

La conversione virtuale è il processo in cui Virtual Standby converte i punti di ripristino di Arcserve Unified Data Protection dai nodi di origine ai formati del computer virtuale, denominati snapshot del punto di ripristino. In caso di errore di un nodo di origine, la funzionalità Virtual Standby utilizza le snapshot del punto di ripristino per attivare un computer virtuale per il nodo di origine.

Si consiglia di impostare il processo di conversione virtuale per il funzionamento continuo. Tuttavia, se si desidera sospendere temporaneamente il processo di conversione virtuale sui server Virtual Standby locali e remoti, è possibile procedere dalla Console. Dopo aver risolto i problemi relativi al nodo di origine, sarà possibile riprendere il processo di conversione virtuale.

Quando i processi di Virtual Standby (processi di conversione) vengono sospesi, l'operazione di sospensione non sospende il processo di conversione attualmente in corso. La sospensione si applica solamente al processo la cui esecuzione è prevista al completamento del successivo processo di backup. Pertanto, il processo di conversione successivo verrà avviato unicamente quando l'utente specifica che desidera riattivare il processo di conversione sospeso.

Se si riprende Virtual Standby per i nodi e se esistono più sessioni di backup senza snapshot del punto di ripristino, viene visualizzata una finestra di dialogo per la selezione dell'opzione di copia intelligente. Se si fa clic su Sì, Virtual Standby converte la sessione combinata in una singola snapshot del punto di ripristino. Se si fa clic su No, Virtual Standby converte ciascuna sessione individualmente

Nota: In via facoltativa, è possibile sospendere e riprendere i processi di Virtual Standby direttamente dai nodi. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi di Virtual Standby.

Effettuare le operazioni seguenti:

1. Accedere all'Arcserve Unified Data Protection.
2. Fare clic sulla scheda **Risorse**.
3. Dal riquadro sinistro, accedere a **Virtual Standby** e fare clic su **Tutti i nodi**.

   Se sono stati aggiunti nodi, questi verranno visualizzati nel riquadro centrale.
4. Selezionare il nodo che si desidera sospendere o riattivare.

5. Nel riquadro centrale, fare clic su **Azioni**, **Virtual Standby**, **Sospendi** o su **Riprendi**.

   La funzione Virtual Standby per il nodo selezionato viene sospesa o ripresa.

Verifica del piano

Per verificare la funzionalità Virtual Standby, confermare la corretta creazione del piano Virtual Standby. Dopo avere verificato che il piano è stato creato correttamente, verificare se il processo di backup sia in esecuzione in base alla pianificazione. Dopo la corretta conclusione del processo di backup, viene eseguito il processo Virtual Standby. È possibile verificare lo stato del processo di backup e del processo Virtual Standby dalla scheda **Jobs** (Processi).

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Per la verifica dei processi Virtual Standby, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Jobs** (Processi).
2. Dal riquadro sinistro, fare clic su **Tutti i Processi**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare la corretta esecuzione del processo di backup e del processo Virtual Standby.

   Il piano per Virtual Standby è stato verificato correttamente.

   Il computer Virtual Standby è stato creato.

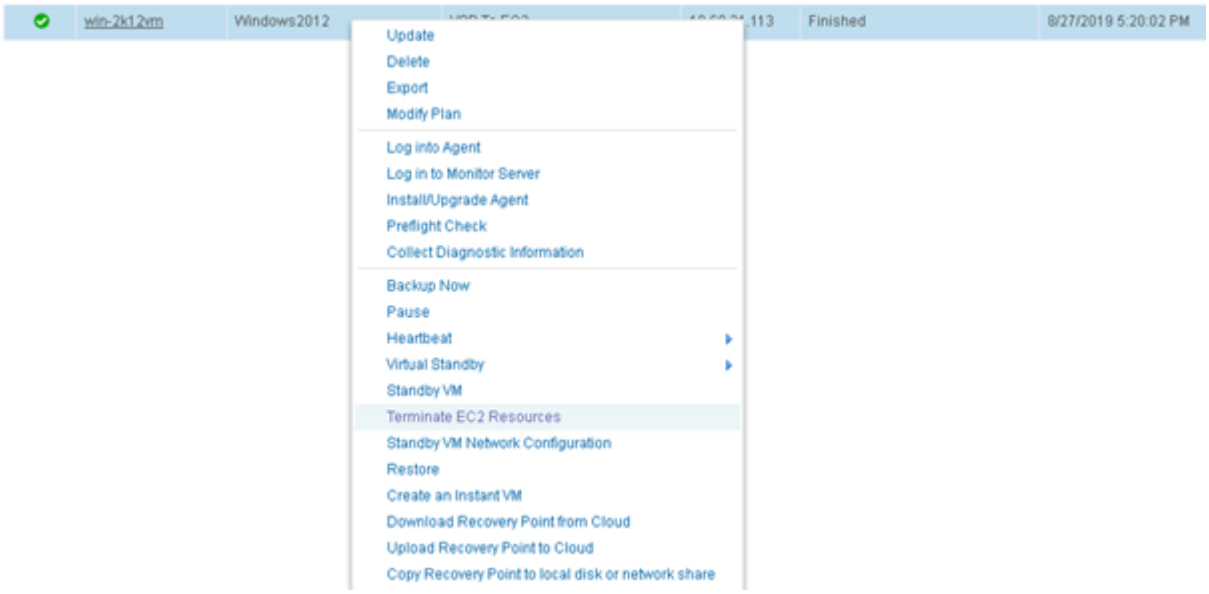
Interruzione delle risorse EC2

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

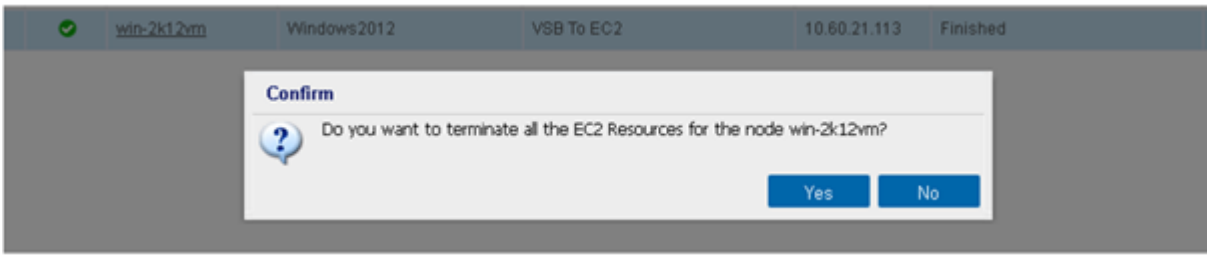
   Tutti i nodi vengono visualizzati nel riquadro centrale.
3. Fare clic con il tasto destro del mouse su un nodo e selezionare Termina risorse EC2.

   Viene visualizzata la finestra di dialogo Conferma.



4. Fare clic su **Sì** per pulire le risorse AWS Cloud generate dall'attività Virtual Standby sull'attività EC2. Fare clic su **No** per interrompere il processo di terminazione.

   Nota: se un nodo non dispone di processi VSB e EC2 riusciti, tale nodo non dispone dell'opzione Termina risorse EC2.



Creazione di un computer Virtual Standby su un piano Microsoft Azure

Lo standby virtuale converte i punti di ripristino in formati di computer virtuale e prepara una snapshot per recuperare facilmente i dati qualora necessario. Questa funzionalità fornisce anche la capacità High Availability e garantisce che il computer virtuale possa intervenire immediatamente quando si verifica un errore nel computer di origine. Il computer Virtual Standby viene creato tramite la conversione dei punti di ripristino in un formato Virtual Standby di Microsoft.

Nota: L'attività Virtual Standby viene eseguita solo se l'attività di backup crea una snapshot valida del punto di ripristino. Se l'attività di backup non riesce, l'attività Virtual Standby viene ignorata.

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di un piano con un'attività di
3. Aggiunta di un computer Virtual Standby a un’attività Azure
4. (Facoltativo) Esecuzione manuale del processo Virtual Standby
5. Sospensione e riattivazione dell'heartbeat
6. Sospensione e riattivazione del processo Virtual Standby.
7. Verifica del piano

Verifica delle considerazioni e dei prerequisiti

Verificare se i prerequisiti seguenti sono stati completati:

- Accedere alla console.
- Installare il componente server e creare gli archivi dati qualora si desideri archiviare i dati di backup nei Recovery Point Server.
- Si dispone di un punto di ripristino valido per creare un computer Virtual Standby. I punti di ripristino possono provenire da una delle attività seguenti:
  - Backup di Windows basato su agente
  - Backup senza agente basato su host
  - Replica
  - Replica da un Recovery Point Server
- Accertarsi che i prerequisiti per l'aggiunta di un account cloud su Microsoft Azure vengano soddisfatti. Per ulteriori informazioni, consultare la sezione Prerequisiti per l'aggiunta di un account cloud su Microsoft Azure.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Creazione di un piano con un’attività di backup

Un piano include diversi tipi di attività da eseguire. Per creare un computer Virtual Standby, creare un piano che include un’attività di backup e un’attività Virtual Standby. Un’attività di backup esegue un backup dei nodi di origine e archivia i dati nella destinazione specificata. Questi dati di backup vengono quindi utilizzati dalla funzionalità Virtual Standby e convertiti in un formato di computer virtuale.

Per ulteriori informazioni, fare riferimento alla sezione Creazione di un piano con un’attività di backup.

Aggiunta al piano di un'attività Virtual Standby

Creare un server Virtual Standby su un'attività Azure in modo che i dati di backup vengano convertiti in un formato di computer virtuale e venga creato un computer virtuale. La funzionalità Virtual Standby controlla anche l'heartbeat del nodo di origine in modo che quando il nodo di origine è inattivo, il computer virtuale assume immediatamente il controllo come nodo di origine.

Note:

- Virtual Standby non è in grado di attivare automaticamente le snapshot del punto di ripristino acquisite dai nodi del computer virtuale basato su host e dai nodi replicati da un Recovery Point Server remoto; soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso. Per tali nodi è necessario alimentare manualmente le snapshot del punto di ripristino.
- Se il piano viene interrotto, il processo Virtual Standby non verrà avviato. Quando il piano viene ripreso, il processo di Virtual Standby non viene ripreso automaticamente. Per avviare il processo Virtual Standby è necessario eseguire un altro processo di backup manualmente. Pertanto, se il piano viene interrotto, l'opzione Sospendi/Riprendi Virtual Standby non sarà disponibile. Se non si desidera che il computer virtuale venga avviato automaticamente dopo l'interruzione del piano, sarà necessario interrompere manualmente l'heartbeat per i nodi.

Effettuare le operazioni seguenti:

1. Fare clic su **Aggiungi un'attività** dal riquadro sinistro.

   Viene aggiunta una nuova attività al riquadro sinistro.

2. Dal menu a discesa **Tipo di attività**, selezionare **Virtual Standby**.

   Viene aggiunta l'attività Virtual Standby.

3. Dalla scheda **Origine**, selezionare un'origine per l'attività Virtual Standby.

4. Fare clic sulla scheda **Server di virtualizzazione** e immettere i dettagli del server di virtualizzazione e del server di monitoraggio.

   Tipo di virtualizzazione - Azure

   Tipo di virtualizzazione

   Specificare Azure come tipo di virtualizzazione.

   Nome account

   Selezionare un account Azure esistente. È inoltre possibile aggiungere un nuovo account facendo clic su **Aggiungi**.

Per ulteriori informazioni, consultare la sezione Aggiunta di un account cloud.

Gruppo di risorse

Specificare un gruppo di risorse. L'utente dovrebbe disporre di un gruppo di risorse in Azure.

Per ulteriori informazioni, consultare la sezione Gruppo di risorse in Azure nella documentazione di Microsoft.

Area

Selezionare l'area Azure in cui si desidera posizionare il computer virtuale di standby. Per ulteriori informazioni sull'area, consultare la sezione Aree in Azure.

Monitoraggio

Specificare il nome host del server che dovrà monitorare lo stato del server di origine.

Note:

- È possibile utilizzare qualsiasi computer fisico o virtuale come server di monitoraggio.
- Non è possibile utilizzare il server di origine di backup come server di monitoraggio.
- Se i nodi vengono replicati da un Recovery Point Server remoto o se soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso, non è necessario configurare il server di monitoraggio.
- La configurazione del server di monitoraggio non è richiesta se l'origine di Virtual Standby corrisponde all'attività di replica e il server RPS di destinazione di replica è contenuto in Azure.

Nome utente

Specificare il nome utente per accedere al sistema di monitoraggio.

Password

Specificare la password del nome utente per accedere al sistema di monitoraggio.

Protocollo

Specificare HTTP o HTTPS come protocollo da utilizzare per la comunicazione tra Arcserve Unified Data Protection e il server di monitoraggio.

Porta

Specificare la porta che si desidera utilizzare per il trasferimento dei dati tra Arcserve Unified Data Protection e il server di monitoraggio.

5. Fare clic sulla scheda **Computer virtuale** e immettere i dettagli relativi alle impostazioni di base del computer virtuale, all'archivio dati del computer virtuale per VMware, al percorso al computer virtuale per Hyper-V e alla rete del computer virtuale.

   Prefisso nome del computer virtuale

   Specificare il prefisso che si desidera aggiungere al nome visualizzato per il computer virtuale su Azure.

   Valore predefinito: UDPVM_

   Snapshot del punto di ripristino

   Specificare il numero di snapshot del punto di ripristino (punti di ripristino) per il computer virtuale di standby. Il numero massimo consentito di snapshot del punto di ripristino corrisponde a 29 per Azure.

   Valore predefinito: 5

   Combina tutte le sessioni non convertite in una snapshot del singolo punto di ripristino

   Consente di specificare se si desidera combinare tutte le sessioni convertite in una singola snapshot del punto di ripristino con l'esecuzione del processo VSB successivo.

   Impostazione predefinita: opzione selezionata

   Dimensioni del computer virtuale

   Microsoft Azure fornisce un'ampia scelta di dimensioni ottimizzate per il computer virtuale adatte ai diversi casi di utilizzo. Dispongono di diverse combinazioni di CPU, memoria, archiviazione e capacità di rete. Per ulteriori informazioni sulle dimensioni del computer virtuale e il soddisfacimento dei requisiti di calcolo, consultare la sezione Computer virtuale Windows in Azure.

   Nome account di archiviazione

   Selezionare un nome per l'account di archiviazione. Azure dovrebbe disporre di un nome per l'account di archiviazione. Per l'account di archiviazione, selezionare Archiviazione (scopo generale v1) o ArchiviazioneV2 (scopo generale v2). Per ulteriori informazioni, consultare la sezione Account di archiviazione in Azure nella documentazione di Microsoft.

   Rete virtuale

Selezionare una rete virtuale. L'utente dovrebbe disporre di una rete virtuale in Azure. Per ulteriori informazioni, consultare la sezione Rete virtuale in Azure nella documentazione di Microsoft.

Subnet

Selezionare una subnet in base alla rete virtuale selezionata. L'utente dovrebbe disporre di una subnet in Azure. Per ulteriori informazioni, consultare la sezione Subnet in Azure nella documentazione di Microsoft.

Gruppo di protezione di rete

Selezionare un gruppo di protezione di rete. L'utente dovrebbe disporre di un gruppo di protezione di rete in Azure. Configurare le regole del gruppo di protezione per aprire le porte correlate, comprese la porta 3389 per il desktop remoto e la porta 8014 e 8015 per la comunicazione con Arcserve UDP. Per ulteriori informazioni, consultare la sezione Gruppo di protezione di rete nella documentazione di Microsoft.

Attivazione dell'assegnazione automatica dell'IP pubblico

Se l'assegnazione automatica dell'IP pubblico è abilitata, l'IP pubblico verrà assegnato automaticamente al computer virtuale di standby se viene avviato in Azure.

6. Fare clic sulla scheda **Avanzate** e fornire i dettagli seguenti:

Avvia il computer virtuale automaticamente

Specificare se si desidera avviare il computer virtuale automaticamente.

Nota: questa opzione non è disponibile per i nodi del computer virtuale basati su host e per i nodi replicati da un Recovery Point Server remoto. Soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso. L'origine di Virtual Standby è un'attività di replica e il server RPS di destinazione della replica è compreso in Azure.

Timeout

Specificare la durata dell'attesa di un heartbeat da parte del server di monitoraggio prima di attivare la snapshot di un punto di ripristino.

Frequenza

Specificare la frequenza con cui il server di origine comunica gli heartbeat al server di monitoraggio.

Esempio: Il valore di timeout specificato è 60. Il valore di frequenza specificato è 10. Il server di origine comunicherà gli heartbeat ogni 10 secondi. Se il server di monitoraggio non rileva un heartbeat entro 60 secondi dell'ultimo heartbeat

rilevato, attiva un computer virtuale utilizzando la snapshot del punto di ripristino più recente.

Personalizzazione dei parametri del processo

È possibile personalizzare i parametri del processo per le seguenti opzioni:

- *Numero di thread in caricamento per ogni processo*: valore predefinito: 4
- *Dimensione di buffer per ciascun thread*: valore predefinito: 4096 KB

Abilitazione degli avvisi di posta elettronica

Consente di ricevere avvisi di posta elettronica a seconda delle impostazioni fornite. Quando si seleziona questa opzione, ulteriori categorie di avvisi di posta elettronica vengono abilitate per la selezione.

- **Heartbeat mancante per il computer di origine** - Virtual Standby invia notifiche di avviso quando il server di monitoraggio non rileva un heartbeat nel server di origine.

  Nota: questa opzione non è disponibile per i nodi associati a Esegui replica da un Recovery Point Server remoto o se soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso.

- **Computer virtuale attivo per il computer di origine configurato con attivazione automatica** - Virtual Standby invia notifiche di avviso quando viene attivato un computer virtuale configurato per l'attivazione automatica nel caso in cui l'heartbeat non venga rilevato.

  Nota: questa opzione non è disponibile per i nodi associati a Esegui replica da un Recovery Point Server remoto o se soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso. Questa opzione non è disponibile per nodi di computer virtuali basati su host.

- **Computer virtuale attivo per il computer di origine configurato con attivazione manuale**: Virtual Standby invia notifiche di avviso con l'attivazione manuale di un computer virtuale.
- **Errori o arresto anomalo di Virtual Standby**: Virtual Standby invia notifiche di avviso quando si verifica un errore durante il processo di conversione.
- **Virtual Standby eseguito correttamente**: Virtual Standby invia notifiche di avviso quando rileva che un computer virtuale è stato attivato correttamente.
- **Errore di avvio di Virtual Standby dalla snapshot del punto di ripristino**: se è stata specificata l'opzione Avvia il computer virtuale automaticamente, Virtual Standby invia notifiche di avviso in caso di rilevamento di computer virtuali non avviati automaticamente.

7. Fare clic su **Salva**.

   Le modifiche vengono salvate e l'attività Virtual Standby viene distribuita automaticamente al server Virtual Standby.

   Nota: una volta completata l’attività Virtual Standby, viee creato il volume di standby del computer virtuale. Il computer virtuale di standby viene creato solo dopo l’attivazione del computer virtuale da Arcserve UDP.

   Virtual Standby è stato creato e distribuito correttamente nel piano Azure.

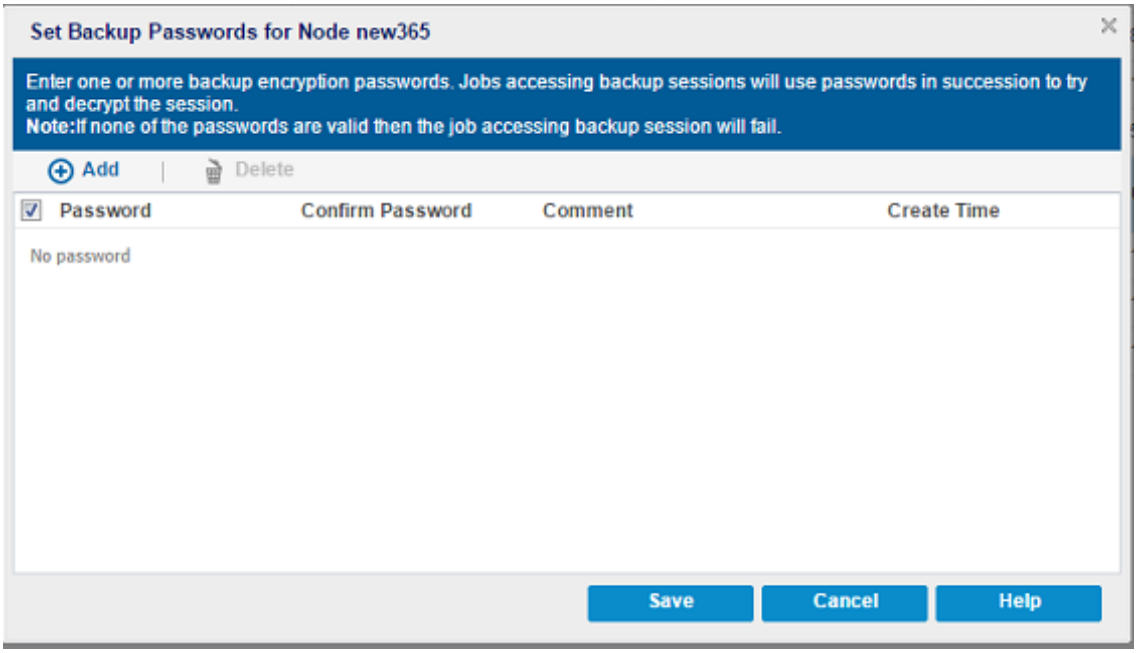
Impostazione delle password di backup per uno o più nodi

Per consentire al convertitore di convertire i punti di ripristino replicati, Virtual Standby permette di specificare le password di backup per i dati utilizzati dal convertitore per la conversione.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.
3. Dal riquadro centrale, fare clic con il tasto destro del mouse sul nodo, quindi selezionare **Imposta password di backup**.

   Viene visualizzata la finestra di dialogo **Imposta password di backup per il nodo**.

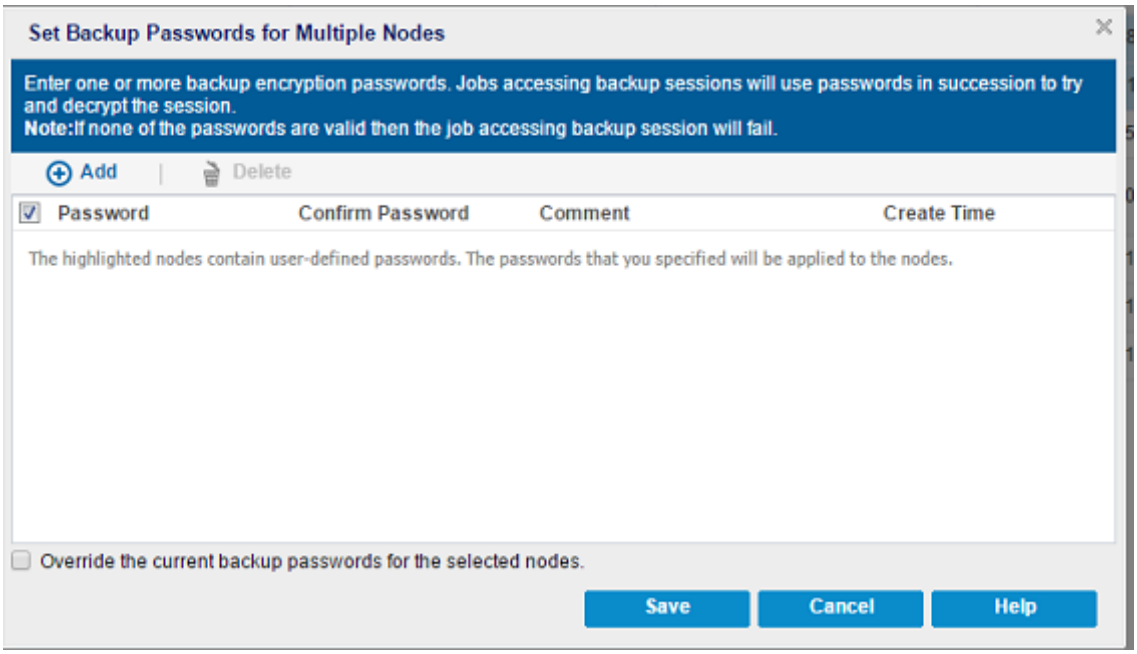


4. La finestra di dialogo **Imposta password di backup** consente di effettuare le azioni seguenti per uno o più nodi:

   Aggiungi: fare clic su **Aggiungi** per aggiungere una o più password di backup ai nodi selezionati.

   Elimina: fare clic su **Elimina** per eliminare una o più password di backup dai nodi selezionati.

   Nota: in caso di nodi multipli, è possibile sovrascrivere le password di backup correnti per i nodi multipli selezionando la casella di controllo **Sovrascrivi le password di backup correnti** per i nodi selezionati.



5. Fare clic su **Salva**.

   La finestra di dialogo viene chiusa e le password di backup vengono impostate per i nodi remoti selezionati.

(Facoltativo) Esecuzione manuale del processo Virtual Standby

Per eseguire manualmente un processo Virtual Standby, occorre prima eseguire un backup manuale. L'attività Virtual Standby è associata a un'attività di backup. Se un piano include un'attività di backup e un'attività Virtual Standby, quando si esegue manualmente il processo di backup, il processo Virtual Standby viene eseguito automaticamente dopo il completamento del processo di backup.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Consente di visualizzare i piani aggiunti.
3. Selezionare i nodi di cui si desidera eseguire il backup. Il nodo selezionato deve avere un piano assegnato.
4. Nel riquadro centrale, fare clic su **Azioni**, **Esegui backup**.

   Verrà visualizzata la finestra di dialogo **Esegui un backup immediato**.
5. Selezionare il tipo di backup e fornire un nome al processo di backup.
6. Fare clic su **OK**.

   Il processo di backup viene eseguito.

   Il processo Virtual Standby viene eseguito immediatamente dopo la conclusione del processo di backup.

   Il processo Virtual Standby viene eseguito manualmente.

Sospensione e riattivazione dell'heartbeat

La soluzione Arcserve Unified Data Protection consente di sospendere e riprendere gli heartbeat rilevati dal server di monitoraggio. L'heartbeat è il processo utilizzato per la comunicazione dello stato del server di origine tra il server di origine e il server di monitoraggio. Se il server di monitoraggio non rileva alcun heartbeat dopo un periodo di tempo specificato, la funzionalità Virtual Standby fa sì che il computer virtuale funga da nodo di origine.

Esempi: Sospensione e riattivazione degli heartbeat

Gli esempi riportati di seguito descrivono i casi che richiedono la sospensione e la riattivazione degli heartbeat:

- Sospendere l'heartbeat se si desidera modificare lo stato del nodo in Non in linea (server di origine) per eseguire operazioni di manutenzione.
- Riattivare l'heartbeat dopo aver completato le attività di manutenzione. Lo stato del nodo (server di origine) è in linea.

Tenere presenti le seguenti considerazioni:

- È possibile sospendere e riattivare gli heartbeat a livello di gruppo o di nodo singolo.
- È possibile sospendere e riattivare gli heartbeat per uno o più nodi in una fase.
- In caso di sospensione dell'heartbeat, la soluzione Arcserve Unified Data Protection
- Durante l'aggiornamento delle installazioni dell'agente sui nodi di origine, Arcserve Unified Data Protection Per garantire che i server di monitoraggio controllino i nodi aggiornati, riattivare l'heartbeat per i nodi, una volta completato l'aggiornamento.

Effettuare le operazioni seguenti:

1. Accedere ad Arcserve UDP Arcserve Unified Data Protection.
2. Fare clic sulla scheda **Risorse**.
3. Dal riquadro sinistro, accedere a **Virtual Standby** e fare clic su **Tutti i nodi**.

   Se sono stati aggiunti nodi, questi verranno visualizzati nel riquadro centrale.
4. Selezionare il nodo che si desidera sospendere o riattivare.
5. Sul riquadro centrale, fare clic su **Azioni**, **Heartbeat**, **Sospendi** o su **Riprendi**.

   L'heartbeat del nodo selezionato viene sospeso o riattivato.

Sospensione e riattivazione del processo Virtual Standby

La conversione virtuale è il processo in cui Virtual Standby converte i punti di ripristino di Arcserve Unified Data Protection dai nodi di origine ai formati del computer virtuale, denominati snapshot del punto di ripristino. In caso di errore di un nodo di origine, la funzionalità Virtual Standby utilizza le snapshot del punto di ripristino per attivare un computer virtuale per il nodo di origine.

Si consiglia di impostare il processo di conversione virtuale per il funzionamento continuo. Tuttavia, se si desidera sospendere temporaneamente il processo di conversione virtuale sui server Virtual Standby locali e remoti, è possibile procedere dalla Console. Dopo aver risolto i problemi relativi al nodo di origine, sarà possibile riprendere il processo di conversione virtuale.

Quando i processi di Virtual Standby (processi di conversione) vengono sospesi, l'operazione di sospensione non sospende il processo di conversione attualmente in corso. La sospensione si applica solamente al processo la cui esecuzione è prevista al completamento del successivo processo di backup. Pertanto, il processo di conversione successivo verrà avviato unicamente quando l'utente specifica che desidera riattivare il processo di conversione sospeso.

Se si riprende Virtual Standby per i nodi e se esistono più sessioni di backup senza snapshot del punto di ripristino, viene visualizzata una finestra di dialogo per la selezione dell'opzione di copia intelligente. Se si fa clic su Sì, Virtual Standby converte la sessione combinata in una singola snapshot del punto di ripristino. Se si fa clic su No, Virtual Standby converte ciascuna sessione individualmente

Nota: In via facoltativa, è possibile sospendere e riprendere i processi di Virtual Standby direttamente dai nodi. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi di Virtual Standby.

Effettuare le operazioni seguenti:

1. Accedere all'Arcserve Unified Data Protection.
2. Fare clic sulla scheda **Risorse**.
3. Dal riquadro sinistro, accedere a **Virtual Standby** e fare clic su **Tutti i nodi**.

   Se sono stati aggiunti nodi, questi verranno visualizzati nel riquadro centrale.
4. Selezionare il nodo che si desidera sospendere o riattivare.

5. Nel riquadro centrale, fare clic su **Azioni**, **Virtual Standby**, **Sospendi** o su **Riprendi**.

   La funzione Virtual Standby per il nodo selezionato viene sospesa o ripresa.

Verifica del piano

Per verificare la funzionalità Virtual Standby, confermare la corretta creazione del piano Virtual Standby. Dopo avere verificato che il piano è stato creato correttamente, verificare se il processo di backup sia in esecuzione in base alla pianificazione. Dopo la corretta conclusione del processo di backup, viene eseguito il processo Virtual Standby. È possibile verificare lo stato del processo di backup e del processo Virtual Standby dalla scheda **Jobs** (Processi).

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Per la verifica dei processi Virtual Standby, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Jobs** (Processi).
2. Dal riquadro sinistro, fare clic su **Tutti i Processi**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare la corretta esecuzione del processo di backup e del processo Virtual Standby.

   Il piano per Virtual Standby è stato verificato correttamente.

   Il computer Virtual Standby è stato creato.

Creazione di un piano di Virtual Standby

Lo standby virtuale converte i punti di ripristino in formati di computer virtuale e prepara una snapshot per recuperare facilmente i dati qualora necessario. Questa funzionalità fornisce anche la capacità High Availability e garantisce che il computer virtuale possa intervenire immediatamente quando si verifica un errore nel computer di origine. Il computer virtuale di standby viene creato mediante la conversione dei punti di ripristino in un formato del computer virtuale VMware o Microsoft Hyper-V.

Nota: L'attività Virtual Standby viene eseguita solo se l'attività di backup crea una snapshot valida del punto di ripristino. Se l'attività di backup non riesce, l'attività Virtual Standby viene ignorata.

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di un piano con un'attività di backup
3. Aggiunta al piano di un'attività Virtual Standby
4. (Facoltativo) Esecuzione manuale del processo Virtual Standby
5. Sospensione e riattivazione dell'heartbeat
6. Sospensione e riattivazione del processo Virtual Standby
7. Verifica del piano

Verifica delle considerazioni e dei prerequisiti

Verificare se i prerequisiti seguenti sono stati completati:

- Accedere alla console.
- Installare il componente server e creare gli archivi dati qualora si desideri archiviare i dati di backup nei Recovery Point Server.
- Si dispone di un punto di ripristino valido per creare un computer Virtual Standby. I punti di ripristino possono provenire da una delle attività seguenti:
  - Backup di Windows basato su agente
  - Backup senza agente basato su host
  - Replica
  - Replica da un Recovery Point Server
- Eseguire il backup del computer completo per abilitare l'attività Virtual Standby. Non è possibile creare un'attività Virtual Standby se il backup non è completo.
- Verificare di disporre delle autorizzazioni minime per eseguire le attività obbligatorie di Virtual Standby. Per ulteriori informazioni, consultare la sezione Autorizzazioni minime richieste per le attività VSB.
- Virtual Standby non è supportato per le origini Linux. Per visualizzare un elenco dei sistemi operativi, dei database e dei browser supportati, consultare la Matrice di compatibilità.

Considerazioni:

- Virtual Standby utilizza i dischi thin provisioning per vSphere.
- Virtual Standby utilizza i dischi rigidi virtuali a espansione dinamica per Hyper-V.
- VMware utilizza un computer separato per il server di monitoraggio su cui è installato l'agente.
- Hyper-v stesso funge da server di monitoraggio con l'agente installato.

Nota: come procedura ottimale, si consiglia di escludere i file dalla scansione antivirus per assicurarsi che Virtual Standby funzioni correttamente. Per ulteriori informazioni, consultare la sezione Esclusione di file dalla scansione antivirus.

Autorizzazioni minime richieste per le attività VSB

Nella tabella sono elencate le autorizzazioni minime richieste per eseguire le attività di Virtual Standby.

Nota: Le autorizzazioni globali sono impostate a livello di vCenter.

Attività	Autorizzazione
Archivio dati	Allocare spazio
	Sfogliare l'archivio dati
	Operazioni file di basso livello
Globale	Disattivare metodi
	Attivare metodi
	Licenze
Host > Configurazione	Configurazione della partizione di archiviazione
Rete	Assegnare rete
Resource	Assegnare un computer virtuale al pool di risorse
Computer virtuale > Configurazione	Aggiunta di un disco esistente
	Aggiunta di un nuovo disco
	Aggiunta o rimozione di un dispositivo
	Avanzato
	Modifica del numero di CPU
	Rilevamento delle modifiche del disco
	Memoria
Computer virtuale > Interazione	Disattiva
	Attiva
	Interazione della console
Computer virtuale > Inventario	Creare da esistente
	Creazione nuovo
	Rimuovi
Computer virtuale > Provisioning	Consentire l'accesso al disco
	Consentire l'accesso di sola lettura al disco
	Consentire il download nel computer virtuale
Computer virtuale > Gestione snapshot	Creare snapshot
	Rimuovere snapshot
	Ripristinare snapshot

Creazione di un piano con un'attività di backup

Un piano include diversi tipi di attività da eseguire. Per creare un computer Virtual Standby, creare un piano che include un'attività di backup e un'attività Virtual Standby. Un'attività di backup esegue un backup dei nodi di origine e archivia i dati nella destinazione specificata. La funzionalità Virtual Standby utilizza i dati di backup e li converte in un formato del computer virtuale.

È possibile creare un computer Virtual Standby da un backup Windows basato su agente e da un backup basato su host senza agente. Inoltre, è possibile creare un computer Virtual Standby dai dati replicati mediante l'attività **Replica**. La procedura seguente è un esempio di come creare un backup Windows basato su agente.

Note:

- Per ulteriori informazioni sul backup senza agente basato su host, consultare la sezione Creazione di un piano di backup di un computer virtuale basato su host.
- Per ulteriori informazioni sulla replica dei dati di backup, consultare la sezione Replica dei dati tra archivi dati gestiti da una console UDP e gestiti da console UPD diverse.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

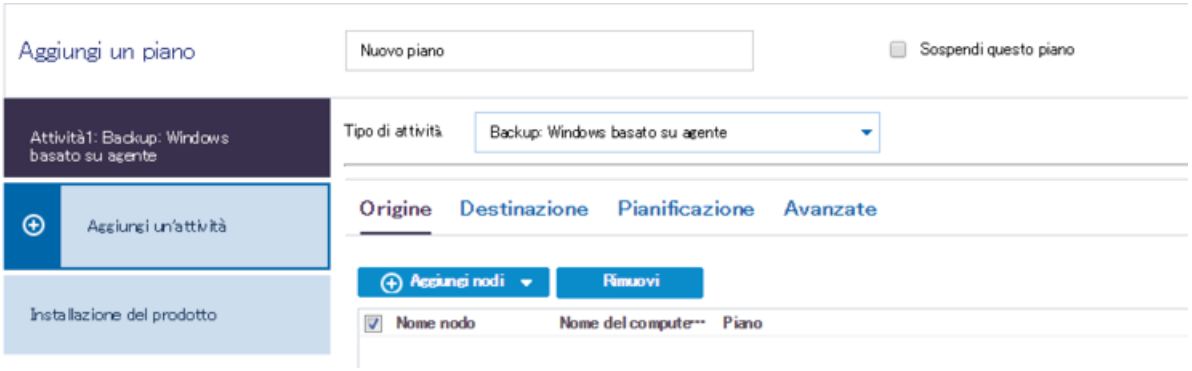
   Viene visualizzata la finestra di dialogo **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on

demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.

6. Dall'elenco a discesa **Tipo di attività**, selezionare **Backup, Windows basato su agente**.



Specificare quindi i dettagli per i campi Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine che si desidera proteggere. È possibile selezionare più di un nodo per un piano. Se non sono stati aggiunti nodi alla console, è possibile aggiungerli in fase di creazione o modifica di un piano dalla pagina Origine. È inoltre possibile salvare un piano senza aggiungere nessun nodo di origine. Il piano viene distribuito soltanto dopo l'aggiunta dei nodi di origine.

Effettuare le operazioni seguenti:

1. Nella scheda Origine, fare clic su **Aggiungi**.
2. Selezionare una delle seguenti opzioni:

   Selezionare i nodi da proteggere in Arcserve UDP

   Consente di visualizzare la finestra di dialogo Selezionare i nodi da proteggere in Arcserve UDP. Selezionare i nodi dall'elenco visualizzato. Selezionare questa opzione se sono stati già aggiunti nodi alla Console.

   Aggiungi nodo Windows

   Viene visualizzata la finestra di dialogo Aggiungi nodi a un piano. Selezionare questa opzione se non sono stati aggiunti nodi e si desidera aggiungere manualmente i nodi da proteggere.

   Rileva nodi da Active Directory

   Consente di aprire la finestra di dialogo Aggiungi nodi alla Console Arcserve UDP. Selezionare questa opzione se si desidera rilevare e aggiungere nodi da Active Directory.

3. Se è stata selezionata l'opzione **Selezionare i nodi da proteggere in Arcserve UDP**, nella finestra di dialogo Selezionare i nodi da proteggere, procedere come segue:

   a. (Facoltativo) Selezionare un filtro dall'elenco a discesa Gruppi per filtrare i nodi. Immettere parole chiave per applicare ulteriori filtri ai nodi.

      I nodi vengono visualizzati nella colonna Nodi disponibili.

   b. Selezionare i nodi dalla colonna Nodi disponibili, quindi fare clic sulla freccia destra singola (>) o sulla freccia destra doppia (>>) per spostare rispettivamente i nodi selezionati o tutti i nodi nella colonna Nodi selezionati.

      I nodi vengono visualizzati nella colonna Nodi selezionati.

   c. Fare clic su **OK** per chiudere la finestra di dialogo.



4. Per scegliere il Tipo di protezione, selezionare una delle seguenti opzioni:

   Backup di tutti i volumi

   Prepara una snapshot del backup di tutti i volumi.

   Backup dei volumi selezionati

   Prepara una snapshot del backup del volume selezionato.

   L'origine viene specificata.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Selezionare un **Tipo di destinazione** tra quelli elencati di seguito:

   Disco locale o cartella condivisa

   Specifica che la destinazione di backup è una destinazione locale o una cartella condivisa. Se si seleziona questa opzione, è possibile salvare i dati come punti di ripristino o set di ripristino. Le opzioni dei punti di ripristino e dei set di ripristino sono disponibili nella scheda **Pianificazione.**

   Recovery Point Server di Arcserve UDP

   Specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono memorizzati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.

2. Se è stato selezionato il **Recovery Point Server di Arcserve UDP**, immettere i seguenti dettagli:
   a. Selezionare un Recovery Point Server.
   b. Selezionare un archivio dati. L'elenco mostra tutti gli archivi dati creati sul Recovery Point Server specificato.
   c. Fornire una password di sessione.
   d. Confermare la password di sessione.
3. Se è stata selezionata l'opzione **Utilizza il disco locale o la cartella condivisa**, fornire i dettagli seguenti:
   a. Fornire il percorso completo della destinazione locale o di rete. Per la destinazione di rete, specificare le credenziali con l'accesso di scrittura.
   b. Selezionare l'algoritmo di crittografia. Per ulteriori informazioni, consultare la sezione Impostazioni di crittografia.
   c. Facoltativamente, fornire una password di crittografia.
   d. Confermare la password di crittografia.
   e. Selezionare un tipo di compressione. Per ulteriori informazioni, consultare la sezione Tipo di compressione.

Nota: Se si archiviano i dati in un disco locale o in una cartella condivisa, non è possibile replicare i dati in un altro Recovery Point Server. La replica è supportata solo se si archiviano i dati in un Recovery Point Server.

La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

Effettuare le operazioni seguenti:

1. (Facoltativo) Selezionare l'opzione per la gestione dei punti di ripristino. Questa opzione è visibile solamente se sono state selezionate le cartelle Locale o Condivisa come destinazione di backup.

   Conserva per punti di ripristino

   I dati di backup vengono archiviati come punti di ripristino.

   Conserva per set di ripristino

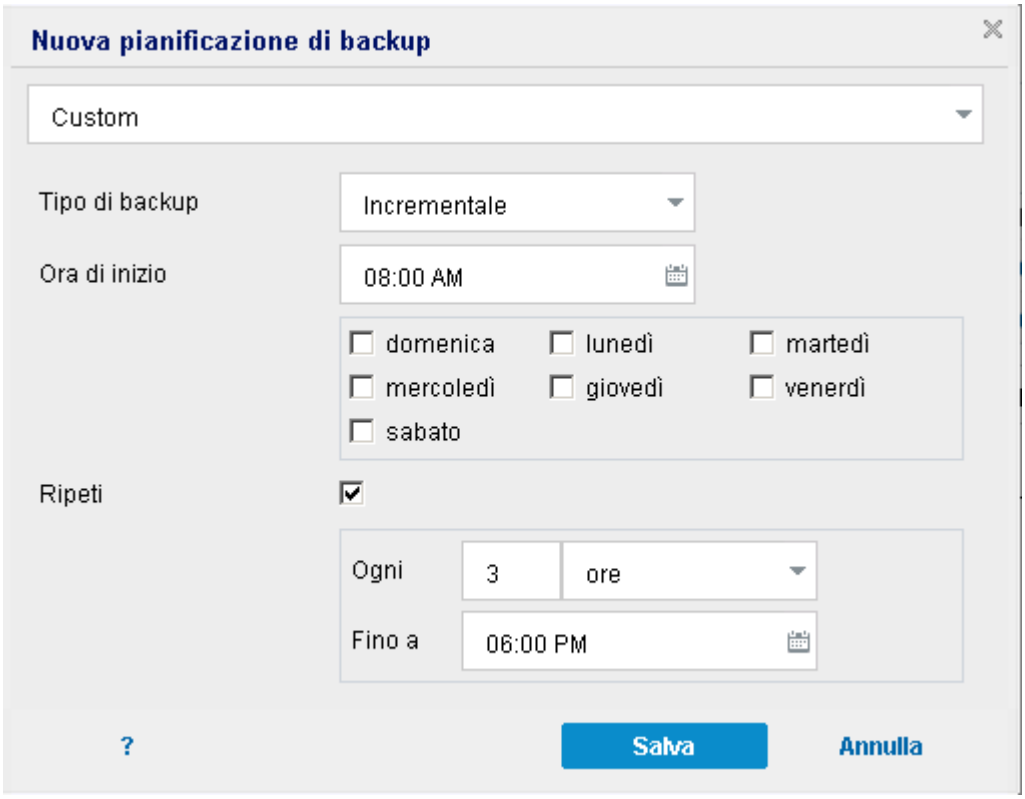
   I dati di backup vengono archiviati come set di ripristino.

2. Aggiungere le pianificazioni di backup, di unione e di definizione del limite di velocità

   Aggiunta di una pianificazione di backup

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base

alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni di backup.

Verifica

Specifica la pianificazione dei backup di verifica.

Arcserve UDP controlla che i dati protetti siano validi e completi eseguendo una verifica di affidabilità dell'immagine di backup archiviata sull'origine di backup. Se necessario esegue la risincronizzazione dell'immagine. Un backup di verifica controlla il backup più recente di ogni blocco e lo confronta con il contenuto e le informazioni di origine. Questo confronto consente di verificare che le informazioni corrispondenti all'origine siano contenute nel blocco di backup più recente. Se l'immagine di backup di un blocco non corrisponde all'origine (probabilmente a causa di modifiche apportate al sistema dall'ultimo backup), Arcserve UDP aggiorna (risincronizza) il backup del blocco non corrispondente. Sebbene si tratti di una procedura poco frequente, il backup di verifica può essere utilizzato per ottenere le stesse garanzie di un backup completo, ma senza occupare lo stesso spazio.

Vantaggi: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.

Svantaggi: il backup di verifica richiede tempi di esecuzione più lunghi, in quanto esegue il confronto di tutti i blocchi originali con i blocchi del backup più recente.

Incrementale

Specifica la pianificazione dei backup incrementali.

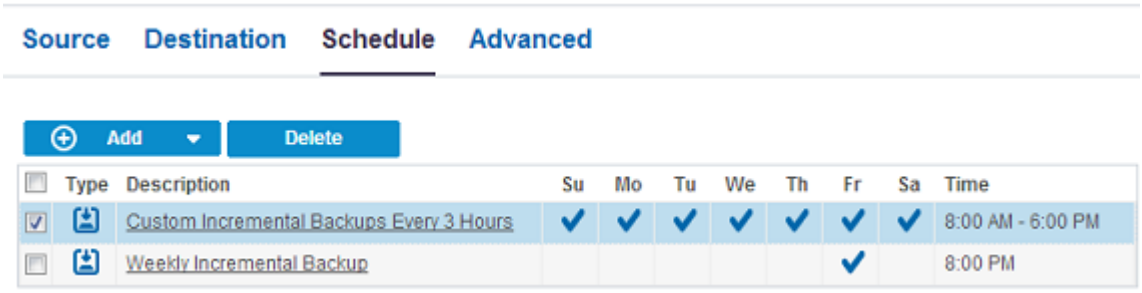
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su Aggiungi e selezionare Aggiungi pianificazione di unione.

   La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

b. Specificare l'ora di inizio per l'avvio del processo di unione.

c. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

d. Fare clic su **Salva**.

   La Pianificazione di unione viene specificata e visualizzata nella pagina **Pianificazione.**

Aggiungi pianificazione del limite delle risorse

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

   Viene visualizzata la finestra di dialogo Aggiungi nuova pianificazione del limite delle risorse.

b. Specificare il limite di velocità effettiva in MB per unità di minuti.

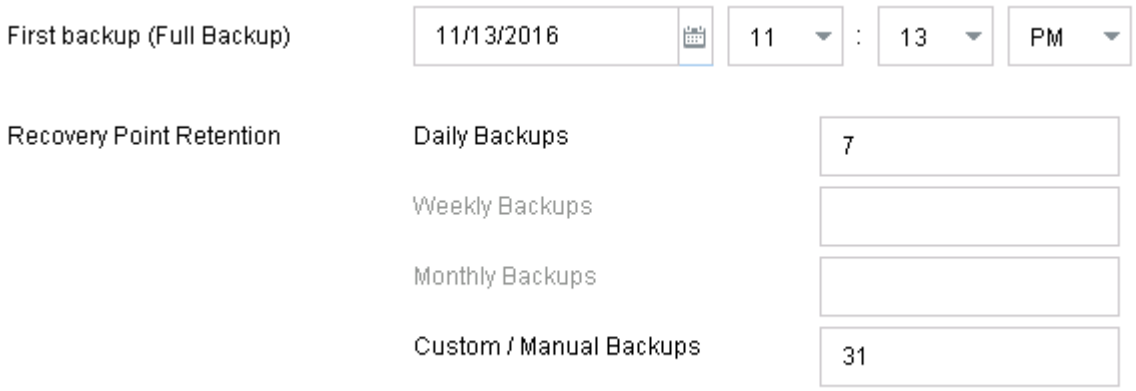
c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

   La pianificazione del limite delle risorse specificata viene visualizzata nella pagina **Pianificazione**.

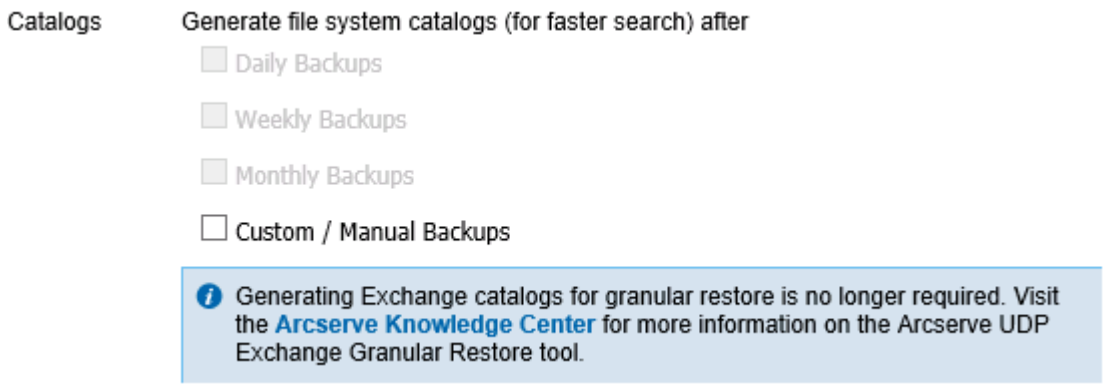
3. Specificare l'ora di inizio per il backup pianificato.



4. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo Pianificazione di backup.

5. Specificare i dettagli relativi al catalogo.



   I cataloghi permettono di generare il catalogo file system. Il catalogo file system è necessario per migliorare e velocizzare la ricerca. Se si selezionano le caselle di controllo del catalogo, i cataloghi verranno abilitati in base al tipo di backup specificato. Deselezionare una casella di controllo per disattivare la generazione del catalogo.

   Viene specificata la pianificazione.

Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione

L'opzione di pianificazione consente di specificare una pianificazione personalizzata o una pianificazione giornaliera/settimanale/mensile o entrambe. Nella pianificazione personalizzata è possibile configurare la pianificazione del backup per ciascun giorno della settimana e aggiungere fino a quattro pianificazioni di backup ogni giorno. È possibile selezionare un giorno specifico di una settimana e creare un intervallo di tempo per definire quando eseguire il backup e la frequenza.

Pianificazione	Processo supportato	Commenti
Backup	Processo di backup	Definire gli intervalli di tempo per eseguire i processi di backup.
Limitazione della velocità di backup	Processo di backup	Definire gli intervalli di tempo per controllare la velocità di backup.
Unione	Processo di unione	Definire quando unire i processi.
Pianificazione quotidiana	Processo di backup	Definire quando eseguire processi di backup quotidiani.
Pianificazione settimanale	Processo di backup	Definire quando eseguire processi di backup settimanali.
Pianificazione mensile	Processo di backup	Definire quando eseguire processi di backup mensili.

È inoltre possibile specificare le impostazioni di memorizzazione per i punti di ripristino.

Nota: All'interno di ogni piano è necessario configurare le impostazioni di conservazione per controllare il modo in cui i nodi assegnati a tale piano vengono memorizzati nell'archivio dati di destinazione.

Le pianificazioni per i backup giornalieri/settimanali/mensili sono indipendenti dalla pianificazione personalizzata e gli uni dagli altri. È possibile configurare di eseguire solo il backup giornaliero, il backup settimanale o il backup mensile senza configurare la pianificazione personalizzata.

Pianificazione del processo di backup

È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del backup. Un intervallo di tempo valido è dalle 00:00 alle 23:59. Non è possibile specificare un intervallo di tempo come ad esempio dalle 18:00 alle 06:00. In tali casi, si devono specificare manualmente due intervalli di tempo diversi.

Per ogni intervallo di tempo l'ora di inizio è inclusa e l'ora di fine è esclusa. Ad esempio, si è configurato il backup incrementale da eseguire ogni ora tra le 06:00 e le 09:00 e il backup inizierà alle 06:00. Ciò significa che il backup verrà eseguito alle 06:00, alle 07:00 e 08:00, ma NON alle 09:00.

Nota: Se si desidera eseguire il processo di backup ripetutamente fino al termine della giornata, impostare la pianificazione fino alle 00:00. Ad esempio, per eseguire un processo di backup ogni 15 minuti per l'intera giornata, impostare la pianificazione dalle 00:00 alle 00:00 ogni 15 minuti.

Pianificazione del limite delle risorse di backup

La pianificazione del limite delle risorse di backup consente di controllare la velocità effettiva di backup, che a sua volta controlla l'utilizzo delle risorse (I/O del disco, CPU, larghezza di banda della rete) del server di cui si esegue il backup. Questo è utile se non si desidera influire sulle prestazioni del server durante i normali orari di ufficio. È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del limite delle risorse di backup. Per ogni intervallo di tempo è possibile specificare un valore, in MB per minuto. Questo valore viene utilizzato per controllare la velocità effettiva di backup. I valori validi sono compresi tra 1 MB/minuto a 99999 MB/minuto.

Se un processo di backup si estende oltre il tempo specificato, il limite della velocità cambia in conformità all'intervallo di tempo specificato. Ad esempio, il limite delle risorse di backup definito è 500 MB/minuto dalle 08:00 alle 20:00 e 2500 MB/minuto dalle 20:00 alle 22:00. Se un processo di backup inizia alle 19:00 e viene eseguito per tre ore, dalle 19:00 alle 20:00 il limite della velocità è pari a 500 MB/minuto e dalle 20:00 alle 22:00 a 2500 MB/minuto.

Se non si definisce alcuna pianificazione del backup e della sua velocità effettiva, il backup viene eseguito il più rapidamente possibile.

Pianificazione di unione

Consente di unire i punti di ripristino in base alla pianificazione fornita.

Considerare i punti seguenti per il processo di unione:

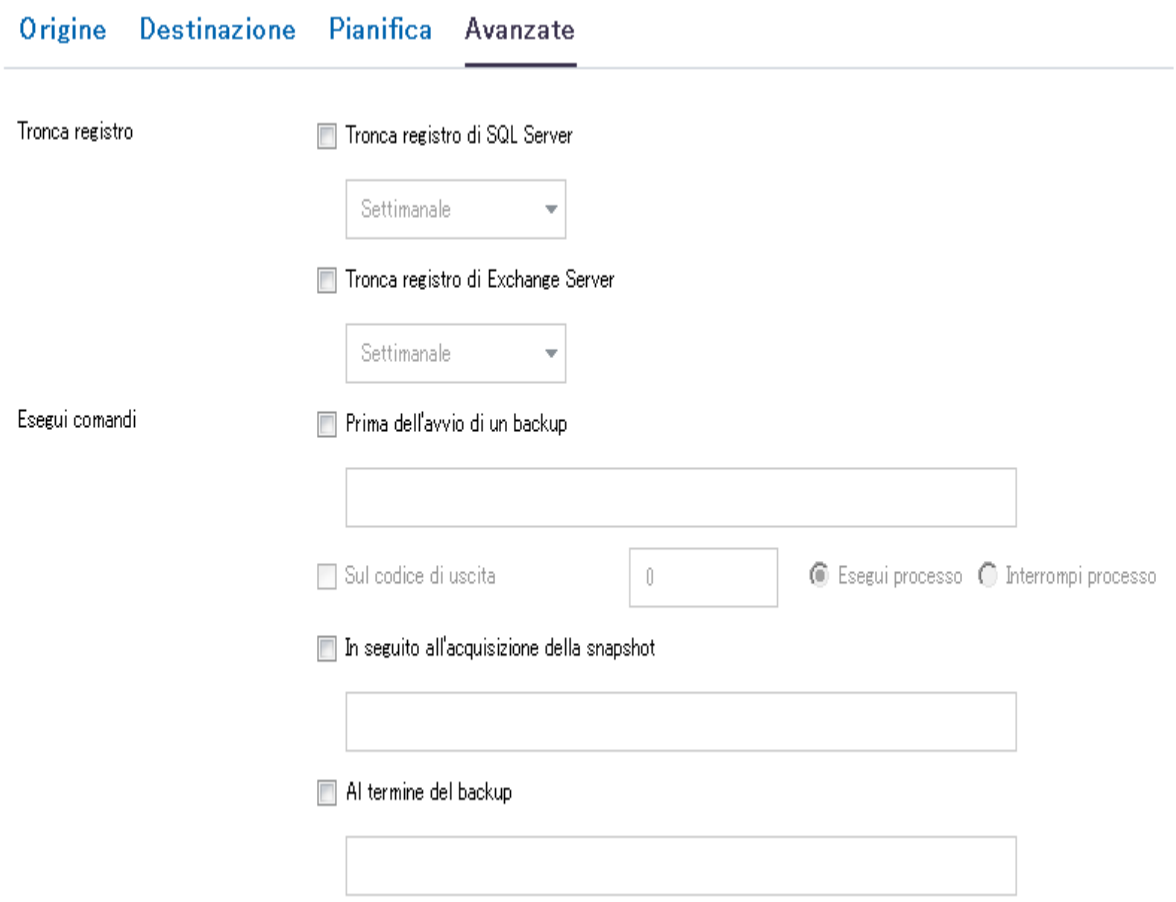
- In qualsiasi momento è possibile eseguire solo un processo di unione per un nodo.
- Se un processo di unione inizia, esso deve essere completato prima di poter avviare il processo di unione successivo. Ciò significa che se uno o più set di punti di ripristino vengono uniti, non è possibile aggiungere nuovi punti di ripristino a questo processo di unione finché il processo di unione dell'insieme corrente dei punti di ripristino non viene completato.

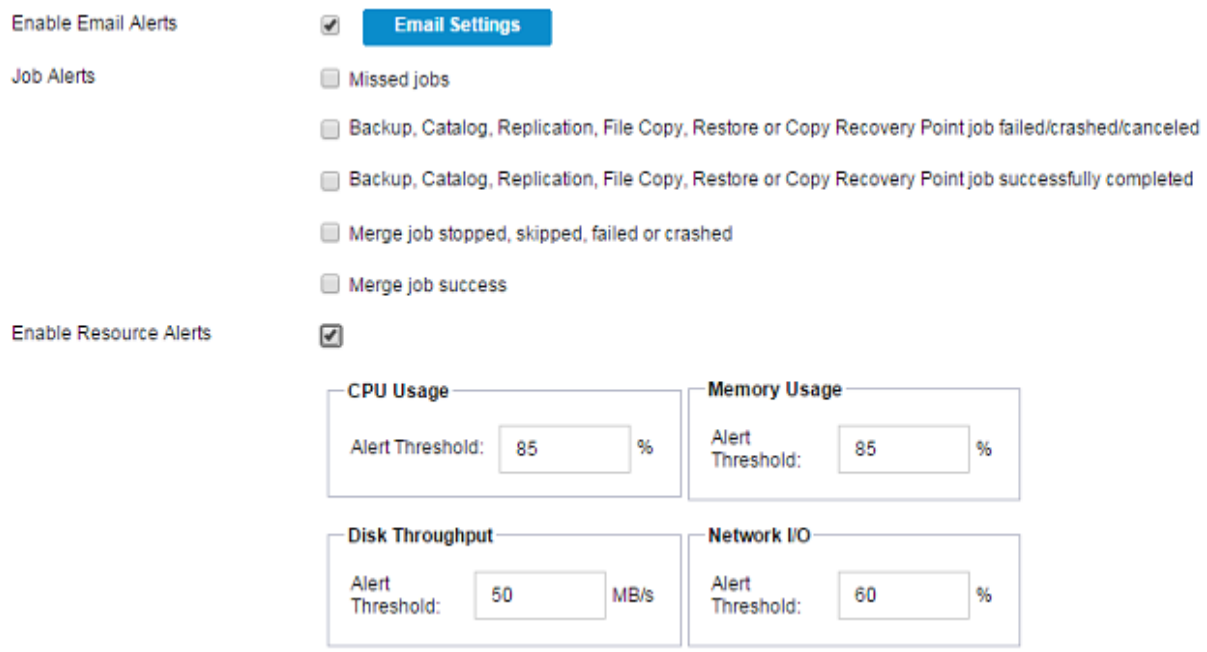
- Se un processo di unione sta elaborando più di un set di punti di ripristino (ad esempio set [1~4], set [5~11] e set [12~14] sono tre set distinti), il Recovery Point Server elabora tali set uno alla volta.
- Se un processo di unione viene ripreso dopo una pausa, il processo individua in quale punto era stato interrotto e riprende l'unione da tale punto.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione delle impostazioni per troncare i registri, l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda Avanzate:





Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

Tronca registro

Consente di specificare la pianificazione per troncare i registri per SQL Server ed Exchange Server. È possibile specificare la pianificazione come **Giornaliero**, **Settimanale** o **Mensile**.

Nome utente

Consente di specificare l'utente autorizzato per l'esecuzione di uno script.

Password

Consente di specificare la password dell'utente autorizzato all'esecuzione dello script.

Esegui un comando prima dell'avvio del backup

Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Esegui processo** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

Esegui un comando dopo l'acquisizione della snapshot

Consente di eseguire uno script dopo l'acquisizione della snapshot del backup. Specificare il percorso di archiviazione dello script.

Esegui un comando al completamento del backup

Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso di archiviazione dello script.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere mediante posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

Abilita avvisi sulle risorse

Consente di specificare una soglia per Utilizzo CPU, Memoria, Velocità del disco, I/O di rete. È possibile fornire il valore in percentuale. Si riceve un messaggio di posta elettronica al superamento del valore Soglia di avviso.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su Salva.

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: Se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo.

Il piano di backup viene creato e distribuito automaticamente al nodo di origine. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

Aggiunta al piano di un'attività Virtual Standby

Creare un'attività Virtual Standby in modo che i dati di backup vengano convertiti in un formato di computer virtuale e venga creato un computer virtuale. La funzionalità Virtual Standby controlla anche l'heartbeat del nodo di origine in modo che quando il nodo di origine è inattivo, il computer virtuale assume immediatamente il controllo come nodo di origine.

Note:

- Virtual Standby non è in grado di attivare automaticamente le snapshot del punto di ripristino acquisite dai nodi del computer virtuale basato su host e dai nodi replicati da un Recovery Point Server remoto; soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso. Per tali nodi è necessario alimentare manualmente le snapshot del punto di ripristino.
- Se il piano viene interrotto, il processo Virtual Standby non verrà avviato. Quando il piano viene ripreso, il processo di Virtual Standby non viene ripreso automaticamente. Per avviare il processo Virtual Standby è necessario eseguire un altro processo di backup manualmente. Pertanto, se il piano viene interrotto, l'opzione Sospendi/Riprendi Virtual Standby non sarà disponibile. Se non si desidera che il computer virtuale venga avviato automaticamente dopo l'interruzione del piano, sarà necessario interrompere manualmente l'heartbeat per i nodi.

Effettuare le operazioni seguenti:

1. Fare clic su **Aggiungi un'attività** dal riquadro sinistro.

   Viene aggiunta una nuova attività al riquadro sinistro.

2. Dal menu a discesa **Tipo di attività**, selezionare **Virtual Standby**.

   Viene aggiunta l'attività Virtual Standby.

3. Dalla scheda **Origine**, selezionare un'origine per l'attività Virtual Standby.

4. Fare clic sulla scheda **Server di virtualizzazione** e immettere i dettagli del server di virtualizzazione e del server di monitoraggio.

   Tipo di virtualizzazione: VMware

   ESX Host/vCenter

   Specificare il nome host del sistema server ESX o vCenter.

   Nome utente

   Specificare il nome utente richiesto per l'accesso al sistema VMware.

Nota: l'account specificato deve essere un account amministrativo o un account con privilegi di amministratore per il sistema server ESX o vCenter.

Password

Specificare la password relativa al nome utente richiesto per l'accesso al sistema VMware.

Protocollo

Specificare HTTP o HTTPS come protocollo da utilizzare per la comunicazione tra l'agente Arcserve Unified Data Protection di origine e il server di monitoraggio.

Porta

Specificare la porta che si desidera utilizzare per il trasferimento dei dati tra il server di origine e il server di monitoraggio.

Nodo ESX

I valori in questo campo variano in base al valore specificato nel campo Host ESX/vCenter.

ESX Server systems (Sistemi server ESX)

Quando viene specificato un sistema server ESX nel campo Host ESX/vCenter, questo campo visualizza il nome host del sistema server ESX.

vCenter Server systems (Sistemi server vCenter)

Quando si specifica un sistema server vCenter nel campo Host ESX/vCenter, questo campo consente specificare (da un elenco a discesa) il sistema server ESX da associare a questo criterio.

Monitoraggio

Specificare il nome host del server che dovrà monitorare lo stato del server di origine.

Note:

- È possibile utilizzare qualsiasi computer fisico o virtuale come server di monitoraggio.
- Non è possibile utilizzare il server di origine di backup come server di monitoraggio.
- Se i nodi vengono replicati da un Recovery Point Server remoto o se soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso, non è necessario configurare il server di monitoraggio.

- La configurazione del server di monitoraggio non è richiesta se l'origine di Virtual Standby corrisponde all'attività di replica e il server RPS di destinazione di replica è contenuto in Azure.

Nome utente

Specificare il nome utente per accedere al sistema di monitoraggio.

Password

Specificare la password del nome utente per accedere al sistema di monitoraggio.

Protocollo

Specificare HTTP o HTTPS come protocollo da utilizzare per la comunicazione tra Arcserve Unified Data Protection e il sistema server ESX (server di monitoraggio).

Porta

Specificare la porta che si desidera utilizzare per il trasferimento dei dati tra Arcserve Unified Data Protection e il sistema server ESX (server di monitoraggio).

Usa server di monitoraggio come proxy per il trasferimento dei dati

Specificare questa opzione affinché il server di monitoraggio copi i dati di conversione dal nodo dell'agente Arcserve Unified Data Protection all'archivio dati del server ESX. Abilitando questa opzione, la funzionalità Virtual Standby trasferisce i dati di conversione dal nodo agente all'archivio dati del server ESX mediante comunicazione con canale a fibre ottiche, più veloce della comunicazione LAN per il trasferimento dei dati. Solo l'operazione di scrittura per la conversione avviene mediante le fibre ottiche. L'operazione di lettura avviene su LAN.

Nota: l'opzione Usa server di monitoraggio come proxy per il trasferimento dei dati è abilitata per impostazione predefinita. È possibile disabilitare questa opzione per consentire al nodo dell'agente Arcserve Unified Data Protection di copiare i dati di conversione direttamente nell'archivio dati del sistema server ESX.

Tipo di virtualizzazione: Hyper-V

Nome host Hyper-V

Specificare il nome host del sistema Hyper-V.

Nome utente

Specificare il nome utente richiesto per l'accesso al sistema Hyper-V.

Nota: L'account specificato deve essere un account amministrativo o un account con privilegi di amministratore sul sistema Hyper-V.

Password

Specificare la password relativa al nome utente richiesto per l'accesso al sistema Hyper-V.

Protocollo

Specificare HTTP o HTTPS come protocollo da utilizzare per la comunicazione tra il server Arcserve Unified Data Protection e il sistema server Hyper-V (server di monitoraggio).

Porta

Specificare la porta che si desidera utilizzare per il trasferimento dei dati tra il server Arcserve Unified Data Protection e il sistema server Hyper-V (server di monitoraggio).

Nota: per convalidare il sistema Hyper-V, fare clic su **Connetti**.

5. Fare clic sulla scheda **Computer virtuale** e immettere i dettagli relativi alle impostazioni di base del computer virtuale, all'archivio dati del computer virtuale per VMware, al percorso al computer virtuale per Hyper-V e alla rete del computer virtuale.

   Sistemi VMware:

   Per sistemi VMware, applicare le opzioni seguenti al computer virtuale:

   Prefisso nome del computer virtuale

   Specificare il prefisso che si desidera aggiungere al nome visualizzato per il computer virtuale sul sistema server ESX.

   Valore predefinito: UDPVM_

   Pool di risorse

   Specificare il nome del pool di risorse in cui si desidera raggruppare il computer virtuale di standby.

   Numero CPU

   Specificare il numero minimo e massimo di CPU supportato dal computer virtuale di standby.

   Memoria

   Specificare la quantità totale di RAM in MB da allocare per il computer virtuale di standby.

Nota: Il valore di RAM specificato deve essere un multiplo di due.

Snapshot del punto di ripristino

Specificare il numero di snapshot del punto di ripristino (punti di ripristino) per il computer virtuale di standby. Il numero massimo di snapshot del punto di ripristino è 29 per server di virtualizzazione VMware.

Tutti i dischi virtuali condividono lo stesso archivio dati

Selezionare questa opzione per copiare tutti i dischi correlati al computer virtuale in un archivio dati.

Deselezionare la casella di controllo per copiare le informazioni relative al disco per il computer virtuale nell'archivio dati corrispondente. Specificare la posizione in cui si desidera archiviare i dati di conversione.

Rete

Consente di definire le NIC, le reti virtuali e i percorsi che il sistema server ESX utilizza per comunicare con i computer virtuali.

Nota: la velocità effettiva VMware SR-IOV e la scheda di rete flessibile non sono supportati.

Stesso numero di schede di rete dell'origine all'ultimo backup

Selezionare l'opzione per definire come eseguire il mapping della NIC virtuale alla rete virtuale. Specificare questa opzione quando il computer virtuale contiene NIC virtuali e una rete virtuale.

Deselezionare la casella di controllo per definire il nome della rete virtuale che si desidera venga utilizzata dalla NIC per la comunicazione.

Sistemi Hyper-V:

Per sistemi Hyper-V, applicare le opzioni seguenti al computer virtuale:

Impostazioni di base

Completare le seguenti Impostazioni di base:

Prefisso nome del computer virtuale

Specificare il prefisso che si desidera aggiungere al nome visualizzato per il computer virtuale sul sistema server Hyper-V.

Valore predefinito: UDPVM_

Numero CPU

Specificare il numero minimo e massimo di CPU supportato dal sistema virtuale di standby.

Memoria

Specificare la quantità totale di RAM in MB da allocare per il computer virtuale di standby.

Nota: Il valore di RAM specificato deve essere un multiplo di quattro.

Snapshot del punto di ripristino

Specificare il numero di snapshot dei punti di ripristino per il computer virtuale di standby. Il numero massimo di snapshot del punto di ripristino è 24 per server di virtualizzazione Hyper-V.

Tutti i dischi virtuali condividono lo stesso percorso

Selezionare questa opzione per specificare la posizione sul server Hyper-V in cui si desidera archiviare i dati di conversione.

Deselezionare la casella di controllo per specificare la posizione sul server Hyper-V in cui si desidera archiviare i dati di conversione per ciascun disco virtuale.

Nota: la soluzione Arcserve UDP non supporta la creazione di immagini di disco virtuale (file VHD/VHDX) su volumi compressi e crittografati dal file system. Se il percorso specificato si trova su volumi Hyper-V compressi o crittografati, Arcserve UDP impedisce la creazione dell'attività Virtual Standby.

Rete del computer virtuale

Consente di definire le NIC, le reti virtuali e i percorsi che il server Hyper-V utilizza per comunicare con i computer virtuali. Specificare una delle opzioni seguenti e completare i campi obbligatori.

Stesso numero di schede di rete dell'origine all'ultimo backup

Selezionare l'opzione per definire come eseguire il mapping della NIC virtuale alla rete virtuale. Specificare questa opzione quando il computer virtuale contiene NIC virtuali e una rete virtuale.

Deselezionare la casella di controllo per definire il nome della rete virtuale che si desidera venga utilizzata dalla NIC per la comunicazione.

6. Fare clic sulla scheda **Avanzate** e fornire i dettagli seguenti:

Avvia il computer virtuale automaticamente

Specificare se si desidera avviare il computer virtuale automaticamente.

Nota: questa opzione non è disponibile per i nodi del computer virtuale basati su host e per i nodi replicati da un Recovery Point Server remoto. Soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso.

Timeout

Specificare la durata dell'attesa di un heartbeat da parte del server di monitoraggio prima di attivare la snapshot di un punto di ripristino.

Frequenza

Specificare la frequenza con cui il server di origine comunica gli heartbeat al server di monitoraggio.

Esempio: Il valore di timeout specificato è 60. Il valore di frequenza specificato è 10. Il server di origine comunicherà gli heartbeat ogni 10 secondi. Se il server di monitoraggio non rileva un heartbeat entro 60 secondi dell'ultimo heartbeat rilevato, attiva un computer virtuale utilizzando la snapshot del punto di ripristino più recente.

Abilitazione degli avvisi di posta elettronica

Consente di ricevere avvisi di posta elettronica a seconda delle impostazioni fornite. Quando si seleziona questa opzione, ulteriori categorie di avvisi di posta elettronica vengono abilitate per la selezione.

- **Heartbeat mancante per il computer di origine** - Virtual Standby invia notifiche di avviso quando il server di monitoraggio non rileva un heartbeat nel server di origine.

  Nota: questa opzione non è disponibile per i nodi associati a Esegui replica da un Recovery Point Server remoto o se soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso.

- **Computer virtuale attivo per il computer di origine configurato con attivazione automatica** - Virtual Standby invia notifiche di avviso quando viene attivato un computer virtuale configurato per l'attivazione automatica nel caso in cui l'heartbeat non venga rilevato.

  Nota: questa opzione non è disponibile per i nodi associati a Esegui replica da un Recovery Point Server remoto o se soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso. Questa opzione non è disponibile per nodi di computer virtuali basati su host.

- **Computer virtuale attivo per il computer di origine configurato con attivazione manuale**: Virtual Standby invia notifiche di avviso con l'attivazione manuale di un computer virtuale.

- **Errori o arresto anomalo di Virtual Standby**: Virtual Standby invia notifiche di avviso quando si verifica un errore durante il processo di conversione.

- **Virtual Standby eseguito correttamente**: Virtual Standby invia notifiche di avviso quando rileva che un computer virtuale è stato attivato correttamente.

- **Errore di avvio di Virtual Standby dalla snapshot del punto di ripristino** - Se è stata specificata l'opzione Avvia il computer virtuale automaticamente, Virtual Standby invia notifiche di avviso in caso di rilevamento di computer virtuali non avviati automaticamente.
- **Hypervisor non raggiungibile** - Virtual Standby invia notifiche di avviso quando vengono rilevati errori di comunicazione con il sistema ESX Server o Hyper-V.
- **Spazio di archiviazione disponibile sul computer virtuale inferiore a** - Virtual Standby invia notifiche di avviso quando viene rilevato spazio su disco insufficiente sul percorso dell'hypervisor definito. Ciò si verifica quando la quantità di spazio disponibile su disco è inferiore alla soglia definita dall'utente. La soglia può essere rappresentata da un valore assoluto (MB) o da una percentuale della capacità del volume.

7. Fare clic su **Salva**.

   Le modifiche vengono salvate e l'attività Virtual Standby viene distribuita automaticamente al server Virtual Standby.

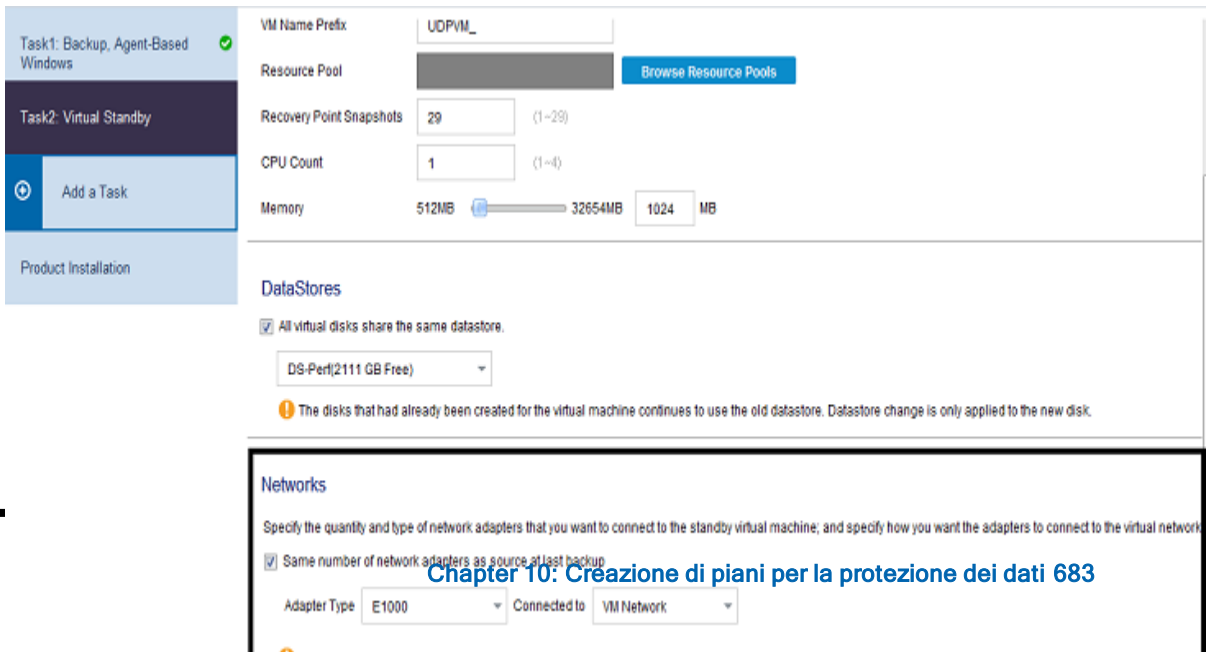
   Il piano Virtual Standby è stato creato e distribuito correttamente.

Definizione del numero di NIC da attivare

Durante l'attivazione dei computer virtuali, Virtual Standby determina il numero di schede di interfaccia di rete da attivare in base alla configurazione della rete del computer virtuale Virtual Standby. La tabella seguente descrive la modalità utilizzata da Virtual Standby per determinare il numero di schede di interfaccia di rete da attivare al momento dell'attivazione dei computer virtuali Virtual Standby:

Valori definiti nel piano per la rete del computer virtuale	L'opzione Attivare il computer di standby virtuale con configurazioni di rete personalizzate non viene specificata.	L'opzione Attivare il computer di standby virtuale con configurazioni di rete personalizzate viene specificata.
I valori definiti sono identici ai valori del computer di origine.	Virtual Standby attiva il numero di schede di interfaccia di rete definito per il computer di origine a partire dall'ultimo processo di backup.	La quantità di schede di interfaccia di rete attivate da Virtual Standby si basa sul valore più elevato tra i seguenti: ■ Il numero definito nella configurazione di rete personalizzata. ■ Il numero di NIC definito per il computer di origine a partire dall'ultimo processo di backup.
I valori definiti sono valori personalizzati.	Virtual Standby attiva il numero di reti personalizzate definite nel piano.	La quantità di schede di interfaccia di rete attivate da Virtual Standby si basa sul valore più elevato tra i seguenti: ■ Il numero definito nella configurazione di rete personalizzata. ■ Il numero di NIC definito per il criterio personalizzato.

La finestra di dialogo seguente, Edit Virtual Standby task (Modifica l'attività Virtual Standby) di Modifica un piano mostra configurazioni personalizzate delle schede di interfaccia di rete da attivare:



La finestra di dialogo seguente, Computer virtuale di standby - <host_name>, mostra la posizione in cui viene specificata l'opzione di accensione del computer virtuale.

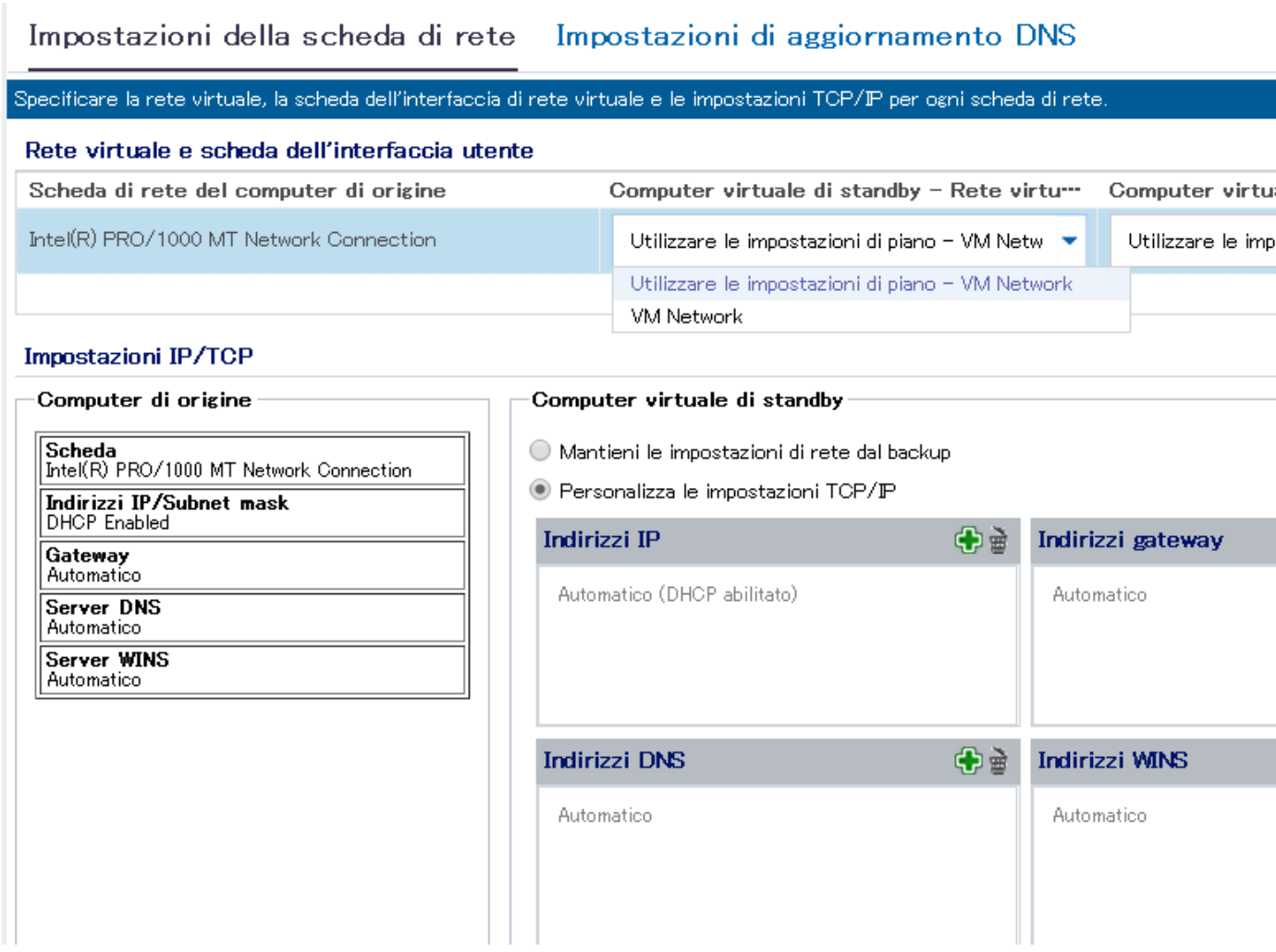


Configurazione della rete del computer virtuale Virtual Standby

È possibile attivare il computer virtuale Virtual Standby mediante impostazioni di rete personalizzate. È possibile configurare le impostazioni di rete seguenti sul computer virtuale Virtual Standby:

- Specificare la rete virtuale, la scheda di interfaccia di rete e le impostazioni TCP/IP per ciascuna scheda di rete nella scheda **Impostazioni della scheda di rete**.
- Aggiornare i server DNS per reindirizzare i client dal computer di origine ai computer virtuali Virtual Standby in base alle impostazioni TCP/IP della scheda **Impostazioni di aggiornamento DNS**.

Nel diagramma seguente è possibile visualizzare la scheda **Impostazioni della scheda di rete** di **Configurazione di rete del computer virtuale di standby**:



Effettuare le operazioni seguenti:

1. Dalla scheda **Risorse**, accedere al gruppo nodi **Virtual Standby**.

   I nodi Virtual Standby vengono mostrati nel riquadro centrale.

2. Nel riquadro centrale selezionare il nodo e fare clic su **Configurazione di rete del computer virtuale di standby**.

   Viene visualizzata la pagina Configurazione di rete del computer virtuale di standby - <node name>.

3. Nella scheda **Impostazioni della scheda di rete** selezionare la rete virtuale dall'elenco **Computer virtuale di standby - Rete virtuale**.

4. Selezionare il tipo di scheda dell'interfaccia utente NIC dall'elenco **Computer virtuale di standby - Tipo di scheda dell'interfaccia utente**.

5. Selezionare **Personalizza le impostazioni TCP/IP**.

6. Fare clic sul pulsante **Aggiungi indirizzo** e aggiungere **Indirizzi IP**, **Indirizzi gateway**, **Indirizzi DNS** e **Indirizzi WINS**.

   Nota: Se si aggiungono **Indirizzi DNS**, configurare i server DNS nella scheda **Impostazioni di aggiornamento DNS**.

7. Fare clic su **Salva**.

   La pagina Configurazione di rete del computer virtuale di standby - <node name> viene chiusa.

   La rete del computer virtuale Virtual Standby è configurata.

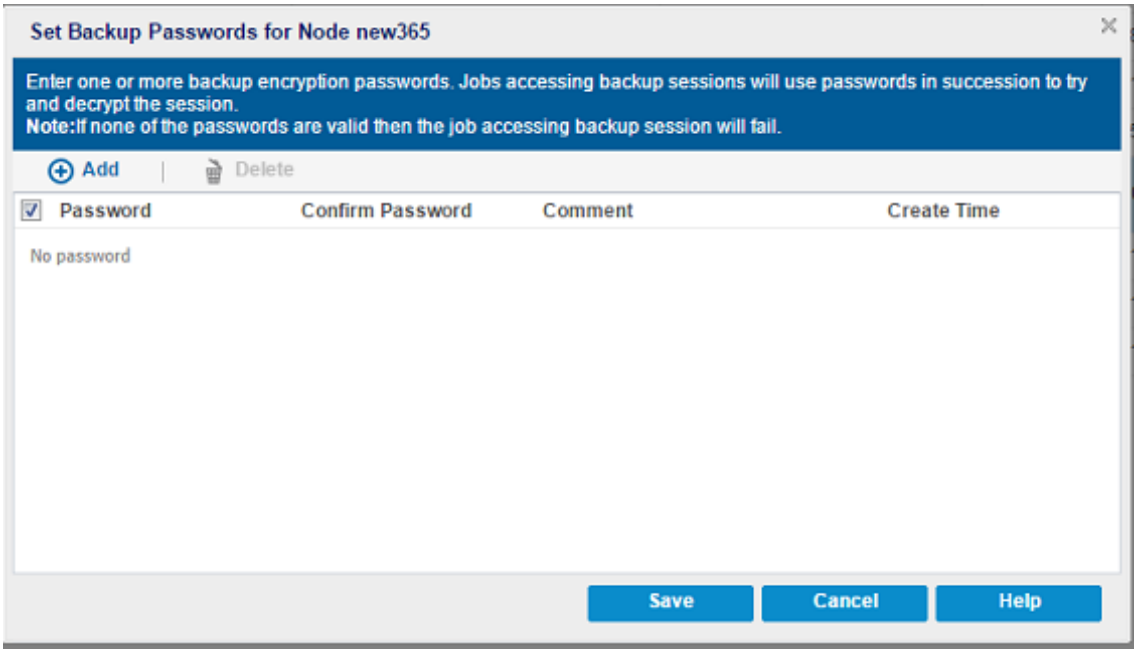
Impostazione delle password di backup per uno o più nodi

Per consentire al convertitore di convertire i punti di ripristino replicati, Virtual Standby permette di specificare le password di backup per i dati utilizzati dal convertitore per la conversione.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.
3. Dal riquadro centrale, fare clic con il tasto destro del mouse sul nodo, quindi selezionare **Imposta password di backup**.

   Viene visualizzata la finestra di dialogo **Imposta password di backup per il nodo**.

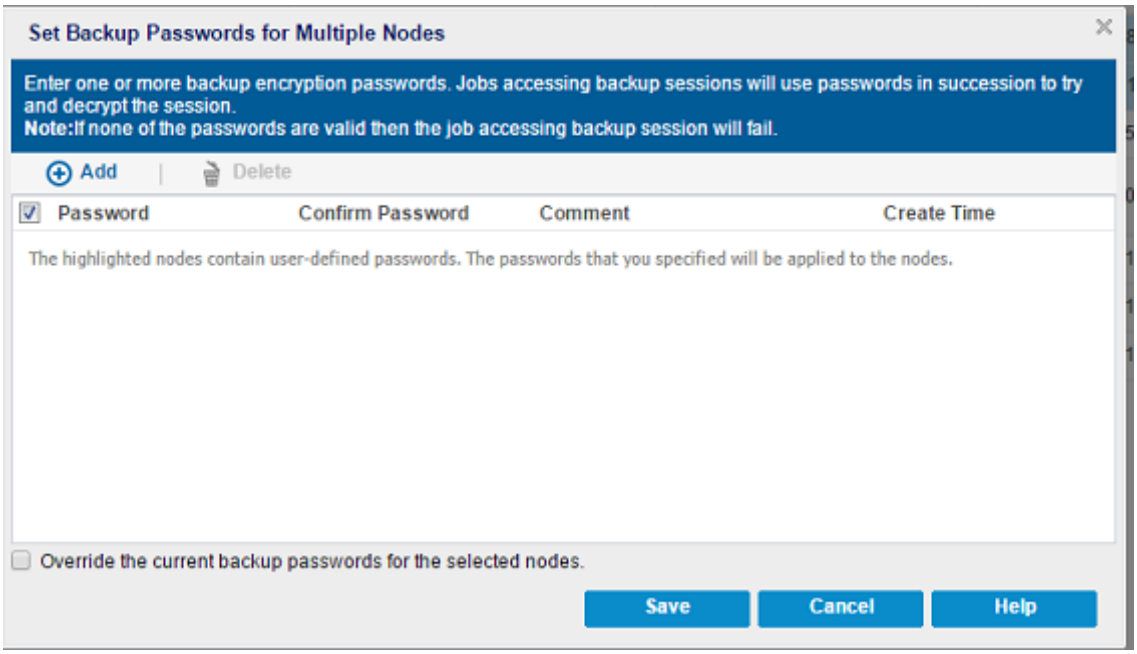


4. La finestra di dialogo **Imposta password di backup** consente di effettuare le azioni seguenti per uno o più nodi:

   Aggiungi: fare clic su **Aggiungi** per aggiungere una o più password di backup ai nodi selezionati.

   Elimina: fare clic su **Elimina** per eliminare una o più password di backup dai nodi selezionati.

   Nota: in caso di nodi multipli, è possibile sovrascrivere le password di backup correnti per i nodi multipli selezionando la casella di controllo **Sovrascrivi le password di backup correnti** per i nodi selezionati.



5. Fare clic su **Salva**.

   La finestra di dialogo viene chiusa e le password di backup vengono impostate per i nodi remoti selezionati.

(Facoltativo) Esecuzione manuale del processo Virtual Standby

Per eseguire manualmente un processo Virtual Standby, occorre prima eseguire un backup manuale. L'attività Virtual Standby è associata a un'attività di backup. Se un piano include un'attività di backup e un'attività Virtual Standby, quando si esegue manualmente il processo di backup, il processo Virtual Standby viene eseguito automaticamente dopo il completamento del processo di backup.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Consente di visualizzare i piani aggiunti.
3. Selezionare i nodi di cui si desidera eseguire il backup. Il nodo selezionato deve avere un piano assegnato.
4. Nel riquadro centrale, fare clic su **Azioni**, **Esegui backup**.

   Verrà visualizzata la finestra di dialogo **Esegui un backup immediato**.
5. Selezionare il tipo di backup e fornire un nome al processo di backup.
6. Fare clic su **OK**.

   Il processo di backup viene eseguito.

   Il processo Virtual Standby viene eseguito immediatamente dopo la conclusione del processo di backup.

   Il processo Virtual Standby viene eseguito manualmente.

Sospensione e riattivazione dell'heartbeat

La soluzione Arcserve Unified Data Protection consente di sospendere e riprendere gli heartbeat rilevati dal server di monitoraggio. L'heartbeat è il processo utilizzato per la comunicazione dello stato del server di origine tra il server di origine e il server di monitoraggio. Se il server di monitoraggio non rileva alcun heartbeat dopo un periodo di tempo specificato, la funzionalità Virtual Standby fa sì che il computer virtuale funga da nodo di origine.

Esempi: Sospensione e riattivazione degli heartbeat

Gli esempi riportati di seguito descrivono i casi che richiedono la sospensione e la riattivazione degli heartbeat:

- Sospendere l'heartbeat se si desidera modificare lo stato del nodo in Non in linea (server di origine) per eseguire operazioni di manutenzione.
- Riattivare l'heartbeat dopo aver completato le attività di manutenzione. Lo stato del nodo (server di origine) è in linea.

Tenere presenti le seguenti considerazioni:

- È possibile sospendere e riattivare gli heartbeat a livello di gruppo o di nodo singolo.
- È possibile sospendere e riattivare gli heartbeat per uno o più nodi in una fase.
- In caso di sospensione dell'heartbeat, la soluzione Arcserve Unified Data Protection
- Durante l'aggiornamento delle installazioni dell'agente sui nodi di origine, Arcserve Unified Data Protection Per garantire che i server di monitoraggio controllino i nodi aggiornati, riattivare l'heartbeat per i nodi, una volta completato l'aggiornamento.

Effettuare le operazioni seguenti:

1. Accedere ad Arcserve UDP Arcserve Unified Data Protection.
2. Fare clic sulla scheda **Risorse**.
3. Dal riquadro sinistro, accedere a **Virtual Standby** e fare clic su **Tutti i nodi**.

   Se sono stati aggiunti nodi, questi verranno visualizzati nel riquadro centrale.
4. Selezionare il nodo che si desidera sospendere o riattivare.
5. Sul riquadro centrale, fare clic su **Azioni**, **Heartbeat**, **Sospendi** o su **Riprendi**.

   L'heartbeat del nodo selezionato viene sospeso o riattivato.

Sospensione e riattivazione del processo Virtual Standby

La conversione virtuale è il processo in cui Virtual Standby converte i punti di ripristino di Arcserve Unified Data Protection dai nodi di origine ai formati del computer virtuale, denominati snapshot del punto di ripristino. In caso di errore di un nodo di origine, la funzionalità Virtual Standby utilizza le snapshot del punto di ripristino per attivare un computer virtuale per il nodo di origine.

Si consiglia di impostare il processo di conversione virtuale per il funzionamento continuo. Tuttavia, se si desidera sospendere temporaneamente il processo di conversione virtuale sui server Virtual Standby locali e remoti, è possibile procedere dalla Console. Dopo aver risolto i problemi relativi al nodo di origine, sarà possibile riprendere il processo di conversione virtuale.

Quando i processi di Virtual Standby (processi di conversione) vengono sospesi, l'operazione di sospensione non sospende il processo di conversione attualmente in corso. La sospensione si applica solamente al processo la cui esecuzione è prevista al completamento del successivo processo di backup. Pertanto, il processo di conversione successivo verrà avviato unicamente quando l'utente specifica che desidera riattivare il processo di conversione sospeso.

Se si riprende Virtual Standby per i nodi e se esistono più sessioni di backup senza snapshot del punto di ripristino, viene visualizzata una finestra di dialogo per la selezione dell'opzione di copia intelligente. Se si fa clic su Sì, Virtual Standby converte la sessione combinata in una singola snapshot del punto di ripristino. Se si fa clic su No, Virtual Standby converte ciascuna sessione individualmente

Nota: In via facoltativa, è possibile sospendere e riprendere i processi di Virtual Standby direttamente dai nodi. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi di Virtual Standby.

Effettuare le operazioni seguenti:

1. Accedere all'Arcserve Unified Data Protection.
2. Fare clic sulla scheda **Risorse**.
3. Dal riquadro sinistro, accedere a **Virtual Standby** e fare clic su **Tutti i nodi**.

   Se sono stati aggiunti nodi, questi verranno visualizzati nel riquadro centrale.
4. Selezionare il nodo che si desidera sospendere o riattivare.

5. Nel riquadro centrale, fare clic su **Azioni**, **Virtual Standby**, **Sospendi** o su **Riprendi**.

   La funzione Virtual Standby per il nodo selezionato viene sospesa o ripresa.

Verifica del piano

Per verificare la funzionalità Virtual Standby, confermare la corretta creazione del piano Virtual Standby. Dopo avere verificato che il piano è stato creato correttamente, verificare se il processo di backup sia in esecuzione in base alla pianificazione. Dopo la corretta conclusione del processo di backup, viene eseguito il processo Virtual Standby. È possibile verificare lo stato del processo di backup e del processo Virtual Standby dalla scheda **Jobs** (Processi).

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Per la verifica dei processi Virtual Standby, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Jobs** (Processi).
2. Dal riquadro sinistro, fare clic su **Tutti i Processi**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare la corretta esecuzione del processo di backup e del processo Virtual Standby.

   Il piano per Virtual Standby è stato verificato correttamente.

   Il computer Virtual Standby è stato creato.

Creazione di un piano Assured Recovery

Per verificare l'accessibilità e garantire il recupero dei dati, è necessario creare un piano Assured Recovery. Il piano per Assured Recovery si basa su un piano di backup/replica. Questa attività di recupero consente di aggiungere un'attività Assured Recovery a un piano di backup o di replica esistenti. L'attività Assured Recovery è composta da un'origine, le impostazioni di verifica, la pianificazione e le impostazioni avanzate. È inoltre possibile eseguire il processo Assured Recovery manualmente.

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Aggiunta di un'attività Assured Recovery a un piano
3. (Facoltativo) Esecuzione manuale del processo di verifica Assured Recovery

Verifica delle considerazioni e dei prerequisiti

Verificare il completamento delle seguenti azioni preliminari:

- Accedere alla console.
- Il componente server è stato installato e gli archivi dati sono stati creati qualora si desideri archiviare i dati di backup nei Recovery Point Server.
- Si dispone di un punto di ripristino valido per creare un computer virtuale istantaneo o un disco virtuale istantaneo. È possibile selezionare i punti di ripristino da una delle seguenti attività:
  - Backup di Windows basato su agente
  - Backup senza agente basato su host
  - Replica
  - Backup, Office 365 Exchange Online
  - Backup, Office 365 OneDrive
  - Backup, Office 365 SharePoint Online
  - Backup, File su UNC o sul percorso NFS
  - Backup, Linux basato sull'agente
- Verificare che gli agenti Arcserve UDP siano già installati sul server proxy.
- Verificare che il sistema operativo del server proxy sia Windows Server 2008 R2 a 64 bit o versioni successive.

  Nota: per i piani di backup nel percorso UNC e di Office 365 (Exchange Online, OneDrive, SharePoint Online), il server proxy Assured Recovery deve corrispondere a Windows 2012 (o a versioni successive).
- Verificare che il server proxy abbia spazio sufficiente per il computer virtuale istantaneo o per il disco virtuale istantaneo.

  Nota: Lo spazio necessario dipende in particolare dalla dimensione della RAM configurata nell'attività AR per il tipo di verifica AR per computer virtuale istantaneo. Per ogni computer virtuale istantaneo, l'hypervisor necessita al massimo della stessa dimensione di RAM per contenere i dati temporanei in file di swapping della memoria. Ad esempio, se si dispone di 5 nodi nello stesso piano con attività AR per computer virtuale istantaneo e la dimensione della memoria per il computer virtuale è impostata su 4 GB, saranno necessari almeno 5 * 4 = 20 GB di spazio libero per contenere i file di swapping della memoria. Inoltre, potrebbero essere necessari altri 10 MB di spazio libero per contenere i file di configurazione del computer virtuale.

- Verificare che la versione del sistema operativo Windows sul server proxy Assured Recovery sia uguale o superiore alla versione del sistema operativo Windows sul computer virtuale di origine.

Aggiunta di un'attività Assured Recovery al piano

L'aggiunta di un'attività Assured Recovery consente di aggiungere un'attività Assured Recovery a un piano di replica o di backup esistente. Ciascuna attività consiste di parametri che definiscono l'origine, le impostazioni dell'attività, la pianificazione e le impostazioni avanzate. Creare un'attività Assured Recovery in base all'attività di backup/replica per verificare l'accessibilità e il valore di Assured Recovery dai dati, nonché per eseguire la verifica dell'integrità dei dati.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Dal riquadro centrale, aprire un piano di backup o di replica esistente.
4. Fare clic su **Aggiungi un'attività** dal riquadro a sinistra.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: Se il piano viene interrotto, il processo Assured Recovery non verrà avviato. Quando il piano viene ripreso, il processo Assured Recovery non viene ripreso automaticamente. Per avviare il processo Assured Recovery è necessario eseguire un altro processo di backup manualmente.
6. Dal menu a discesa **Tipo di attività**, selezionare **Verifica Assured Recovery**.
7. Specificare i dettagli Origine, le impostazioni dell'attività (computer virtuale istantaneo o IVD), Pianificazione e Avanzate.
8. Fare clic su **Salva**.

   Le modifiche vengono salvate e l'attività Assured Recovery viene distribuita automaticamente.

Definizione dell’origine

La scheda Origine consente di specificare i punti di ripristino di origine che si desidera proteggere.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Origine**.
2. Fare clic sull'elenco a discesa dei punti di ripristino di origine per la verifica Assured Recovery, quindi selezionare l'opzione desiderata.
3. Selezionare i tipi di punti di ripristino per la verifica Assured Recovery. È possibile selezionare una delle due opzioni seguenti:
   - Verifica Assured Recovery da tipi di backup selezionati

     È possibile selezionare Backup giornalieri, Backup settimanali e Backup mensili. Le opzioni relative alla frequenza giornaliera, settimanale o mensile sono abilitate in base alla pianificazione del backup di origine. Ad esempio, se per il backup di origine è pianificato soltanto un backup mensile, per la verifica Assured Recovery da tipi di backup selezionati sono attivi soltanto i backup mensili.
   - Verifica Assured Recovery dai punti di ripristino più recenti

L'origine viene specificata

Definizione delle impostazioni di un'attività per il tipo di verifica - Computer virtuale istantaneo

Se si seleziona un computer virtuale istantaneo come tipo di verifica, è possibile avviare il computer virtuale dal punto di ripristino ed eseguire facoltativamente lo script personalizzato. Il punto di ripristino viene considerato in buono stato se il computer virtuale viene avviato correttamente e lo script di verifica restituisce un esito positivo entro l'intervallo di tempo specificato dall'utente.

Nota: Questo passaggio non è obbligatorio se si seleziona **Disco virtuale istantaneo** come tipo di verifica.

È possibile selezionare un tipo di hypervisor da VMware vSphere e Microsoft Hyper-V, quindi immettere i dettagli delle Impostazioni proxy. Immettere inoltre le impostazioni del computer virtuale per specificare le impostazioni dell'attività per il computer virtuale istantaneo.

Effettuare le operazioni seguenti:

1. Selezionare **Computer virtuale istantaneo** come tipo di verifica.

   Nota: Quando l'attività di origine consiste nel backup o nella replica Linux basato su agente, l'opzione Computer virtuale istantaneo è l'unico tipo di verifica supportato.

2. Selezionare una delle opzioni dell'hypervisor e immettere i dettagli corrispondenti:

   VMware vSphere

   Nota: Se l'attività AR è impostata sul computer virtuale istantaneo con vSphere, è necessaria la stessa licenza di VMware richiesta dalla funzionalità di computer virtuale istantaneo.

   a. Eseguire una delle seguenti opzioni per fornire un server vCenter/ESX(i):

      - Se è stato già aggiunto un nodo VMware al sito selezionato nella Console, selezionare tale nodo dall'elenco a discesa Server vCenter/ESX(i).
      - Se non è stato aggiunto nessun nodo VMware, fare clic su **Aggiungi**.

        Viene visualizzata la finestra di dialogo **Specifica destinazione del computer virtuale**.
      - Specificare i dettagli del computer virtuale, quindi fare clic su OK.

        Tutti gli ESX(i) o i pool di risorse vengono visualizzati nel riquadro centrale della pagina Posizione computer virtuale.

b. Selezionare una delle opzioni da ESX(i), dal cluster, dal pool di risorse o dall'applicazione virtuale come posizione.

   Il computer VMware vSphere è stato specificato.

   Nota: Specificare l'archivio dati del server ESX(i) se l'attività di origine corrisponde al backup o alla replica di Linux basato su agente o senza agente basato su host.

Definizione di Microsoft Hyper-V

Eseguire una delle seguenti opzioni per fornire Microsoft Hyper-V:

- Se è stato già aggiunto un nodo Hyper-V al sito selezionato nella Console, selezionare tale nodo dall'elenco a discesa Server/Cluster Hyper-V.
- Se non è stato aggiunto nessun nodo Hyper-V, fare clic su **Aggiungi**.

  Viene visualizzata la finestra di dialogo Specifica destinazione del computer virtuale.

  Nota: Quando ci si connette al computer virtuale istantaneo Hyper-V mediante un account di amministratore locale non integrato, occorre disabilitare il controllo dell'account utente remoto. Per ulteriori informazioni sulla disattivazione del controllo dell'account utente remoto per l'amministratore non integrato, consultare la sezione Disattivazione del controllo dell'account utente remoto per un amministratore non integrato.
- Specificare i dettagli del server Hyper-V, quindi fare clic su **OK**.

Il computer virtuale Hyper-V è stato specificato.

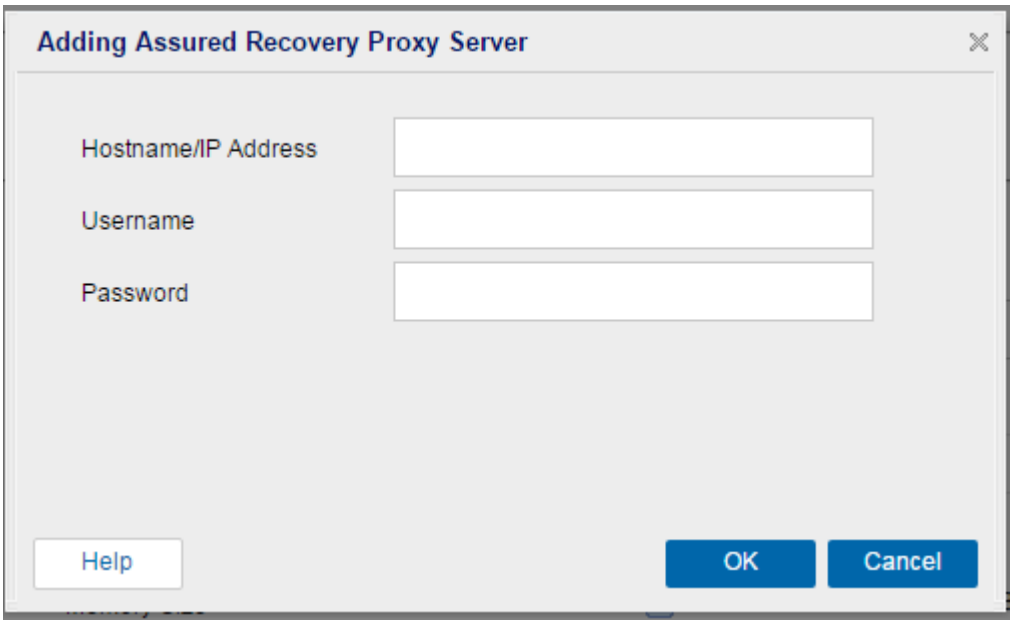
Specificare Nutanix AHV

L'operazione riguarda soltanto il supporto per i computer virtuali Linux. Per ulteriori informazioni, consultare la sezione Protezione di un computer virtuale istantaneo su Nutanix AHV per un nodo Linux.

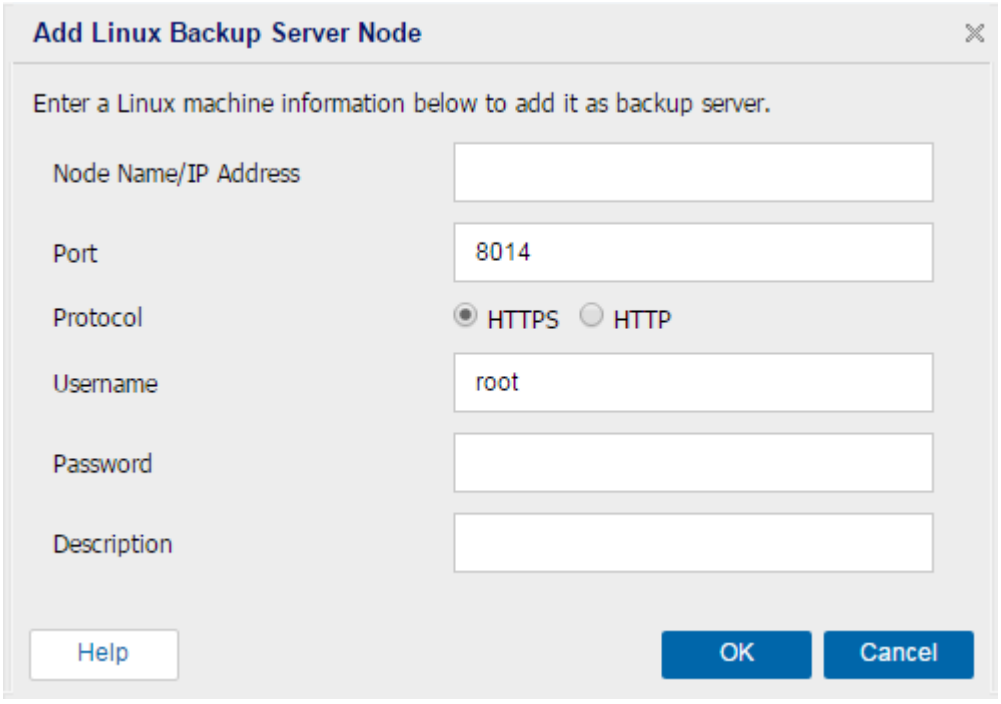
3. Eseguire una delle seguenti opzioni per fornire il **Server proxy**:
   - Se è stato già aggiunto un nodo proxy al sito selezionato nella Console, selezionare tale nodo dall'elenco a discesa dei server proxy.
   - Se non è stato aggiunto nessun nodo proxy, fare clic su **Aggiungi**.

     Viene visualizzata la finestra di dialogo **Aggiunta del server proxy Assured Recovery**.

Per il server proxy Windows



Per il server proxy Linux



- Definizione dei dettagli del server proxy
- Fare clic su **OK**.

I nodi vengono visualizzati nell'area **Nodi disponibili**.

Note:

- È necessario selezionare un server proxy solo quando l'hypervisor è VMware vSphere.
- Quando l'hypervisor è VMware vSphere, il ruolo Network File System (NFS) di Windows deve essere installato sul Recovery Point Server. Il processo del computer virtuale istantaneo installa automaticamente NFS. Per installare manualmente il servizio NFS, consultare la sezione Installazione manuale di NFS su un server Windows.
- Selezionare i server proxy in base ai tipi di nodi selezionati inclusi nel piano. Ad esempio, il server proxy Windows per il nodo Windows e il server proxy Linus per il nodo Linus.

4. (Facoltativo) Completare i passaggi seguenti per specificare le impostazioni del gateway per Assured Recovery.

   Nota: Applicabile solo a Linux.

   a. Utilizzare le impostazioni DHCP o specificare manualmente l'indirizzo IP, la maschera e il gateway predefinito.

   b. Selezionare una rete virtuale dall'elenco a discesa.

   Nota: Le impostazioni del gateway sono obbligatorie solo se l'origine della verifica Assured Recovery è un processo di backup o replica di Linux basato su agente o senza agente basato su host.

5. Specificare i dettagli delle **Impostazioni del computer virtuale** di Assured Recovery.

   Prefisso nome del computer virtuale

   Specifica il prefisso del nome del computer virtuale. Il nome del nodo di origine con prefisso diventa il nome predefinito del computer virtuale istantaneo. Per il nome non sono ammessi alcuni caratteri speciali, quali @, \ e così via.

   Valore predefinito: UDPARVM_

   Cartella dei file del computer virtuale

   Consente di specificare il percorso della cartella del computer virtuale Assured Recovery sul server proxy. È possibile esplorare le informazioni sul volume del server proxy.

   Numero CPU

   Specifica il numero di CPU necessarie nel computer virtuale Assured Recovery.

   Dimensioni memoria

   Specifica le dimensioni della memoria necessarie nel computer virtuale Assured Recovery.

Impostazioni di rete

Consente di specificare le impostazioni di rete per il computer virtuale Assured Recovery. È possibile selezionare l'opzione di connessione del computer virtuale Assured Recovery alla rete. È inoltre possibile utilizzare le impostazioni DHCP per il computer virtuale Assured Recovery oppure utilizzare le impostazioni TCP/IP della sessione di backup.

Tipo di scheda

Specifica il tipo di scheda del computer virtuale Assured Recovery. Il tipo di scheda disponibile può variare a seconda dell'hypervisor.

Definizione delle impostazioni dell'attività per il tipo di verifica - Disco virtuale istantaneo

La selezione del disco virtuale istantaneo come tipo di verifica per le impostazioni di verifica consente di montare il punto di ripristino come disco locale, di verificare l'integrità del volume e del file system, nonché di eseguire lo script personalizzato. Il punto di ripristino viene considerato in buono stato se viene montato correttamente e se tutti i test producono risultati positivi.

Nota:

- Questo passaggio non è richiesto se si seleziona il **computer virtuale istantaneo** come tipo di verifica.
- L'opzione **Disco virtuale istantaneo** non supporta i nodi non Windows.

Effettuare le operazioni seguenti:

1. Eseguire una delle seguenti operazioni per specificare i server del **server proxy di Windows:**
   a. Selezionare un nodo disponibile dall'elenco a discesa.

      Nota: se è stato già aggiunto un nodo proxy al sito selezionato nella Console, è possibile visualizzare l'elenco dei nodi dall'elenco a discesa dei **server proxy di Windows**.

   b. Se non è stato aggiunto nessun nodo proxy, procedere come segue:
      i. Fare clic su **Aggiungi**.
      ii. Viene visualizzata la finestra di dialogo **Aggiunta del server proxy Assured Recovery**.
      iii. Specificare i dettagli del server proxy, quindi fare clic su **OK**.
2. **Sfogliare** la posizione della cartella del disco rigido virtuale sul server proxy.

Definizione di una pianificazione del processo di verifica Assured Recovery

La scheda Pianificazione consente di specificare la pianificazione del processo di verifica di Assured Recovery. Se non si specifica una pianificazione, l'attività viene avviata immediatamente una volta completata l'attività principale.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Pianificazione**.
2. Fare clic su **Aggiungi**, quindi selezionare **Aggiungi pianificazione processo di verifica Assured Recovery**.

   Viene visualizzata la finestra di dialogo Aggiungi pianificazione processo di verifica Assured Recovery.
3. Specificare la pianificazione e fare clic su **Salva**.

   La finestra di dialogo viene chiusa e nella scheda di pianificazione vengono visualizzate le opzioni specificate.

Note:

- Se l'origine Assured Recovery è Punti di ripristino più recenti e si abilita la pianificazione di Assured Recovery, il valore predefinito è 1. Di conseguenza, viene verificato il più recente per impostazione predefinita.

  Se il valore è <=0, vengono provati tutti i punti di ripristino non verificati.
- Se l'origine Assured Recovery è Giornaliero/Settimanale/Mensile e si abilita la pianificazione di Assured Recovery, il valore predefinito è 9 (7 giornalieri + 1 settimanale + 1 mensile).

  Se il valore è <=0, vengono provati tutti i punti di ripristino non verificati.
- Se non si desidera utilizzare il valore predefinito, è possibile aggiungere una chiave del Registro di sistema DWORD a 32 bit nella posizione seguente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AssuredRecovery\MaxNumberOfRecoveryPoint

Definizione delle impostazioni avanzate

La scheda Avanzate consente di applicare altre impostazioni necessarie per completare il piano. Questo parametro è facoltativo se non si desidera aggiungere ulteriori impostazioni. Alcune delle opzioni visualizzate nella scheda **Avanzate** variano in base alla selezione nella scheda precedente. Ad esempio, l'opzione Proprietà heartbeat è visibile soltanto se il tipo di verifica selezionato corrisponde a Computer virtuale istantaneo nelle **Impostazioni di verifica**.

Proprietà heartbeat

Nota: L'opzione è visibile solo se è stato selezionato Computer virtuale istantaneo come valore di Tipo di verifica.

Timeout

Consente di specificare il tempo massimo di attesa dell'heartbeat da parte del server proxy del computer virtuale Assured Recovery. Se il computer virtuale Assured Recovery non è disponibile oltre la scadenza definita, il processo di verifica di Assured Recovery produce un errore.

Frequenza

Specifica la frequenza di verifica da parte del server proxy dello stato dell'heartbeat del computer virtuale Assured Recovery.

Nota: Questa opzione non è visibile se è stato selezionato il backup o la replica di Linux basato su agente come valore di Origine punto di ripristino per verifica Assured Recovery.

Punti di verifica

Nota: L'opzione è visibile solo se è stato selezionato il disco virtuale istantaneo come tipo di verifica.

Verifica del file system

Verifica se il file system e le dimensioni del volume corrispondono a quelle del computer di origine.

Esegui comando del disco di verifica

Verifica l'integrità dei dati mediante l'esecuzione del comando del disco di verifica sui volumi esposti dal disco virtuale istantaneo.

Posizione del comando personalizzato su proxy

Nota: Questa opzione non è visibile se è stato selezionato il backup o la replica di Linux basato su agente come valore di Origine punto di ripristino per verifica Assured Recovery.

Specifica lo script personalizzato archiviato sul server proxy. È possibile esplorare le informazioni sul volume del server proxy. Se è selezionato il tipo Assured Recovery del computer virtuale, lo script viene copiato nel computer virtuale ed eseguito con l'avvio del computer virtuale. Se è selezionato il tipo Assured Recovery IVHD, lo script viene eseguito sul server proxy.

Nota: Il processo di Assured Recovery è in grado di supportare soltanto lo script bat eseguibile di Windows o il file binario eseguibile. Tuttavia, questa restrizione non limita l'utilizzo del processo di Assured Recovery. È possibile utilizzare uno script in batch di Windows per avviare lo script Powershell, ad esempio test.bat con il contenuto seguente:

Powershell.exe -NoProfile -ExecutionPolicy ByPass -Command "& '%ScriptPath%\AR-check.ps1'"

I seguenti argomenti vengono trasmessi allo script in base alle proprie esigenze.

- set PlanName=%1%

- set NodeName=%2%

- set ProxyServer=%3%

- set RecoveryPointName=%3%

- set MountPointRootPathName=%5% (applicabile solo al tipo di test Disco virtuale istantaneo)

Di conseguenza, lo script bat viene richiamato ed eseguito come indicato sotto:

Per il tipo di test Computer virtuale istantaneo:

"%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName

Per il tipo di test Disco virtuale istantaneo:

%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName MountPointRootPathName

Codice di uscita

Specifica il codice di uscita in caso di esito positivo o di errore del processo.

Processo Procedura completata

Specifica che il processo Assured Recovery viene impostato su Procedura completata quando lo script restituisce il codice di uscita.

Processo con errore

Specifica che il processo Assured Recovery viene impostato sulla restituzione di un errore se lo script restituisce il codice di uscita.

Interrompi processo se richiede più di

Specifica se l'esecuzione dello script richiede tempi più lunghi rispetto al tempo specificato.

Valore predefinito: 15 minuti.

Impostazione script pre/post-backup Linux su proxy

Nota: Questa opzione è visibile solo se è stato selezionato il backup o la replica di Linux basato su agente o senza agente basato su host come valore di Origine punto di ripristino per verifica Assured Recovery.

Esegui su server di backup Linux al termine del processo Assured Recovery

Specifica lo script presente sul proxy Linux ed eseguito al termine del processo Assured Recovery sul server di backup Linux.

Esegui su computer virtuale Assured Recovery una volta avviato

Specifica lo script presente sul proxy Linux ed eseguito dopo il riavvio del computer virtuale Assured Recovery.

Interrompi processo se richiede più di

Specifica se l'esecuzione dello script richiede tempi più lunghi rispetto al tempo specificato.

Avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere in un messaggio di posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Note: Non è disponibile per i processi in esecuzione con il server di backup Linux.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy nella finestra di dialogo **Impostazioni di posta elettronica.**

Impostazione delle password di backup per uno o più nodi

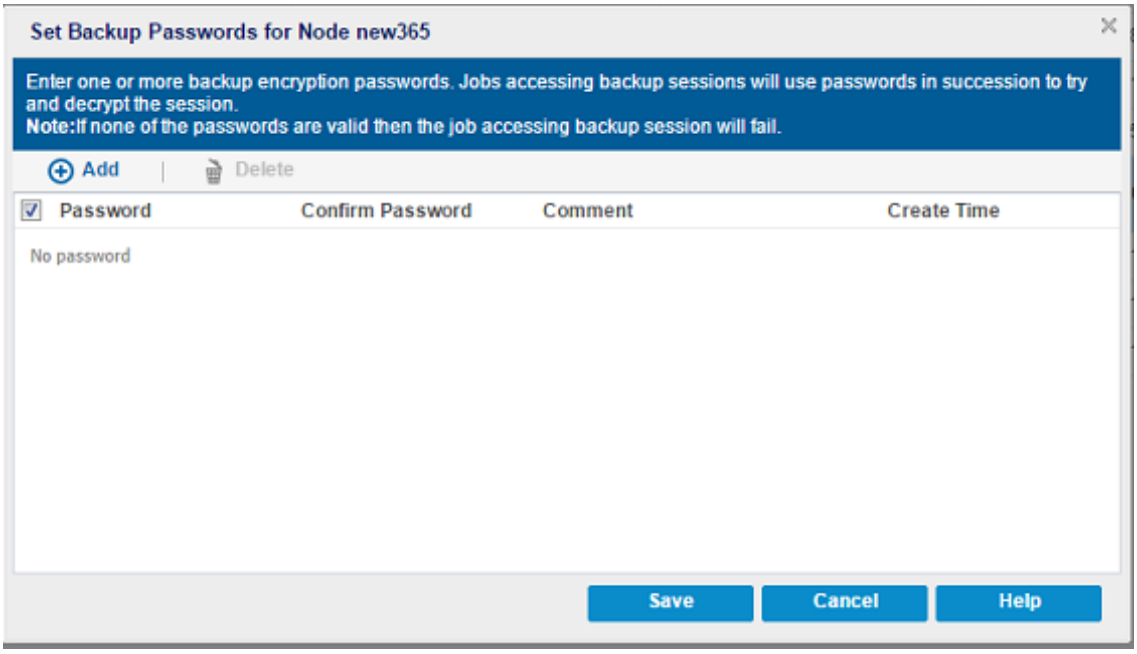
Per garantire che il processo Assured Recovery sia in grado di verificare i punti di ripristino replicati, tale processo consente di specificare password di backup per i dati. I processi che accedono alle sessioni di backup utilizzano continuamente le password per decrittografare la sessione.

Nota: Se nessuna delle password è valida, il processo che accede alla sessione di backup non riesce.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.
3. Dal riquadro centrale, fare clic con il tasto destro del mouse sul nodo, quindi selezionare **Imposta password di backup**.

   Viene visualizzata la finestra di dialogo **Imposta password di backup per il nodo**.

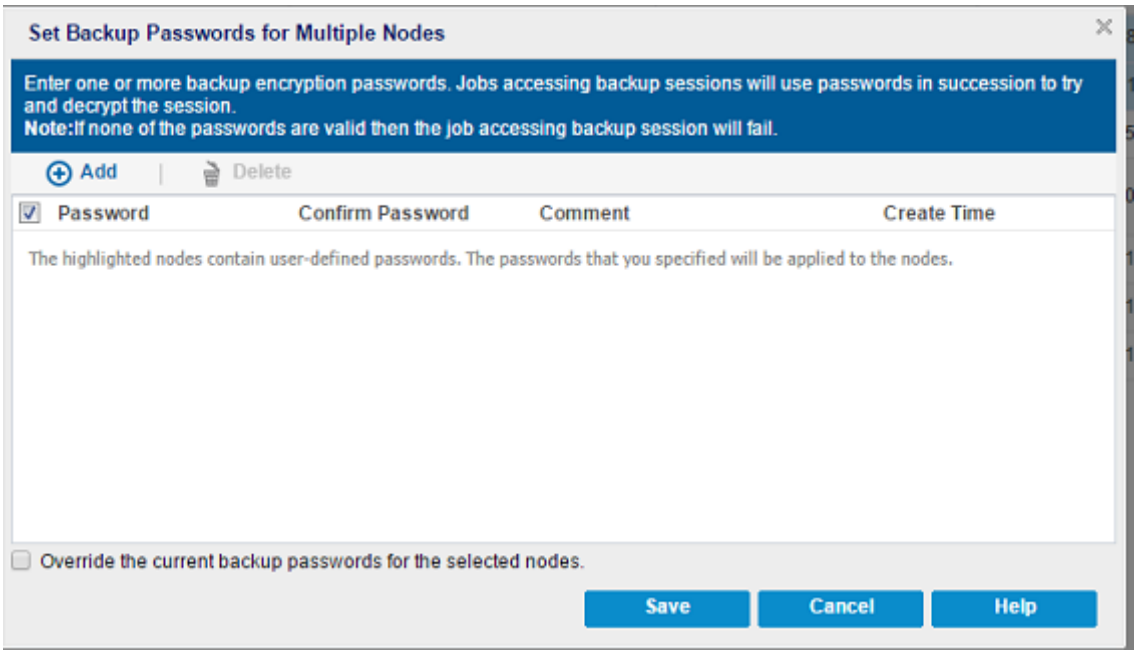


4. La finestra di dialogo **Imposta password di backup** consente di effettuare le azioni seguenti per uno o più nodi:

   Aggiungi: fare clic su **Aggiungi** per aggiungere una o più password di backup ai nodi selezionati.

   Elimina: fare clic su **Elimina** per eliminare una o più password di backup dai nodi selezionati.

Nota: in caso di nodi multipli, è possibile sovrascrivere le password di backup correnti per i nodi multipli selezionando la casella di controllo **Sovrascrivi le password di backup correnti** per i nodi selezionati.



5. Fare clic su **Salva**.

   La finestra di dialogo viene chiusa e le password di backup vengono impostate per i nodi remoti selezionati.

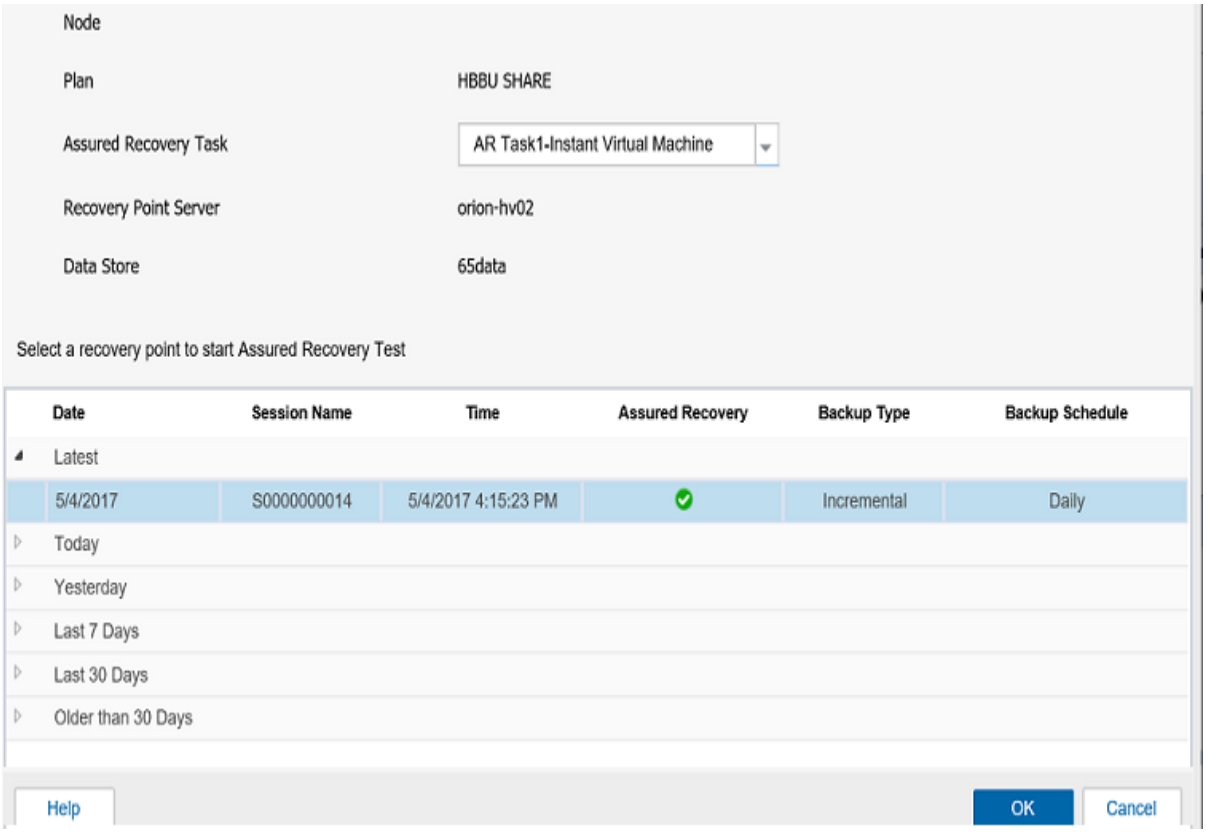
(Facoltativo) Esecuzione manuale del processo Verifica Assured Recovery

Tutti i piani di Arcserve UDP, inclusi i processi Assured Recovery, vengono eseguiti automaticamente e sono controllati dalle impostazioni di pianificazione. Per i processi Assured Recovery, oltre all'esecuzione pianificata, Arcserve UDP consente di eseguire un test manuale di nodi e piani per la verifica Assured Recovery. In questa sezione vengono descritte le diverse procedure per eseguire manualmente la verifica Assured Recovery di nodi e piani.

Per l'esecuzione manuale della verifica Assured Recovery per i nodi, procedere come segue:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a Nodi, quindi fare clic su **Tutti i nodi**.
3. Nel riquadro centrale, selezionare i nodi che dispongono di un piano Assured Recovery assegnato e fare clic su **Azioni**.
4. Tra le opzioni visualizzate per Azioni, fare clic su **Run Assured Recovery Test Now** (Esegui verifica Assured Recovery ora).

   Viene visualizzata la finestra di dialogo Assured Recovery.



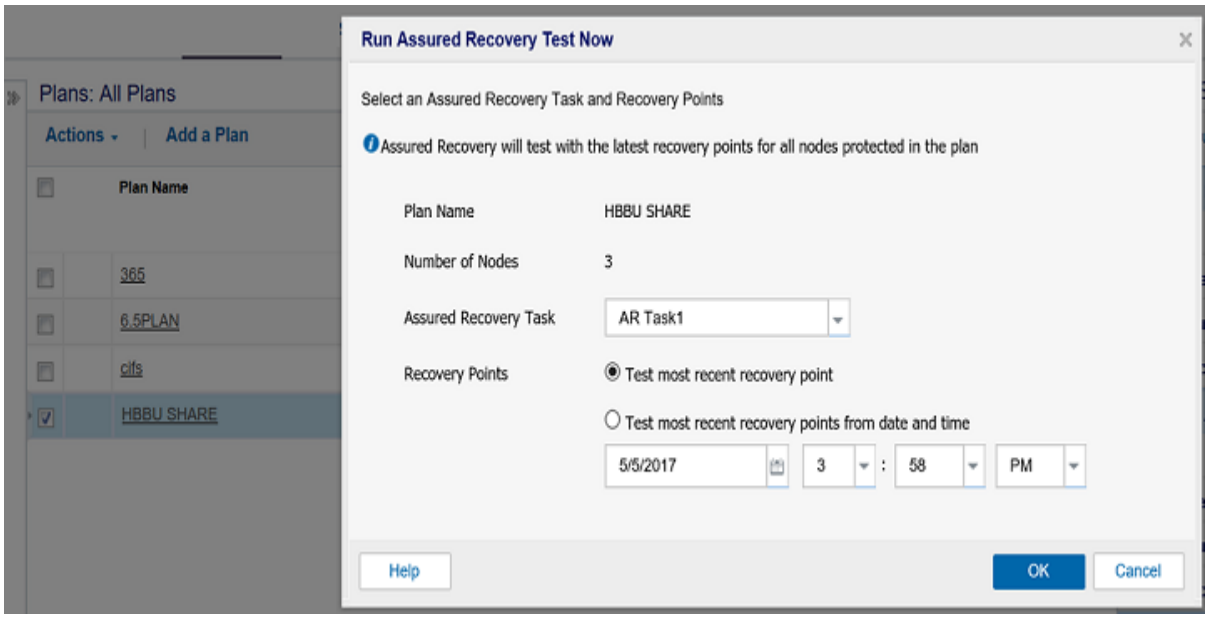
5. Selezionare un'attività Assured Recovery e un punto di ripristino, quindi fare clic su **OK**.

   Viene eseguita la verifica Assured Recovery del nodo.

   Per l'esecuzione manuale della verifica Assured Recovery per i piani, procedere come segue:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a Piani, e fare clic su **Tutti i piani**.
3. Nel riquadro centrale, selezionare un piano Assured Recovery e fare clic su **Azioni**.
4. Tra le opzioni visualizzate per Azioni, fare clic su **Run Assured Recovery Test Now** (Esegui verifica Assured Recovery ora).

   Viene visualizzata la finestra di dialogo Assured Recovery.



5. Selezionare un'attività Assured Recovery e una delle opzioni per il punto di ripristino, quindi fare clic su **OK**.

   Viene eseguita la verifica Assured Recovery del piano.

Creazione di un piano di backup del percorso UNC/NFS

Per proteggere le directory e i file contenuti nel percorso UNC/NFS, è necessario creare un piano. Un piano per il percorso UNC/NFS consiste in un'attività di backup. Questa attività di backup consente di specificare i nodi che si desidera proteggere, la destinazione di backup e la pianificazione dei backup. La destinazione di backup è un Recovery Point Server su cui archiviare i dati sottoposti a backup. La destinazione è una cartella condivisa remota. Per il percorso UNC/NFS, la dimensione massima di backup è 128 TB.

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di una condivisione file
3. Creazione di un piano di backup
4. (Facoltativo) Esecuzione di un backup manuale
5. Creazione di altre attività nel piano UNC/NFS
6. Verifica del backup

Verifica delle considerazioni e dei prerequisiti

Verificare il completamento delle seguenti azioni preliminari:

1. Accedere alla console.
2. Preparare un server proxy di backup del percorso UNC/NFS in cui è installato Agente Arcserve Unified Data Protection per Windows.
3. Disporre delle credenziali utente con almeno l'autorizzazione in lettura per il percorso UNC/NFS che si desidera proteggere.

   Nota: per aggiungere, aggiornare ed eliminare un nodo del percorso UNC/NFS , consultare la sezione Aggiunta e gestione di un percorso UNC/NFS.
4. Accertarsi di disporre di un Recovery Point Server con un archivio dati non di deduplicazione o di deduplicazione.
5. Creare un archivio dati per archiviare i dati di backup.
6. Creare una condivisione file su Nutanix Prism Web Portal.

Considerazioni:

- Utilizzo di licenze aggiuntive per i percorsi UNC. Per risolvere il problema, vedere Risoluzione dei problemi.
- Il proxy di backup è sempre un computer Windows.
- Affinché il piano NFS di Nutanix funzioni, NfsUtils deve essere preinstallato sul computer proxy di backup (come nel caso del piano NFS integrato).
- Per Nutanix File Server, se una delle FSVM del cluster non riesce, l'altra FSVM assume la proprietà principale del File Server e HA viene abilitata per il cluster FSVM.

Creazione di una condivisione file

La pagina Condividi/Esporta consente di creare condivisioni di file standard o distribuite. Una condivisione distribuita o una condivisione principale è un repository in cui risiedono i file personali di un utente, mentre la condivisione standard o la condivisione generica è un archivio condiviso dal gruppo. Una condivisione distribuita viene distribuita nelle directory principali, mentre la condivisione standard si trova su un computer virtuale a file singolo (FSVM). Questa sezione fornisce informazioni su come creare una condivisione file per eseguire il backup UNC/NFS per Nutanix Files.

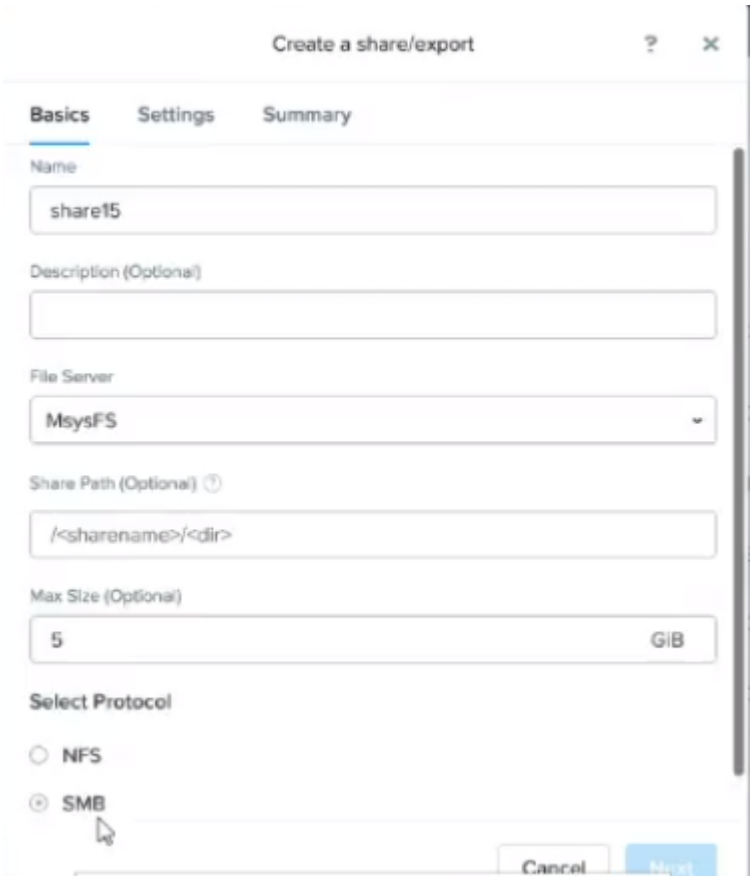
Effettuare le operazioni seguenti:

1. Accedere al portale Web Nutanix Prism.
2. Accedere a **File server** dal menu principale, quindi fare clic su **Condividi/Esporta** nel dashboard File server.

   Viene visualizzata la finestra Crea condivisione/esportazione con la scheda Nozioni di base.
3. Nella scheda Nozioni di base, eseguire le operazioni seguenti, quindi fare clic su **Avanti**:
   - Nome: immettere un nome per la condivisione.

     Nota: le convenzioni di denominazione per il nome della condivisione sono le seguenti:
     - Ogni nome deve essere univoco.
     - I nomi non fanno distinzione tra maiuscole e minuscole.
     - I file consentono i caratteri Unicode.
     - La lunghezza massima del nome è di 80 caratteri.
     - Uno spazio vuoto o uno spazio semplice non possono essere visualizzati come primo o ultimo carattere nel nome.
     - I nomi che terminano con $ sono condivisioni nascoste.
   - Descrizione (facoltativo): immettere una descrizione per la condivisione, se necessario.
   - File server: dall'elenco a discesa, selezionare un file server in cui risiede la condivisione.
   - Percorso di condivisione (facoltativo): fornire il percorso del file per la condivisione.
   - Dimensione massima (facoltativo): immettere la dimensione massima della condivisione. Per impostazione predefinita, la dimensione è in GiB.
   - Seleziona protocollo: selezionare **SMB** come protocollo.

     Nota: per attivare la funzionalità multiprotocollo, selezionare la casella di controllo **Abilita accesso multiprotocollo per NFS**.



4. Nella scheda Impostazioni, conservare le impostazioni predefinite o apportare le modifiche necessarie, quindi fare clic su **Avanti**.

   Utilizzare il tipo di condivisione "Distribuito" anziché "Standard"

   Consente di creare una condivisione distribuita.

   Nota: per impostazione predefinita, le condivisioni su distribuzioni FSVM singole sono di tipo standard.

   Attiva ripristino self-service

   Consente di ripristinare i file da snapshot precedenti.

   Attiva compressione file system

   Consente di risparmiare spazio e ridurre i dati sulla condivisione mediante la compressione in linea dei dati scritti.

   Nota: assicurarsi di disattivare la compressione a livello di contenitore. Se è stata attivata la compressione, l'opzione Abilita compressione file system viene disattivata.

   Abilita enumerazione basata sull'accesso (ABE)

   Consente di attivare l'enumerazione basata sull'accesso (ABE).

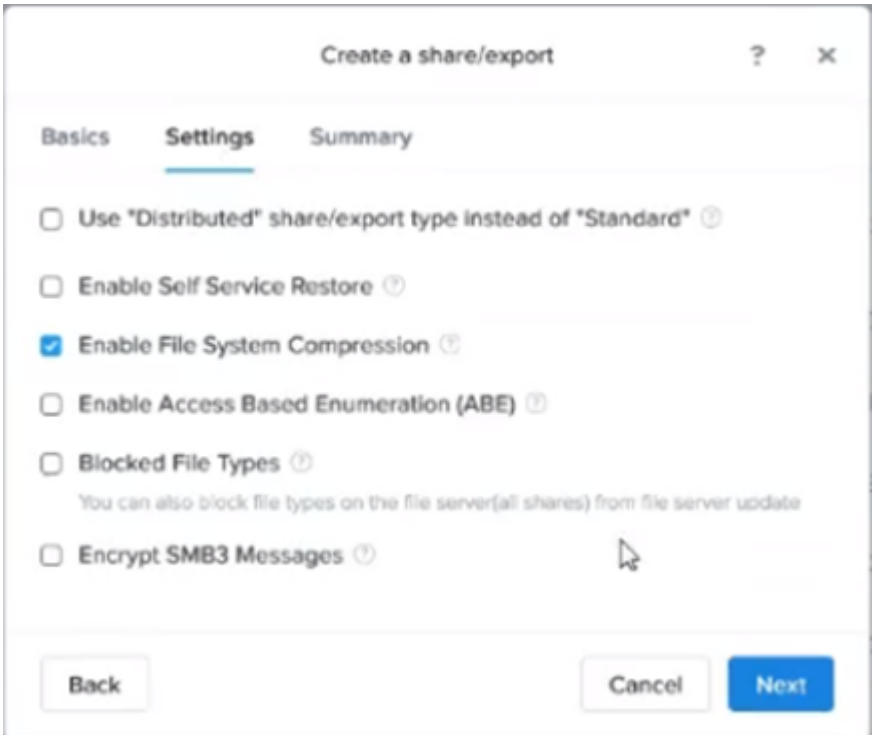
Tipi di file bloccati

Consente di specificare i tipi di file bloccati.

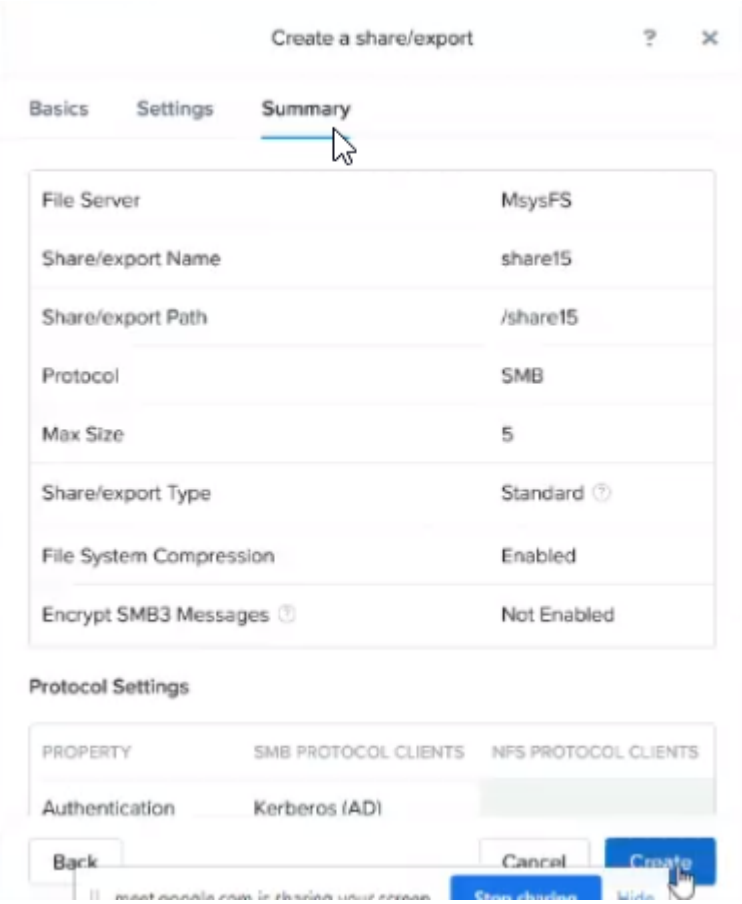
Immettere un elenco separato da virgole dei tipi di file che si desidera bloccare dalla condivisione.

Crittografa messaggi SMB3

Consente di attivare la crittografia dei messaggi tra il file server e il client.



5. Nella pagina Riepilogo, verificare i dettagli, quindi fare clic su **Crea**.



Nota: per apportare modifiche alle impostazioni delle pagine precedenti, fare clic su **Indietro**.

La condivisione file è stata creata correttamente.

Nota: successivamente, copiare il percorso di montaggio e mappare la condivisione appena creata nell'UDP locale. Per ulteriori informazioni, consultare il passaggio 6 (a1) della sezione Definizione dell'origine.

Creazione di un piano di backup con un'attività del percorso UNC/NFS

Un piano di backup include un'attività di backup che esegue un backup del nodo fisico e archivia i dati nella destinazione specificata. Ciascuna attività consiste di parametri che definiscono l'origine, la destinazione, la pianificazione, e altri dettagli di backup.

Effettuare le operazioni seguenti:

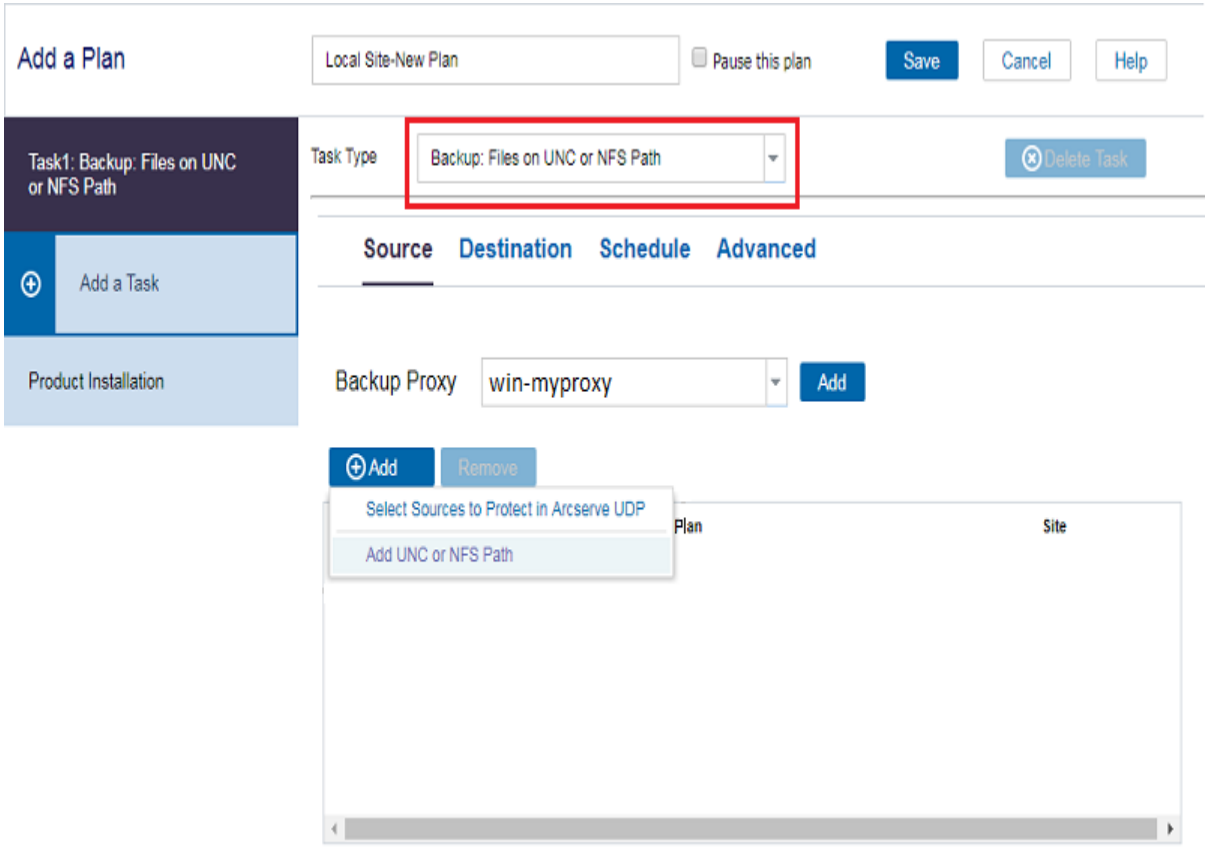
1. Accedere alla console Arcserve UDP.
2. Fare clic sulla scheda **Risorse**.
3. Dal riquadro sinistro, accedere a **Piani**, quindi fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
4. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina Aggiungi un piano.
5. Immettere un nome per il piano.
6. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
7. Dall'elenco a discesa Tipo di attività, selezionare **Backup: File nel percorso UNC/NFS**.



Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine che si desidera proteggere. È possibile selezionare più di un nodo per un piano. Se non sono stati aggiunti nodi alla console, è possibile aggiungerli in fase di creazione o modifica di un piano dalla pagina Origine. È inoltre possibile salvare un piano senza aggiungere nessun nodo di origine. Il piano viene distribuito soltanto dopo l'aggiunta dei nodi di origine.

Effettuare le operazioni seguenti:

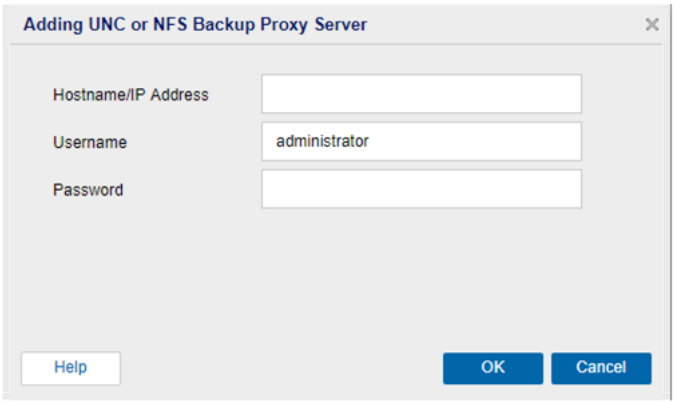
1. Fare clic sulla scheda **Origine**.
2. Se il proxy di backup è già stato aggiunto, selezionarlo dall'elenco a discesa Proxy di backup.

   Il server proxy è un nodo in cui viene installato Agente Arcserve Unified Data Protection per Windows.



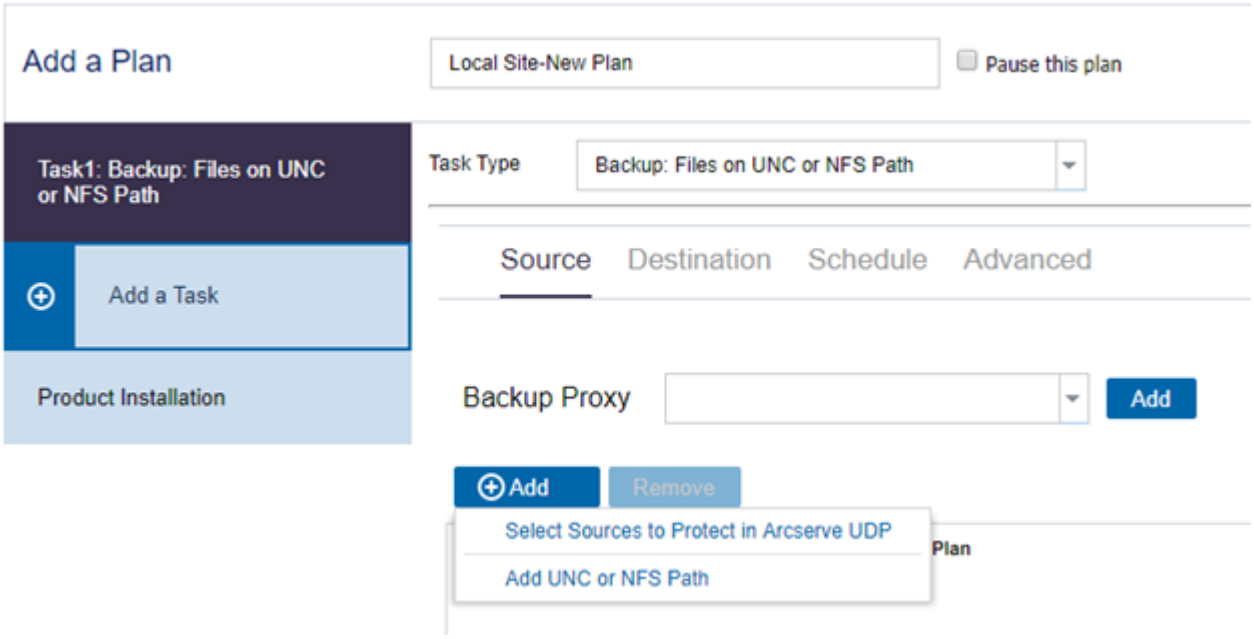
3. Se il proxy di backup non viene aggiunto, procedere come segue:
   a. Fare clic su **Aggiungi**.

      Viene visualizzata la finestra di dialogo per l'aggiunta del server proxy di backup del percorso UNC o NFS.



   b. Specificare i dettagli del server proxy, quindi fare clic su **OK**.

4. Per aggiungere il nodo del percorso UNC o NFS, fare clic su **+Aggiungi**, quindi selezionare una delle seguenti opzioni:



Selezionare le origini da proteggere in Arcserve UDP

Consente di aprire la finestra di dialogo Selezionare i nodi da proteggere in cui è possibile scegliere i nodi dall'elenco visualizzato. Selezionare questa opzione se sono stati già aggiunti nodi alla Console.

Aggiunta del percorso UNC o NFS

Consente di aprire la finestra di dialogo Aggiungi nodi alla Console Arcserve UDP. Selezionare questa opzione se non sono stati aggiunti i nodi e si desidera aggiungere manualmente i nodi da proteggere.

5. Se si opta per la **selezione delle origini da proteggere in Arcserve UDP**, procedere come segue:

   a. (Facoltativo) Selezionare un filtro dall'elenco a discesa Gruppi per filtrare i nodi. Immettere parole chiave per applicare ulteriori filtri ai nodi.



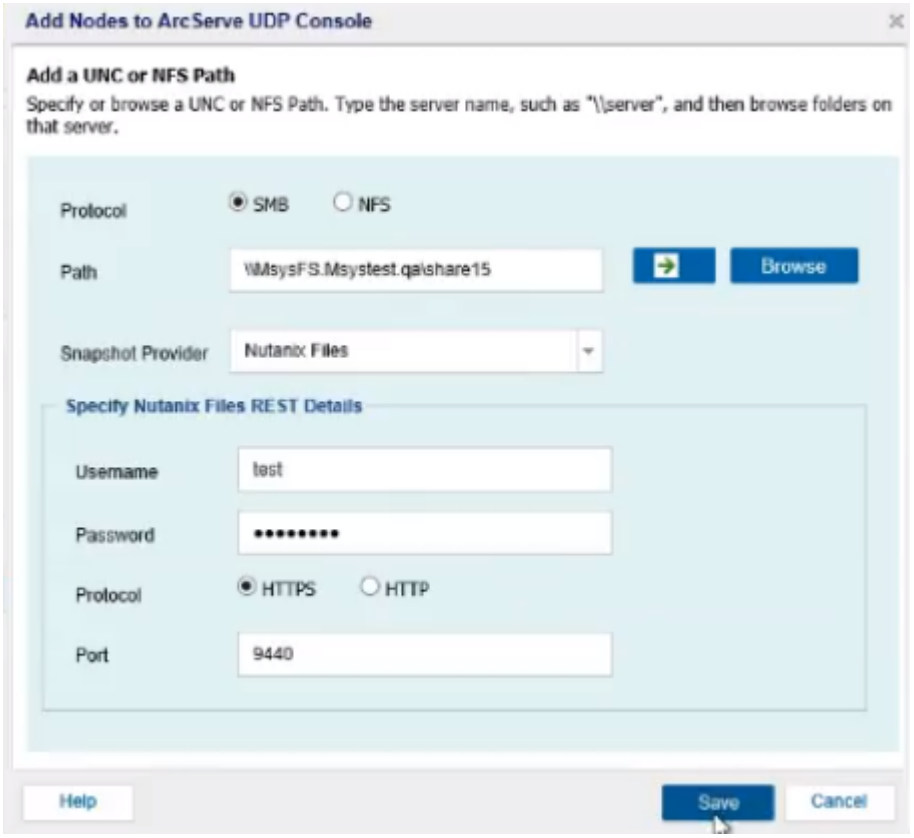
I nodi vengono visualizzati nell'area Nodi disponibili.

b. Selezionare i nodi dall'area Nodi disponibili e fare clic sull'icona **Aggiungi tutti i nodi** (>>) o **Aggiungi i nodi selezionati** (>).

I nodi selezionati vengono visualizzati nell'area Nodi selezionati.

c. Fare clic su **OK** per chiudere la finestra di dialogo.

6. Se si seleziona l'opzione **Aggiungi percorso UNC o NFS**, procedere come segue nella pagina Aggiungi percorso UNC o NFS:



a. Selezionare **SMB** o **NFS** come protocollo.

- Se si seleziona **SMB**, procedere come segue:

1. Immettere il percorso UNC nel formato seguente:

   *Hostname**share*

   Note:

   - Pur fornendo la condivisione Nutanix Files come origine per il backup con Nutanix Files come provider di snapshot, i backup possono essere eseguiti solo a livello di condivisione ma non a livello di sottocartella.
   - Per ottenere il percorso UNC, procedere come segue:

     a. Selezionare la condivisione appena creata nel riquadro centrale.

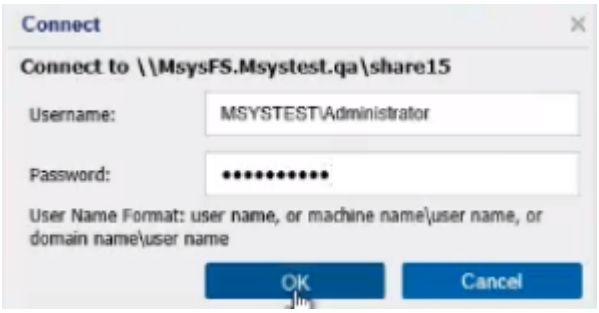
     b. Nella colonna Condividi/Esporta dettagli, dal riquadro Riepilogo, accedere a **Percorso di montaggio**, quindi copiare il percorso di montaggio.

     Se il percorso UNC è valido, vengono visualizzate una freccia rivolta verso destra e l'opzione Sfoglia.

2. Fare clic sulla freccia destra (>) per convalidare il percorso UNC.

   Viene visualizzata la finestra di dialogo Connetti.

3. Immettere il nome utente e la password, quindi fare clic su **OK**.



Nella finestra di dialogo Aggiungi nodi alla console Arcserve UDP viene riportato il percorso UNC verificato.

- Se si seleziona NFS, procedere come segue:
  1. Immettere il percorso UNC nel formato seguente:

     *Hostname**share*

  2. Selezionare codifica dalle opzioni disponibili - ANSI, GB2312-80, KSC5601, BIG5, SHIFT JIS, EUC-KR, EUC-TW, EUC-JP.

     Il valore predefinito è ANSI.

     Nota: durante il backup di una cartella NFS condivisa, tutti i file e le cartelle il cui nome è associato a una codifica di lingua non supportata vengono ignorati oppure il loro nome non viene visualizzato correttamente.

b. Dall'elenco a discesa Provider snapshot, selezionare **Nutanix Files**.

c. Per la casella Specificare i dettagli REST di Nutanix Files, fornire le seguenti credenziali:

   Nome utente

   Fa riferimento al nome utente creato dall'utente dell'API REST utilizzando Nutanix Prism.

   Password

   Fa riferimento alla password per il nome utente.

   Protocollo

   Specificare il protocollo che si desidera utilizzare per la comunicazione con il server di destinazione. Le opzioni disponibili sono HTTP e HTTPS.

   Nota: Per una comunicazione più sicura, selezionare il protocollo HTTPS.

   Porta

   Si riferisce al numero di porta. Il valore predefinito della porta è 9440, il quale consente di accedere alle chiamate API REST e a Prism.

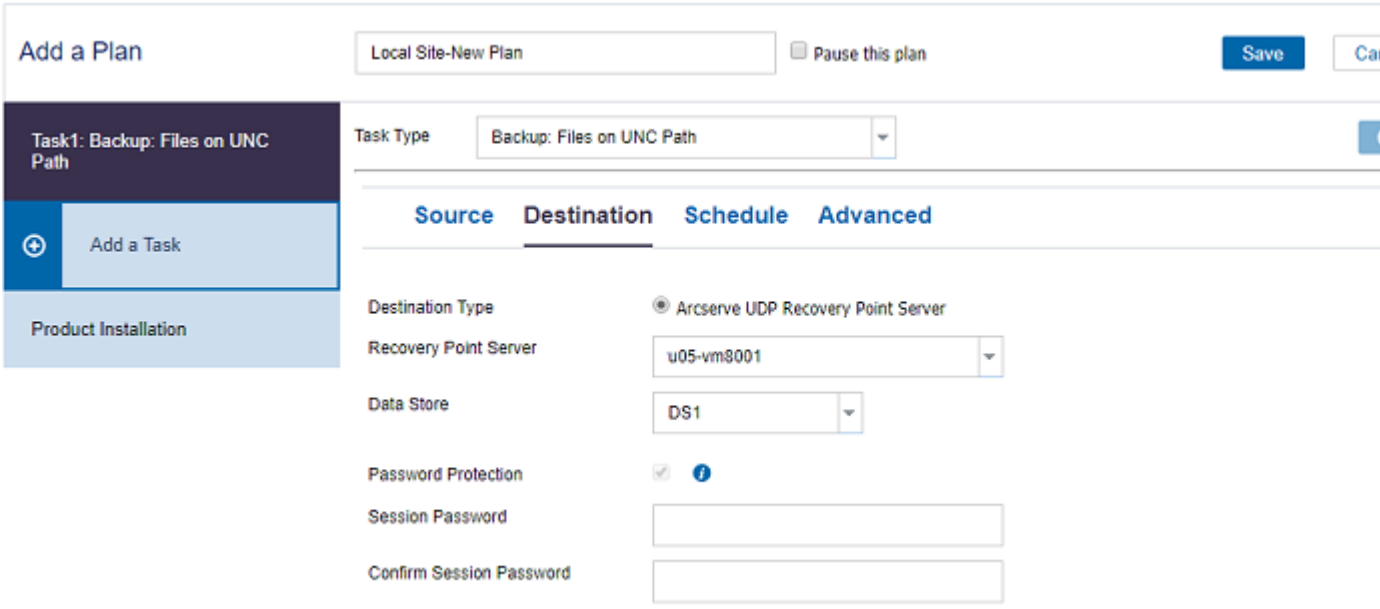
d. Fare clic su **Salva**.

   Nota: se la connessione al server Nutanix Files non riesce, viene visualizzata la finestra di dialogo Errore o la finestra di notifica. Fare clic su **OK** per chiudere la finestra di dialogo di errore.

L'origine viene specificata.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.



Specificare i seguenti dettagli:

- Tipo di destinazione: verificare che l'opzione **Recovery Point Server di Arcserve UDP** sia selezionata per impostazione predefinita.
- Recovery Point Server: selezionare un Recovery Point Server dall'elenco a discesa.
- Archivio dati: selezionare un archivio dati dall'elenco a discesa.

  L'elenco mostra tutti gli archivi dati creati sul Recovery Point Server specificato.
- Protezione password: fornire una password di sessione, quindi digitare nuovamente la password di sessione per confermarla.

  Nota: la password di sessione è facoltativa se la destinazione di backup è un archivio di dati RPS non crittografato.

  La destinazione viene specificata.

Definizione della pianificazione

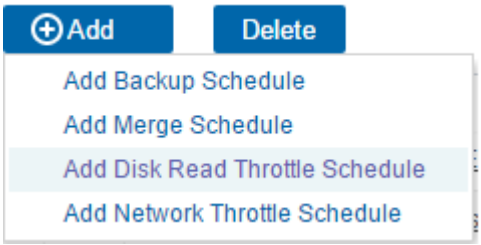
La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito una pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

Effettuare le operazioni seguenti:

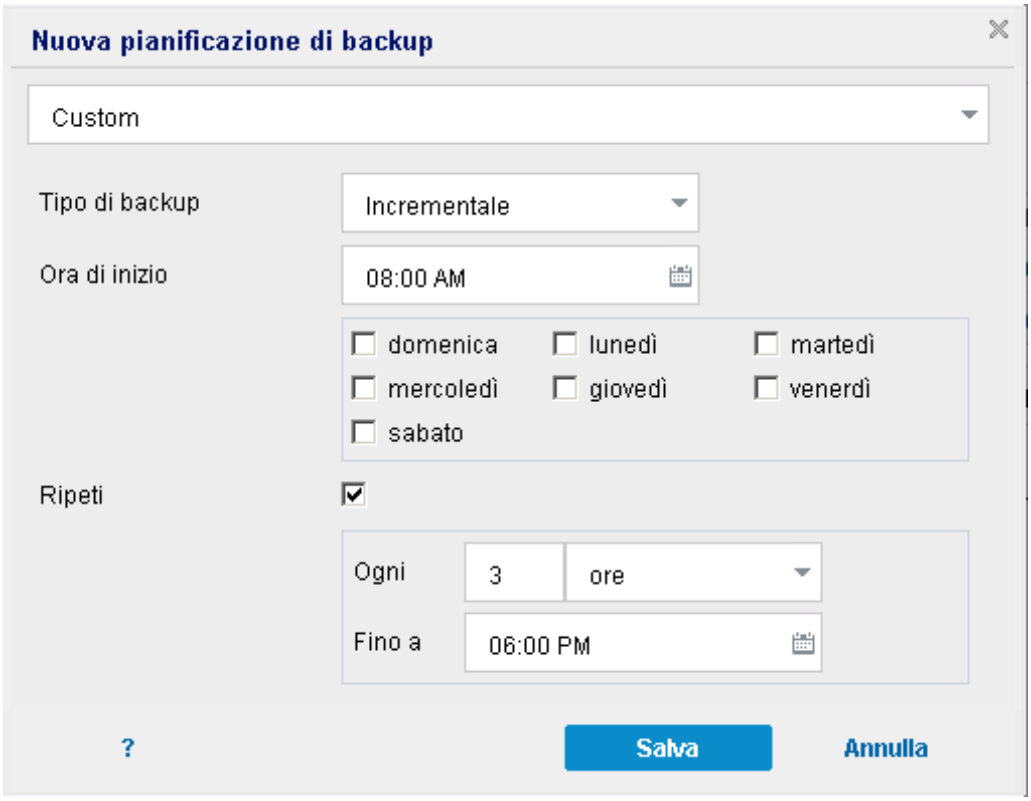
1. Aggiungere le pianificazioni di backup, di unione, Limitazione di lettura del disco e Limite delle risorse di rete.



Aggiunta di una pianificazione di backup

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

   Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni del backup.

Verifica

Specifica la pianificazione dei backup di verifica.

Arcserve UDP controlla che i dati protetti siano validi e completi eseguendo una verifica di affidabilità dell'immagine di backup archiviata sull'origine di backup. Se necessario esegue la risincronizzazione dell'immagine. Un backup di verifica controlla il backup più recente di ogni blocco e lo confronta con il contenuto e le informazioni di origine. Questo confronto consente di verificare che il blocco di backup più recente rappresenti le informazioni corrispondenti all'origine. Se l'immagine di backup di un blocco non corrisponde all'origine (probabilmente a causa di modifiche apportate al sistema dall'ultimo backup), Arcserve UDP aggiorna (risincronizza) il backup del blocco non corrispondente. Sebbene si tratti di una procedura poco frequente, il backup di verifica può essere utilizzato per ottenere le stesse garanzie di un backup completo, ma senza occupare lo stesso spazio.

Vantaggi: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.

Svantaggi: il backup di verifica richiede tempi di esecuzione più lunghi, in quanto esegue il confronto di tutti i blocchi originali con i blocchi del backup più recente.

Incrementale

Specifica la pianificazione dei backup incrementali.

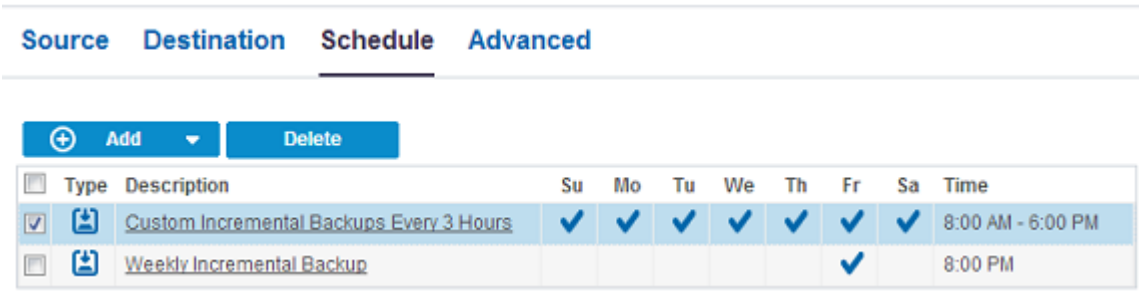
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

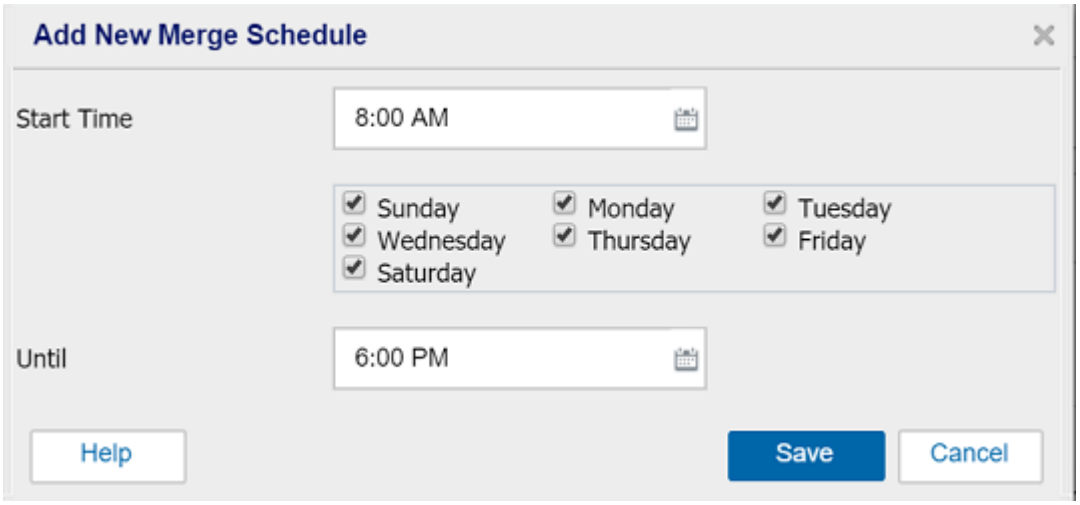
La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di unione**.

   La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.



b. Specificare l'ora di inizio per l'avvio del processo di unione.

c. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

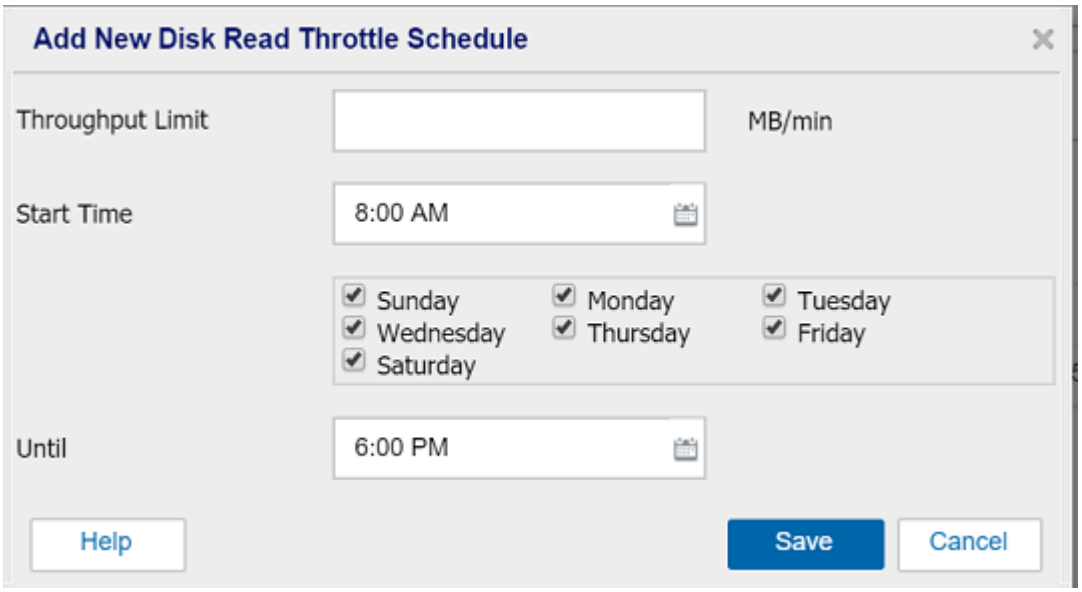
d. Fare clic su **Salva**.

La Pianificazione di unione viene specificata e viene visualizzata nella pagina **Pianificazione**.

Aggiunta della pianificazione di limitazione di lettura del disco

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di limitazione di lettura del disco**.

   Viene visualizzata la finestra di dialogo **Aggiungi nuova pianificazione della limitazione di lettura del disco**.



b. Specificare il limite di velocità effettiva in MB per unità di minuti.

c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

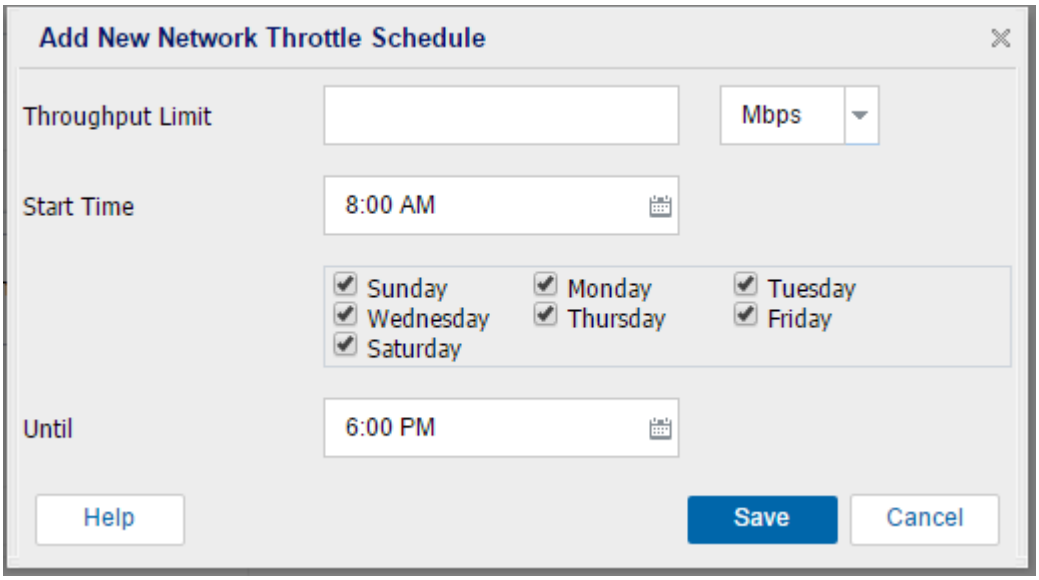
La pianificazione della limitazione di lettura del disco specificata viene visualizzata nella pagina **Pianificazione**.

Aggiunta di una pianificazione del limite delle risorse di rete

Nota: La pianificazione Limite delle risorse di rete viene visualizzata solo per il backup basato sull'agente Windows quando viene definita come destinazione per il piano un archivio dati con deduplicazione abilitata.

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse di rete**.

   Viene visualizzata la finestra di dialogo **Aggiungi una nuova pianificazione del limite delle risorse di rete**.



b. Specificare il limite di velocità effettiva in Mbps o Kbps.

   Nota: Il valore minimo predefinito è 500 kbps. Per modificare il valore predefinito valore procedere come segue:

   i. Dal percorso di registro SOFTWARE\Arcserve\Unified Data Protection\Management\Console, aggiungere una chiave MinNetworkThrottleValueInKpbs, tipo REG_SZ e impostare il valore.

   ii. Riavviare il servizio di gestione di Arcserve UDP.

   iii. Modificare il piano o crearne uno nuovo.

   Il valore personalizzato inizia ad avere effetto.

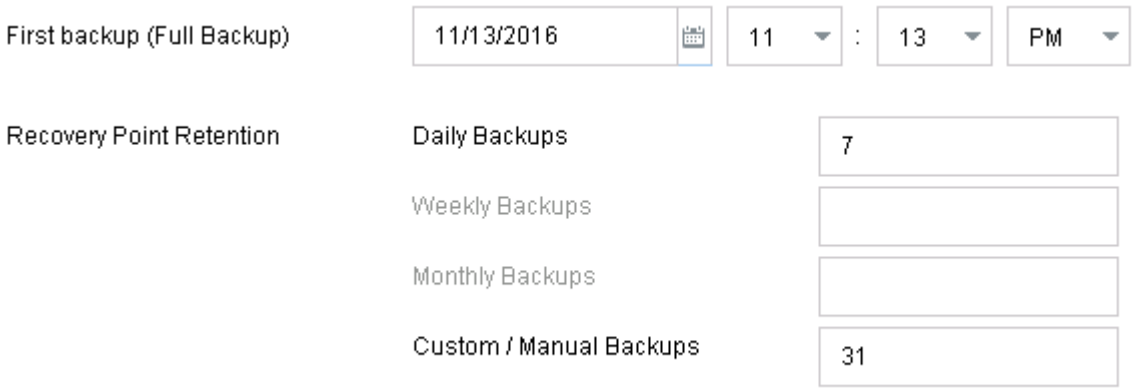
c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

La pianificazione del limite delle risorse di rete specificata viene visualizzata nella pagina **Pianificazione**.

2. Specificare l'ora di inizio per il backup pianificato.



3. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

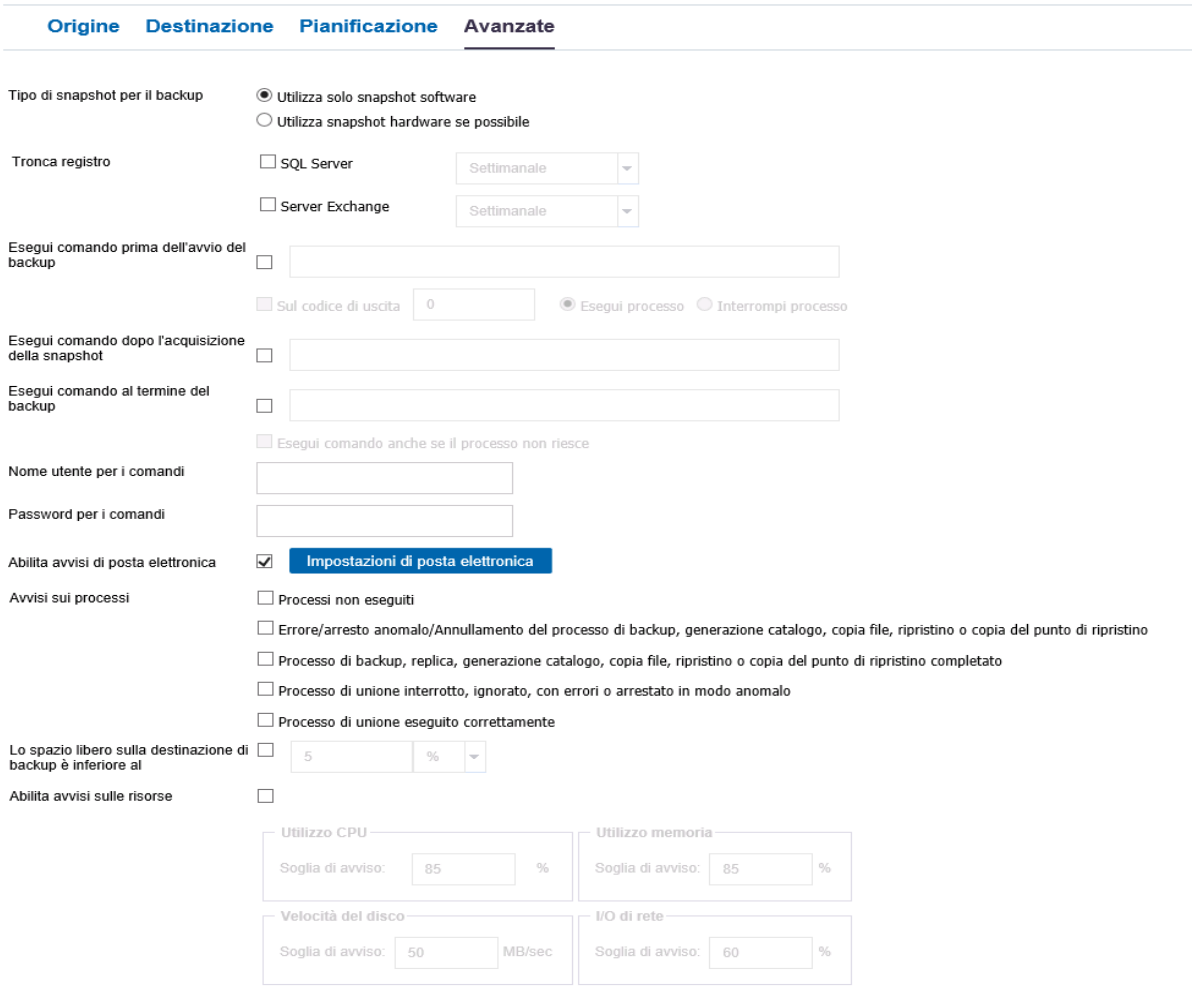
   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo Pianificazione di backup.

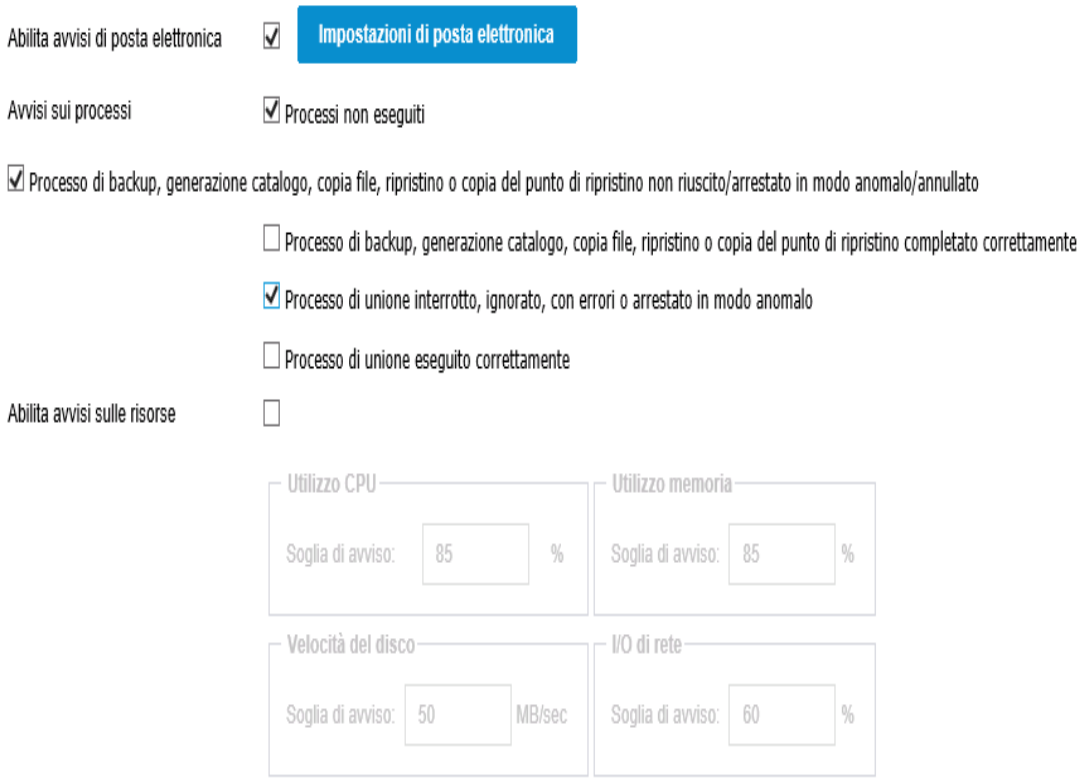
   Viene specificata la pianificazione.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione delle impostazioni per troncare i registri, l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda Avanzate:


Origine
Destinazione
Pianificazione
Avanzate
Tipo di snapshot per il backup
Utilizza solo snapshot software
Utilizza snapshot hardware se possibile
Tronca registro
SQL Server
Settimanale
Server Exchange
Settimanale
Esegui comando prima dell'avvio del backup
Sul codice di uscita
0
Esegui processo
Interrompi processo
Esegui comando dopo l'acquisizione della snapshot
Esegui comando al termine del backup
Esegui comando anche se il processo non riesce
Nome utente per i comandi
Password per i comandi
Abilita avvisi di posta elettronica
Impostazioni di posta elettronica
Avvisi sui processi
Processi non eseguiti
Errore/arresto anomalo/Annullamento del processo di backup, generazione catalogo, copia file, ripristino o copia del punto di ripristino
Processo di backup, replica, generazione catalogo, copia file, ripristino o copia del punto di ripristino completato
Processo di unione interrotto, ignorato, con errori o arrestato in modo anomalo
Processo di unione eseguito correttamente
Lo spazio libero sulla destinazione di backup è inferiore al
5
%
Abilita avvisi sulle risorse
Utilizzo CPU
Soglia di avviso:
85
%
Utilizzo memoria
Soglia di avviso:
85
%
Velocità del disco
Soglia di avviso:
50
MB/sec
I/O di rete
Soglia di avviso:
60
%



Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

   Tipo di snapshot per il backup

   Selezionare una delle seguenti opzioni per la snapshot del backup:

   Utilizza solo snapshot software

   Specifica che il tipo di backup utilizza solo la snapshot software. Arcserve UDP non cercherà la snapshot hardware. La snapshot software utilizza un numero minore di risorse sui computer virtuali. È possibile utilizzare questa opzione se il server presenta configurazioni e velocità di elaborazione inferiori.

   Utilizza snapshot hardware se possibile

   Specificare che il tipo di backup verifica innanzitutto una la presenza di una snapshot hardware. Se tutti i criteri vengono soddisfatti, il tipo di backup utilizza la snapshot hardware.

   Nota: Per ulteriori informazioni sui criteri della snapshot hardware, consultare la sezione dedicata ai prerequisiti.

   Tronca registro

Consente di specificare la pianificazione per troncare i registri per SQL Server ed Exchange Server. È possibile specificare la pianificazione come **Giornaliero**, **Settimanale** o **Mensile**.

Abilitare l'eliminazione dei registri con cadenza oraria per SQL Server tramite un'opzione del Registro di sistema

- Configurare le impostazioni del piano. Selezionare l'opzione "SQL Server" nella sezione "Tronca registro" della scheda "Avanzate", quindi selezionare "Ogni giorno".
- Impostare la chiave del Registro di sistema sul computer SQL Server che ospita l'agente UDP. "PurgeSqlLogPerHour" è dell'intervallo di tempo in ore per l'eliminazione del registro di SQL Server.

  Percorso: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

  Nome valore: PurgeSqlLogPerHour (indica l'intervallo di tempo in ore per l'eliminazione del registro di SQL Server).

  Tipo valore: REG_DWORD

Nome utente

Consente di specificare l'utente autorizzato per l'esecuzione di uno script.

Password

Consente di specificare la password dell'utente autorizzato all'esecuzione dello script.

Esegui un comando prima dell'avvio del backup

Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso completo di archiviazione dello script. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Esegui processo** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

Esegui un comando dopo l'acquisizione della snapshot

Consente di eseguire uno script dopo l'acquisizione della snapshot del backup. Specificare il percorso completo di archiviazione dello script.

Per eseguire lo script successivo alla snapshot anche durante un errore di snapshot, selezionare l'opzione **Esegui il comando anche se la snapshot non riesce**.

Esegui un comando al completamento del backup

Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso completo di archiviazione dello script.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere mediante posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy. Per ulteriori informazioni sulla configurazione delle impostazioni di posta elettronica, consultare la sezione Configurazione di posta elettronica e avvisi.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

Abilita avvisi sulle risorse

Consente di specificare una soglia per Utilizzo CPU, Memoria, Velocità del disco, I/O di rete. È possibile fornire il valore in percentuale. Si riceve un messaggio di posta elettronica al superamento del valore Soglia di avviso.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su Salva.

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: Se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo.

Il piano di backup viene creato e distribuito automaticamente al nodo di origine. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

(Facoltativo) Esecuzione di un backup manuale

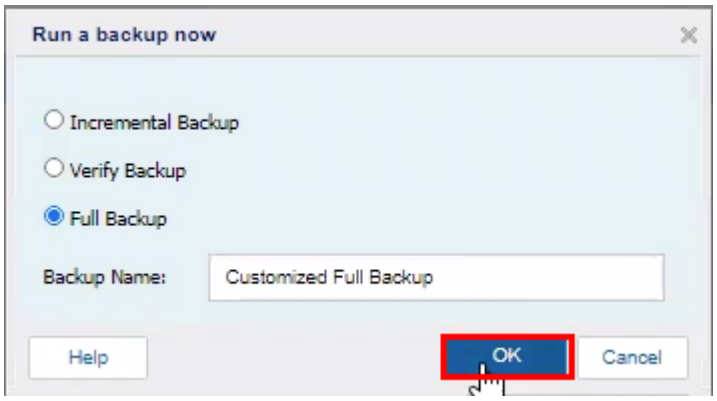
In genere, i backup vengono eseguiti automaticamente e vengono controllati attraverso le impostazioni di pianificazione. In aggiunta al backup pianificato, un backup manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze. Ad esempio, se si dispone di una pianificazione di ripetizione per backup completi, incrementali e di verifica e si desidera apportare modifiche sostanziali al computer, sarà necessario eseguire un backup manuale immediato senza attendere l'esecuzione del successivo backup pianificato.

Effettuare le operazioni seguenti:

1. Accedere alla console Arcserve UDP.
2. Accedere a **Risorse** > **Piano** > **Tutti i piani**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i piani.
3. Fare clic con il pulsante destro del mouse sul piano, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
4. Nella finestra di dialogo Esegui backup immediato, selezionare il tipo di backup che si desidera eseguire, quindi specificare il nome del backup, se necessario.



Le opzioni disponibili sono:

Backup incrementale

Avvia un backup incrementale del computer. Un backup incrementale esegue il backup solo dei blocchi modificati dopo l'ultimo backup.

Nota: se si esegue un backup per la prima volta, il backup completo viene avviato automaticamente anche se è stata selezionata l'opzione Backup incrementale.

I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup con dimensioni molto ridotte. Questa modalità di esecuzione backup è ottimale.

Backup di verifica

Avvia un backup di verifica individuando il backup più recente di ciascun blocco e ne confronta il contenuto e le informazioni con l'origine. Questo confronto consente di verificare che il blocco di backup più recente rappresenti le informazioni corrispondenti all'origine. Se l'immagine di backup di un blocco non corrisponde all'origine, l'agente Arcserve UDP (Windows) aggiornerà (risincronizzerà) il backup di tale blocco.

Vantaggi: viene prodotta un'immagine di backup di dimensioni molto ridotte rispetto al backup completo, poiché viene eseguito solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono all'ultimo backup.

Svantaggi: la velocità del backup è ridotta poiché tutti i blocchi del disco di origine vengono confrontati con i blocchi dell'ultimo backup.

Backup completo

Avvia un backup completo dell'intero computer o dei volumi selezionati.

Note:

- Se si aggiunge un nuovo volume all'origine di backup, il volume appena aggiunto verrà sottoposto a un backup completo, indipendentemente dal metodo di backup generale utilizzato.
- Se non viene specificato alcun nome di backup, per impostazione predefinita viene automaticamente denominato Backup completo personalizzato/Incrementale/Di verifica.

5. Fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.

6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.

7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Nota: è possibile eseguire un solo processo alla volta. Se si tenta di avviare manualmente un processo di backup durante l'esecuzione di un altro processo, verrà visualizzato un messaggio di avviso indicante che un altro processo è in esecuzione, per cui sarà necessario riprovare in un momento successivo.

   Il backup manuale è stato eseguito correttamente.

Altre attività nel piano UNC/NFS

È possibile seguire le attività del piano del percorso UNC/NFS con altre attività. È possibile creare attività di completamento, come la copia di un punto di ripristino, la replica in Arcserve Cloud, la copia su nastro, la replica semplice e la replica su un server RPS gestito in remoto.

Attività di copia dei punti di ripristino

Consente di copiare i punti di ripristino in una cartella locale o condivisa oppure su cloud.

Copia su nastro

Consente di archiviare il punto di ripristino su nastro mediante l'integrazione con Arcserve Backup.

Attività di replica

Consente di creare un'attività per la replica dei dati di backup da un Recovery Point Server a un altro.

Replica in un Recovery Point Server gestito remotamente

Consente di creare un'attività di replica o inviare dati in un Recovery Point Server remoto.

Replica in Arcserve Cloud

Consente di creare un'attività di replica o inviare dati in un Recovery Point Server cloud.

Verifica di Assured Recovery

Consente di verificare l’accessibilità e i valori di Assured Recovery dei dati.

Verifica del backup

Per verificare il processo di backup, confermare di avere creato correttamente il piano di backup. Dopo avere verificato che il piano è stato creato correttamente, confermare se il processo di backup è in esecuzione secondo quanto pianificato. È possibile verificare lo stato dei processi di backup dalla scheda **Processi**.

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Attenersi a uno dei seguenti metodi per verificare i processi di backup:

Metodo 1

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Tutti i processi completati**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Metodo 2

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Processi completati correttamente**.

   L'elenco dei processi di backup completati viene visualizzato nel riquadro centrale.
3. Fare clic sul processo che si desidera verificare.

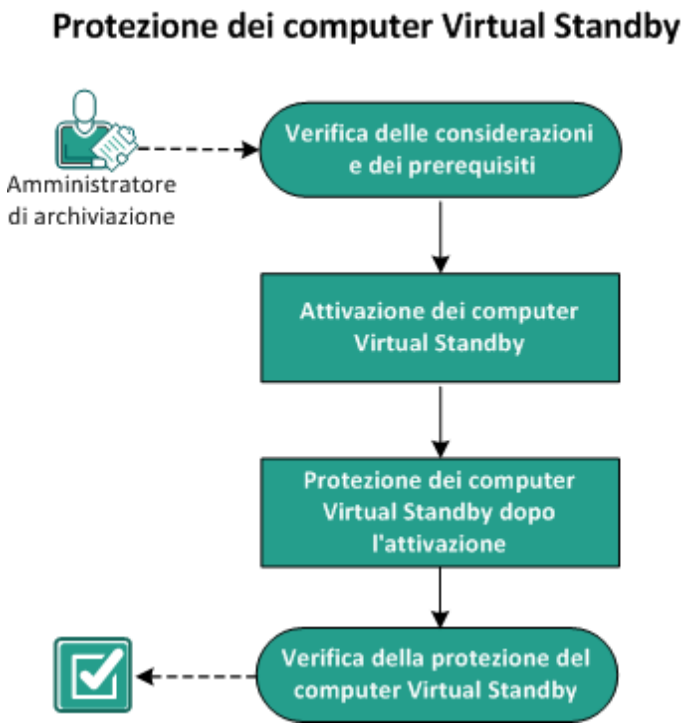
   Il riquadro destro viene aggiornato.
4. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
5. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Protezione dei computer Virtual Standby

È possibile eseguire il backup di computer Virtual Standby ed impedire il danneggiamento dei dati. Prima di proteggere il computer, è necessario attivarlo.

Nel diagramma seguente viene illustrato il processo di protezione dei computer Virtual Standby:



Come procedere?

- Verifica delle considerazioni e dei prerequisiti
- Attivazione dei computer Virtual Standby
- Protezione dei computer Virtual Standby dopo l'attivazione
- Verifica della protezione del computer Virtual Standby

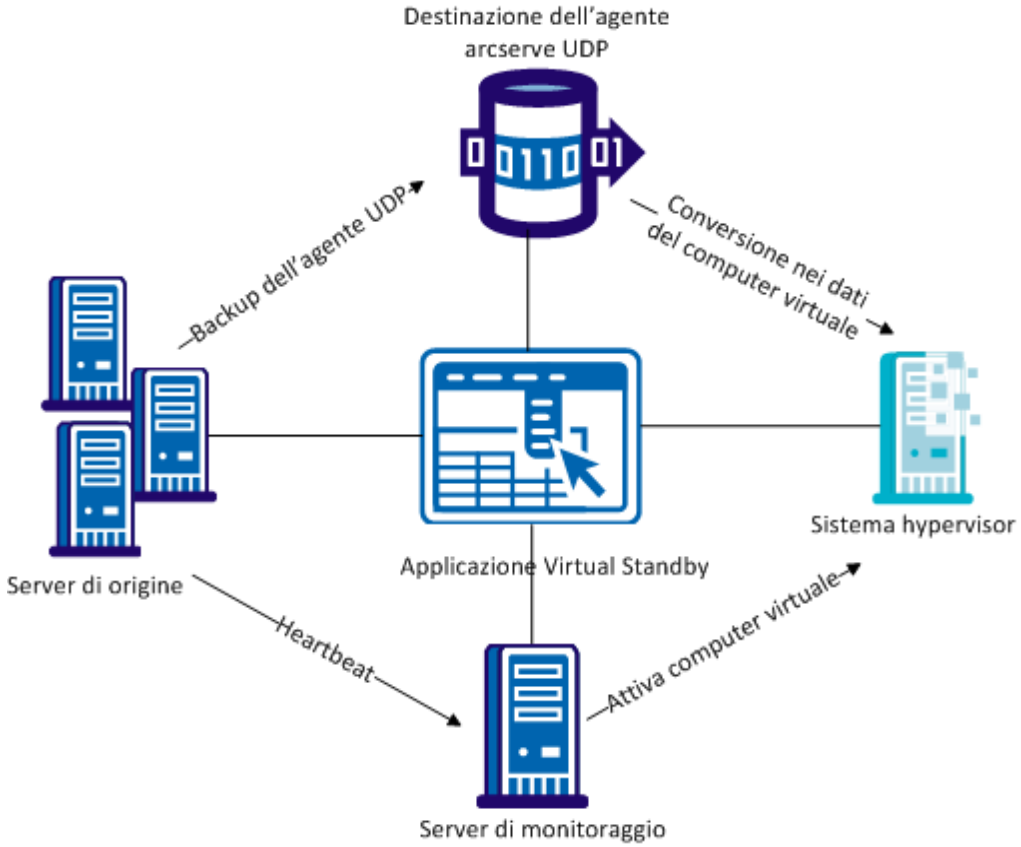
Verifica delle considerazioni e dei prerequisiti

Verificare il completamento delle seguenti azioni preliminari:

- Avere effettuato l'accesso alla Console
- Disporre di un computer Virtual Standby
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Attivazione dei computer Virtual Standby

È possibile attivare i computer Virtual Standby e proteggere i computer virtuali una volta attivati. Nel diagramma seguente viene descritto il flusso di processo per l'attivazione dei computer virtuali:



Attivazione dei computer Virtual Standby a partire da snapshot del punto di ripristino

Virtual Standby può essere configurato in modo tale da attivare computer Virtual Standby a partire da snapshot del punto di ripristino quando il server di monitoraggio non rileva heartbeat dal server di origine. In alternativa, è possibile attivare manualmente i computer Virtual Standby dalle snapshot del punto di ripristino in caso di errore del server di origine, di emergenza o per utilizzare un nodo di origine in modalità non in linea per la manutenzione.

Nota: Le operazioni riportate di seguito descrivono la procedura per attivare manualmente i computer Virtual Standby a partire da snapshot del punto di ripristino. Per informazioni sull'attivazione automatica di Virtual Standby a partire da snapshot del punto di ripristino, consultare la sezione Aggiunta di un'attività Virtual Standby su EC2 al piano.

Effettuare le operazioni seguenti:

1. Dalla scheda **Risorse**, accedere al gruppo nodi **Virtual Standby**.

   I nodi Virtual Standby vengono mostrati nel riquadro centrale.

2. Nel riquadro centrale, selezionare il nodo e fare clic su **Computer virtuale di standby**.

   Viene visualizzata la finestra di dialogo **Computer virtuale di standby**.

3. Nella finestra di dialogo **Computer virtuale di standby**, completare le attività seguenti:

   - Selezionare un intervallo di tempo della snapshot del punto di ripristino per l'attivazione del computer virtuale.

     Nota: Se il computer virtuale di standby non è stato ancora configurato, verrà visualizzato il collegamento seguente: "La rete del computer virtuale di standby non è configurata".

     a. Fare clic su questo collegamento per configurare la rete.

     b. Fare clic su **Salva**. Le impostazioni vengono salvate per il computer virtuale Virtual Standby.

     c. Fare clic su **Chiudi**. Viene visualizzata la finestra di dialogo **Snapshot del punto di ripristino**.

   - Fare clic su **Attiva computer virtuale**.

     Il computer virtuale viene attivato utilizzando i dati contenuti nella snapshot del punto di ripristino.

Nota: Dopo l'attivazione del computer virtuale è possibile che venga richiesto di riavviare il computer più volte. Questo comportamento si verifica perché il driver Amazon PV è installato sul computer virtuale.

Dopo l'attivazione dei computer Virtual Standby dalle snapshot del punto di ripristino, potrebbe essere necessario effettuare le seguenti attività:

- Attivare il sistema operativo di Windows in esecuzione sul computer virtuale.
- Avviare l'Agente Arcserve Unified Data Protection per Windows sul computer virtuale.
- Aggiornare Arcserve UDP con il nome host, l'indirizzo IP e le credenziali di accesso del computer virtuale.
- Assegnare il nodo a un piano.

Nota: Questa attività è richiesta solo se si desidera creare snapshot del punto di ripristino per il computer virtuale attivo.

Attivazione di computer Virtual Standby dalla console di gestione Hyper-V

Se si desidera attivare manualmente i computer virtuali Virtual Standby, si consiglia di eseguire tale procedura dalla finestra di dialogo Computer virtuale di standby del server Arcserve Unified Data Protection. Per ulteriori informazioni, consultare la sezione Attivazione di computer virtuali Virtual Standby a partire da snapshot dei punti di ripristino. Tuttavia, se si desidera attivare i computer virtuali Virtual Standby a partire dal server Hyper-V, è possibile utilizzare la Gestione Hyper-V.

Nota: La console di gestione di Hyper-V consente di accedere alle snapshot del punto di ripristino create da Virtual Standby per la protezione del nodo. Si consiglia di non eliminare le snapshot. Quando le snapshot vengono eliminate, la relazione esistente tra i dati contenuti nelle snapshot diventerà incoerente alla successiva esecuzione di un processo Virtual Standby. I dati inconsistenti non consentono la corretta attivazione dei computer virtuali Virtual Standby.

Effettuare le operazioni seguenti:

1. Accedere al server Hyper-V che esegue il monitoraggio dei nodi protetti.
2. Avviare Gestione Hyper-V seguendo la procedura seguente:
   a. Fare clic Start, Tutti i programmi, selezionare Strumenti di amministrazione e fare clic su Gestione Hyper-V.

      Viene visualizzata la Gestione Hyper-V.

   b. Dalla struttura di directory della Gestione Hyper-V, espandere la Gestione Hyper-V e fare clic sul server Hyper-V contenente il computer virtuale che si desidera attivare.

      I computer virtuali associati al server Hyper-V specificato vengono visualizzati nell'elenco di computer virtuali del riquadro centrale.
3. Eseguire una delle seguenti operazioni:
   - **Per attivare il computer virtuale mediante la snapshot più recente:** dall'elenco Computer virtuali, fare clic con il pulsante destro del mouse sul computer virtuale che si desidera attivare, quindi fare clic su Avvia nel menu di scelta rapida.
   - **Per attivare il computer virtuale mediante una snapshot meno recente:**
     a. Dall'elenco Computer virtuali, selezionare il computer virtuale che si desidera attivare.

Le snapshot associate al computer virtuale vengono visualizzate nell'elenco Snapshot.

b. Fare clic con il tasto destro del mouse sulla snapshot che si desidera utilizzare per attivare il computer virtuale, quindi fare clic su Applica del menu di scelta rapida.

   Viene visualizzata la finestra di dialogo di applicazione della snapshot.

c. Fare clic su Applica.

d. Dall'elenco Computer virtuali, fare clic con il tasto destro del mouse sul computer virtuale che si desidera attivare, quindi fare clic su Avvia del menu di scelta rapida.

   Il computer Virtual Standby è stato attivato.

Se necessario, è possibile eseguire il backup dei computer virtuali e creare snapshot del punto di ripristino dopo aver attivato il computer virtuale.

Attivazione di computer Virtual Standby dal client VMware vSphere

Se si desidera attivare manualmente i computer Virtual Standby, si consiglia di eseguire tale procedura dalla finestra di dialogo Computer virtuale di standby di Arcserve UDP. Per ulteriori informazioni, consultare la sezione Attivazione di computer virtuali Virtual Standby a partire da snapshot dei punti di ripristino. Tuttavia, se si desidera avviare i computer Virtual Standby a partire dal sistema server ESX o vCenter, è possibile utilizzare il client VMware vSphere.

Nota: Il client VMware vSphere consente di accedere alle snapshot del punto di ripristino create da Virtual Standby per la protezione del nodo. Si consiglia di non eliminare le snapshot. Quando le snapshot vengono eliminate, la relazione esistente tra i dati contenuti nelle snapshot diventerà incoerente alla successiva esecuzione di Virtual Standby. I dati incoerenti non permettono la corretta attivazione dei computer Virtual Standby.

Effettuare le operazioni seguenti:

1. Aprire il client VMware vSphere ed accedere al sistema server ESX o vCenter che esegue il monitoraggio dei nodi protetti.
2. Dalla struttura di directory, espandere il sistema server ESX o vCenter, individuare e selezionare il computer virtuale che si desidera attivare.
3. Eseguire una delle seguenti operazioni:

   Per attivare il computer virtuale mediante la snapshot più recente: Fare clic sulla scheda Introduzione, quindi selezionare l'opzione di attivazione del computer virtuale situata nella parte inferiore della schermata.

   Per attivare il computer virtuale mediante una snapshot meno recente:

   a. Fare clic sul pulsante di gestione snapshot della barra degli strumenti.

      Viene visualizzata la finestra di dialogo Snapshot per (nome del computer virtuale) contenente un elenco delle snapshot disponibili per il computer virtuale.

   b. Selezionare la snapshot dall'elenco che si desidera utilizzare per l'attivazione del computer virtuale, quindi fare clic su Vai a.

      Il computer Virtual Standby è stato attivato.

   Se necessario, è possibile eseguire il backup dei computer virtuali e creare snapshot del punto di ripristino dopo aver attivato il computer virtuale.

Protezione dei computer Virtual Standby dopo l'attivazione

Dopo l'attivazione (manuale o automatica) di un computer Virtual Standby, i processi di backup e Virtual Standby dell'Agente Arcserve Unified Data Protection per Windows non vengono eseguiti come pianificato. È necessario configurare manualmente il computer Virtual Standby per la protezione.

Effettuare le operazioni seguenti:

1. Modificare il **prefisso del nome del computer virtuale** nell'attività Virtual Standby.

   Al momento dell'attivazione dei computer Virtual Standby, l'applicazione definisce i nomi dei computer virtuali attivi come la concatenazione dell'opzione **Prefisso nome del computer virtuale** specificata nell'attività Virtual Standby e del nome host del nodo di origine.

   Esempio:

   - Prefisso nome del computer virtuale: AA_
   - Nome host del nodo di origine: Server1
   - Nome del computer Virtual Standby: AA_Server1

   Dopo l'attivazione dei computer Virtual Standby, possono verificarsi conflitti di nome se non si modifica il **prefisso del nome del computer virtuale** nell'attività Virtual Standby. Questo tipo di problemi si verifica quando i nodi di origine e i computer Virtual Standby risiedono sullo stesso hypervisor.

   Se necessario, è possibile aggiornare le altre impostazioni dell'attività Virtual Standby. In alternativa, è possibile creare una nuova attività Virtual Standby per proteggere il computer virtuale.

2. Dopo la distribuzione del piano sul computer Virtual Standby, riprendere il processo Virtual Standby.

   Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi Virtual Standby.

3. Dopo la distribuzione del piano, accedere all'Agente Arcserve Unified Data Protection per Windows sul computer Virtual Standby e pianificare un metodo di ripetizione per il processo di backup dell'Agente Arcserve Unified Data Protection per Windows.

   Per ulteriori informazioni, consultare la *Guida per l'utente dell'Agente Arcserve Uni-*

fied Data Protection per Windows.

Nota: Sospensione e riattivazione dei processi Virtual Standby.

Verifica della protezione del computer Virtual Standby

Verificare che i computer Virtual Standby siano protetti confermando la disponibilità dei punti di ripristino validi sulla destinazione di backup.

Effettuare le operazioni seguenti:

1. Accedere alla destinazione di backup e accedere alla cartella di destinazione di backup.
2. Verificare che il backup del computer Virtual Standby sia stato eseguito correttamente e che i punti di ripristino siano disponibili.

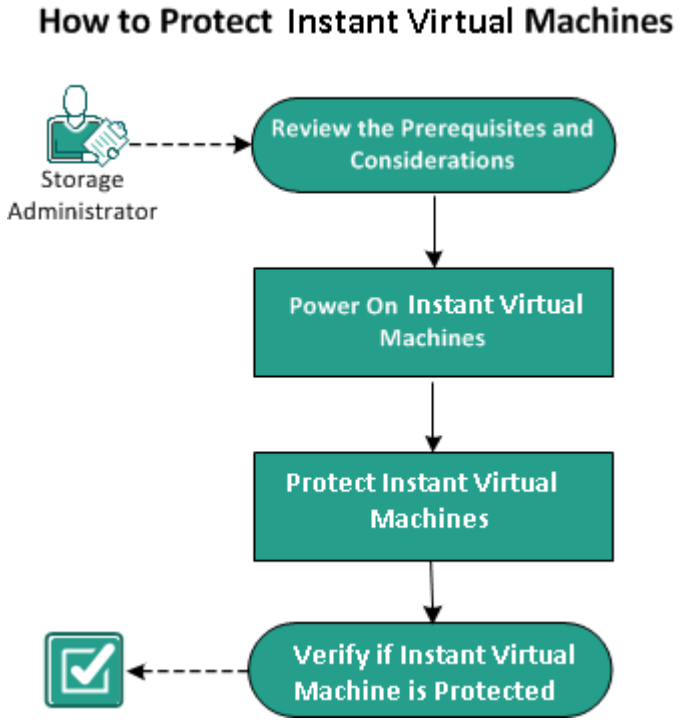
   Il computer Virtual Standby è stato verificato.

   I computer Virtual Standby verranno protetti correttamente.

Protezione dei computer virtuali istantanei

È possibile eseguire il backup dei computer virtuali istantanei ed impedire il danneggiamento dei dati. Prima di proteggere il computer, è necessario attivarlo.

Nel diagramma seguente viene illustrato il processo di protezione dei computer virtuali istantanei:



Come procedere?

- Verifica delle considerazioni e dei prerequisiti
- Avvio del computer virtuale
- Protezione dei computer virtuali istantanei
- Verifica della protezione del computer virtuale istantaneo

Verifica delle considerazioni e dei prerequisiti

Verificare il completamento delle seguenti azioni preliminari:

- Avere effettuato l'accesso alla Console.
- Aver preparato un computer virtuale istantaneo.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Attivazione di computer virtuali istantanei da un punto di ripristino

È possibile creare computer virtuali istantanei e proteggere manualmente i computer virtuali dal punto di ripristino in seguito all'attivazione dei computer.

Durante la creazione di un computer virtuale istantaneo, è possibile selezionare Avvia ora oppure Avvia più tardi. La selezione dell'opzione Avvia ora consente di avviare il computer virtuale immediatamente in seguito alla corretta creazione. In caso contrario, sarà necessario attivare il computer virtuale manualmente.

È possibile attivare computer virtuali istantanei dal punto di ripristino solo se si desidera creare un punto di ripristino per il computer virtuale attivato.

Effettuare le operazioni seguenti:

1. Dalla scheda **Risorse**, accedere al gruppo di nodi **Infrastruttura: Computer virtuali istantanei**.

   I nodi dei computer virtuali istantanei vengono visualizzati nel riquadro centrale.

2. Dal riquadro centrale, selezionare il nodo, fare clic su **Azioni**, quindi fare clic su **Attiva** dall'elenco a discesa.

   Il computer virtuale viene attivato utilizzando i dati contenuti nella snapshot del punto di ripristino.

   Nota: Dopo l'attivazione del computer virtuale è possibile che venga richiesto di riavviare il computer una o più volte. Ciò si verifica se VMware installa gli strumenti VMware o Windows Hyper-V installa i servizi di integrazione sul computer virtuale.

   Dopo l'attivazione dei computer virtuali istantanei dalle snapshot del punto di ripristino, potrebbe essere necessario effettuare le seguenti attività:

   - Attivare il sistema operativo di Windows in esecuzione sul computer virtuale.
   - Avviare l'Agente Arcserve Unified Data Protection per Windows sul computer virtuale.
   - Aggiornare Arcserve UDP con il nome host, l'indirizzo IP e le credenziali di accesso del computer virtuale.

Protezione di un computer virtuale istantaneo al momento dell'attivazione

Dopo l'attivazione (manuale o automatica) di un computer virtuale istantaneo, i processi di backup e Virtual Standby dell'Agente Arcserve Unified Data Protection per Windows non vengono eseguiti come pianificato. È necessario configurare manualmente il computer virtuale istantaneo da proteggere.

Effettuare le operazioni seguenti:

1. Aggiungere un computer virtuale istantaneo alla console.

   Nota: È possibile aggiungere un nodo specificando manualmente i dettagli del nodo oppure importando i computer virtuali dai server ESX/vCenter e Hyper-V.

   Per ulteriori informazioni, consultare la sezione Aggiunta di nodi.

2. Aggiungere una destinazione.

   Per destinazione si intende un Recovery Point Server, una cartella locale o una cartella condivisa remota.

3. Creare un piano per proteggere il nodo del computer virtuale istantaneo.

   Un piano è un gruppo di attività per la gestione del backup, della replica e della creazione di computer Virtual Standby.

   Nota: È possibile creare un piano con l'attività di backup di Windows basata sull'agente o l'attività di backup senza agente basata sull'host.

4. Eseguire processi di backup, di creazione Virtual Standby e di replica.

   Per ulteriori informazioni, consultare la *Guida per l'utente dell'agente Arcserve UDP (Windows)*.

Verifica della protezione del computer virtuale istantaneo

Verificare che il computer virtuale istantaneo sia protetto confermando la disponibilità dei punti di ripristino validi sulla destinazione di backup.

Effettuare le operazioni seguenti:

1. Accedere alla destinazione di backup e accedere alla cartella di destinazione di backup.
2. Verificare che il backup del computer virtuale istantaneo sia stato eseguito correttamente e che i punti di ripristino siano disponibili.

   Il computer virtuale istantaneo viene verificato.

   Il computer virtuale è protetto.

Replica dei dati tra archivi dati gestiti da una console UDP

Arcserve UDP consente di replicare i dati di backup da un archivio dati a un altro. Questi archivi dati vengono gestiti dalla stessa Console UDP, ma si trovano in Recovery Point Server diversi. È necessario creare un piano con due attività: backup e replica. L'attività di backup eseguirà il backup dei dati in base alla pianificazione e l'attività di replica replicherà i dati di backup nel Recovery Point Server specificato. I processi di replica vengono eseguiti in base alla pianificazione specificata nell'attività Replica. È possibile creare più attività di replica in un piano.

Se il processo di replica produce un errore per determinate ragioni (ad esempio per problemi di rete), il processo di replica non riuscito verrà ripreso prima del trasferimento a qualsiasi altra nuova sessione. Il processo di replica viene ripreso dal punto di interruzione dell'ultimo processo di replica non riuscito.

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di un piano con un'attività di
3. Aggiunta al piano di un'attività di replica
4. (Facoltativo) Esecuzione di una replica manuale
5. Verifica del piano

Verifica delle considerazioni e dei prerequisiti

Verificare se i prerequisiti seguenti sono stati completati:

- Accedere alla console.
- Installare il componente del server e creare gli archivi dati.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Creazione di un'attività di backup

Un piano include diversi tipi di attività da eseguire. In genere, un piano include attività principali seguite da un'attività secondaria. In genere, un'attività principale è un'attività di backup o di replica da un'attività di console remota. Un'attività di backup consiste nella creazione di un backup dei nodi di origine che si desidera proteggere. È possibile eseguire il backup dei dati dai computer virtuali e fisici di Windows e Linux. È quindi possibile salvare i dati di backup in un'altra posizione come precauzione aggiuntiva.

Per ulteriori informazioni su:

- Come eseguire il backup di un nodo Windows, consultare la sezione Creazione di un piano di backup di Windows.
- Come eseguire il backup di computer virtuali, consultare la sezione Creazione di un piano di backup virtuale basato su host.
- Come eseguire il backup di nodi Linux, consultare la sezione Creazione di un piano di backup di Linux.

Aggiunta al piano di un'attività di replica

Creare un'attività di replica per proteggere ulteriormente i dati copiando i dati di backup da un Recovery Point Server a un altro. È possibile copiare i dati di backup da un archivio dati in un altro archivio dati nello stesso Recovery Point Server. La destinazione della replica deve essere un archivio dati nel Recovery Point Server. È possibile creare più attività di replica per eseguire più repliche.

Note:

- **Per il processo di unione:** quando è configurata un'attività di replica e si esegue un processo di unione su richiesta dall'archivio dati di origine, il processo non verifica se le sessioni sono state già replicate. Di conseguenza, le sessioni unite non possono essere replicate nell'archivio dati di destinazione e si andranno a replicare ulteriori dati. Ad esempio, si supponga di avere cinque sessioni: s1, s2, s3, s4 e s5 rispettivamente. s1 e s2 vengono replicate. A questo punto, si esegue un processo di unione on-demand sul lato di origine e si conservano due sessioni, s4 ed s5. s4 è una sessione completa. Pertanto, all'avvio del successivo processo di replica, si dovrà replicare una sessione completa.
- **Per il processo di eliminazione:** quando è configurata un'attività di replica e si esegue un processo di eliminazione nell'archivio dati di destinazione, il successivo processo di replica esegue la replica di tutte le sessioni nell'archivio dati di destinazione.
- Non è possibile eseguire la replica da un archivio dati abilitato per la deduplicazione a un archivio dati non abilitato per la deduplicazione.
- Non è possibile eseguire la replica da un archivio dati abilitato per la crittografia a un archivio dati non abilitato per la crittografia.

Effettuare le operazioni seguenti:

1. Fare clic su **Aggiungi un'attività** dal riquadro sinistro.

   Viene aggiunta una nuova attività al riquadro sinistro.

2. Dal menu a discesa **Tipo di attività**, selezionare **Replica**.

   Viene aggiunta l'attività di replica. Non è necessario configurare la scheda **Origine** nell'attività di replica perché rispecchia la destinazione di backup dall'attività di backup.

   Nota: non è possibile replicare un'attività senza l'attività principale, ad esempio Backup su Recovery Point Server.

3. Fare clic sulla scheda **Destinazione** e immettere i dettagli relativi al Recovery Point Server, quindi immettere nuovamente i dettagli di pianificazione.



Recovery Point Server

Selezionare il Recovery Point Server dall'elenco.

Archivio dati

Selezionare l'archivio dati dall'elenco.

Avvia nuovo tentativo

Specificare il tempo (in minuti) per il riavvio del processo di replica in seguito all'errore del processo. Ad esempio, se si specificano 10 minuti, il processo di replica verrà riavviato 10 minuti dopo l'errore.

Limite: da 1 a 60

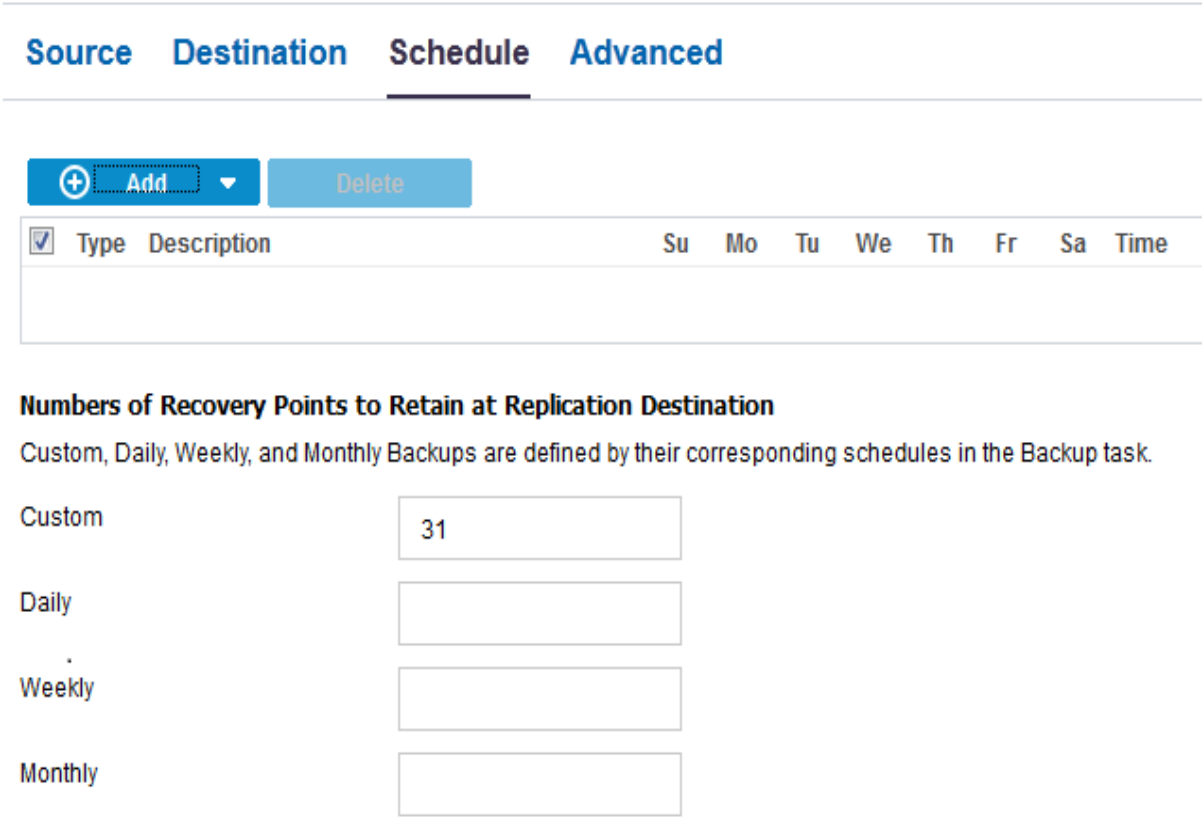
Riprova

Specificare il numero di volte in cui si desidera avviare il processo di replica in seguito a un errore del processo. Il processo di replica verrà eseguito fino a quando il processo avrà esito positivo, oppure fino al raggiungimento del limite.

Limite: da 1 a 99

4. Fare clic sulla scheda **Pianificazione** e aggiungere **Pianificazione processo di replica**, **Pianificazione del limite delle risorse di replica**, **Pianificazione di unione** e **Impostazioni di memorizzazione**.

   Nota: La quota del limite delle risorse di replica viene divisa in media da tutti i processi di replica avviati da tutti i nodi di un piano corrente.



5. Fare clic sulla scheda **Avanzate** e immettere i dettagli.
6. Fare clic su **Salvare le modifiche** o **Aggiungi un'attività**.

   Se si è aggiunta un'attività, è possibile creare un'altra attività di replica per eseguire più livelli di replica. È possibile aggiungere al piano più attività di replica.

   Se si salvano le modifiche, il piano viene salvato e l'attività di replica viene distribuita nella destinazione di replica.

   L'attività di replica è stata creata.

   Il piano di replica è stato creato correttamente e distribuito in automatico.

(Facoltativo) Esecuzione di una replica manuale

Per eseguire manualmente un processo di replica, è necessario disporre di almeno un set di dati di backup eseguiti correttamente. Se la pianificazione di replica non è stata impostata, il processo di replica verrà eseguito immediatamente in seguito al processo di backup. In caso contrario, dipenderà dalle impostazioni della pianificazione di replica.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Se sono stati aggiunti, questi piani verranno mostrati nel riquadro centrale.
3. Selezionare i nodi di cui si desidera eseguire il backup e ai quali è stato assegnato un piano.
4. Nel riquadro centrale, fare clic su **Azioni**, **Replica ora**.

   Viene visualizzata la finestra di dialogo **Replica nodo**.
5. Selezionare il server RPS di origine e di destinazione per il processo.
6. Fare clic su **OK**.

   Il processo di replica viene eseguito.

   La replica manuale è stata eseguita correttamente.

Verifica del piano

Per verificare la funzionalità di replica, confermare di avere creato correttamente il piano di replica. Dopo avere verificato che il piano è stato creato correttamente, verificare se il processo di backup sia in esecuzione in base alla pianificazione. Dopo la corretta conclusione del processo di backup, viene eseguito il processo di replica. È possibile verificare lo stato dei processi di backup e replica dalla scheda **Processi**.

Effettuare le operazioni seguenti: per la verifica dei piani

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Effettuare le operazioni seguenti: per la verifica dei processi di replica

1. Fare clic sulla scheda **Jobs** (Processi).
2. Dal riquadro sinistro, fare clic su **Tutti i Processi**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare la corretta esecuzione del processo di backup e del processo di replica.

Replica dei dati tra archivi dati gestiti da console UDP diverse

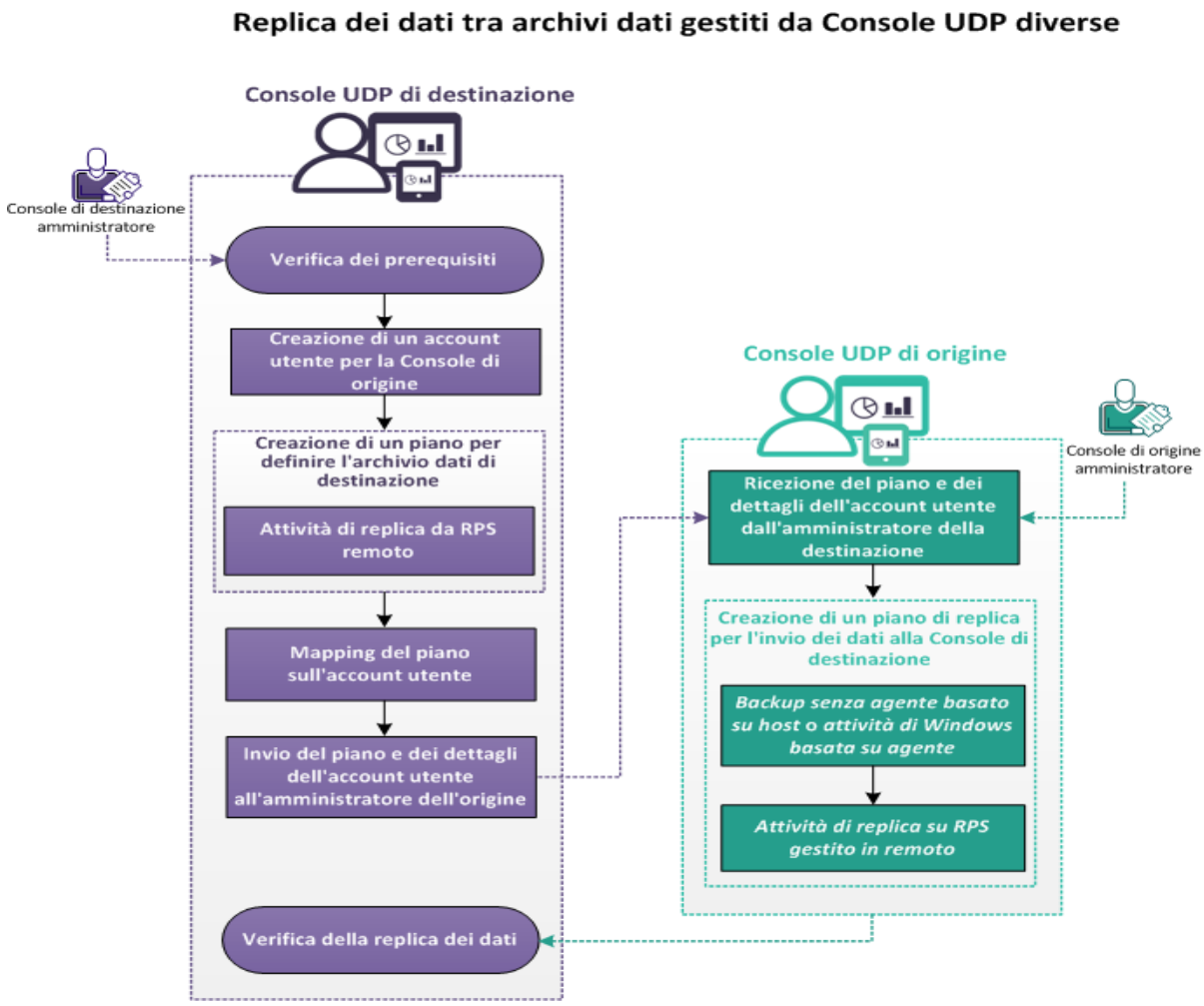
Ai fini della protezione dei dati, potrebbe essere necessario eseguire la replica dei dati di backup su un altro Recovery Point Server gestito da una console Arcserve UDP diversa. Ad esempio, è possibile eseguire la replica dei dati su un provider di servizi che offre servizi di replica a più clienti. In questo esempio, la replica dei dati viene eseguita da un archivio dati di origine (sulla console di origine) a un archivio dati di destinazione (sulla console di destinazione).

L'amministratore della console di destinazione, crea un nome utente univoco, una password e un piano per la console di origine. Il piano definisce l'archivio dati di destinazione. Il nome utente e la password consentono all'amministratore dell'origine di connettersi al server dell'utente ed eseguire la replica dei dati.

L'amministratore della console di origine crea un piano per la replica dei dati sull'archivio dati di destinazione. Durante il processo di creazione del piano, l'utente deve effettuare la connessione al server di destinazione e selezionare il piano assegnato all'utente dall'amministratore della destinazione.

Nota: come procedura ottimale, si consiglia di configurare i parametri multistream. Per ulteriori informazioni, consultare la sezione Configurazione dei parametri multistream.

Il diagramma seguente mostra il processo di replica dei dati su un altro archivio dati gestito da una console differente:



Come procedere?

1. Verifica dei prerequisiti
2. Creazione di un account utente per la console di origine
3. Creazione di un piano per definire l'archivio dati di destinazione
4. Mapping del piano sull'account utente
5. Invio del piano e dei dettagli dell'account utente all'amministratore dell'origine

6. Ricezione del piano e dei dettagli dell'account utente dall'amministratore della destinazione
7. Creazione di un piano di replica per l'invio dei dati alla console di destinazione
8. Verifica della replica dei dati

Verifica dei prerequisiti

Verificare i prerequisiti seguenti prima di eseguire la replica dei dati:

- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Amministratore - Console di destinazione

- Verificare che Arcserve UDP sia stato installato sul server di destinazione.
- Verificare di disporre dei privilegi completi per la creazione di account utenti Windows sul server di destinazione.
- Verificare di aver attivato la casella di controllo **Consenti il recupero dei punti di ripristino** nelle Impostazioni avanzate durante la creazione della replica da un piano RPS gestito in remoto.

  Nota: se non si attiva la casella di controllo **Consenti il recupero dei punti di ripristino** e si avvia il processo di replica inversa per la console remota, viene richiesto di attivare il flag Consenti il recupero dei punti di ripristino per la replica inversa.

Amministratore - Console di origine UDP

- Verificare che Arcserve UDP sia stato installato sul server di origine.
- Verificare che sia stato completato almeno un backup completo su un archivio dati.

Creazione di un account utente per la Console di origine

Amministratore della destinazione

Per identificare e gestire i dati replicati sul server di destinazione, creare un account utente di Windows. In caso di gestione di più di una Console di origine, creare un account utente per ciascuna Console di origine.

L'amministratore della Console di origine utilizza i dettagli di tale account per la connessione al server di destinazione.

Per creare un account utente in un sistema operativo Windows, utilizzare la sezione di Account utente del Pannello di controllo di Windows. Per ulteriori informazioni sulla creazione di account utenti in Microsoft Windows, consultare la documentazione di Microsoft.

Creazione di un piano per definire l'archivio dati di destinazione

Amministratore della destinazione

La replica dei dati di origine viene eseguita sul archivio dati di destinazione. Per definire l'archivio dati di destinazione, creare un piano. Il piano consente di definire l'archivio dati di destinazione e la pianificazione di unione.

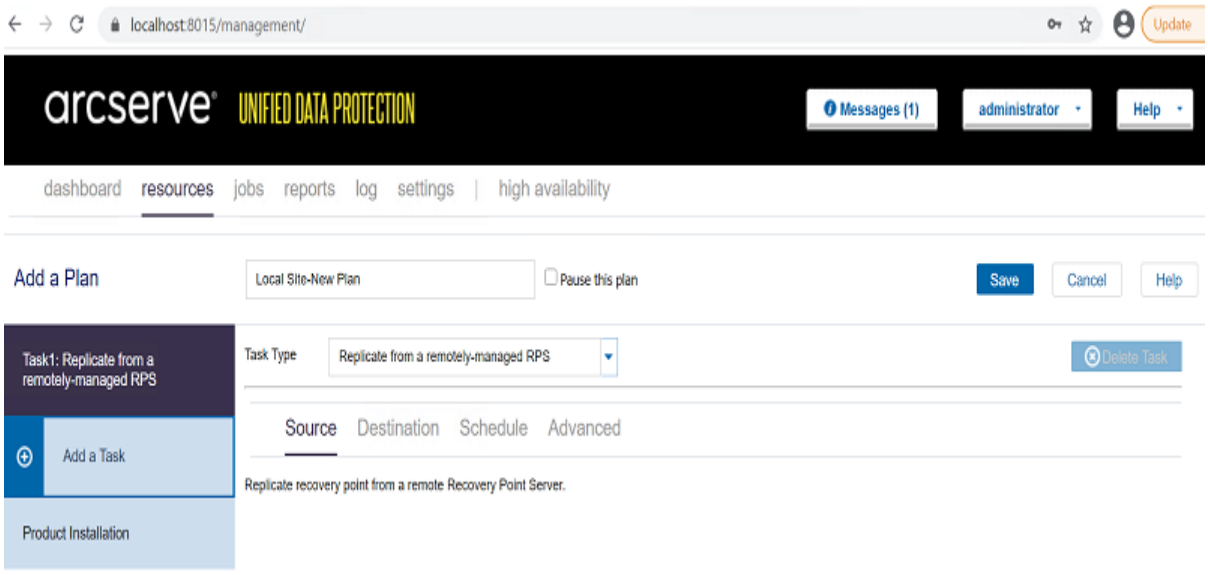
Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati aggiunti piani, questi verranno mostrati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina **Aggiungi un piano**.
4. Immettere un nome per il piano nel campo **Nuovo piano**.
5. Dall'elenco a discesa **Tipo di attività**, selezionare **Replica da server RPS gestito in remoto**.

   Viene visualizzata la scheda **Origine.** Non è possibile specificare alcun dettaglio nella scheda Origine. I dettagli della Console di origine vengono specificati dall'amministratore.



6. Fare clic sulla scheda **Destinazione** e specificare il Recovery Point Server e l'archivio dati.

7. (Facoltativo) Selezionare la casella di controllo **Il server si trova dietro il router NAT** e fornire l'indirizzo del server e il numero di porta.
8. Fare clic sulla scheda **Pianificazione**.

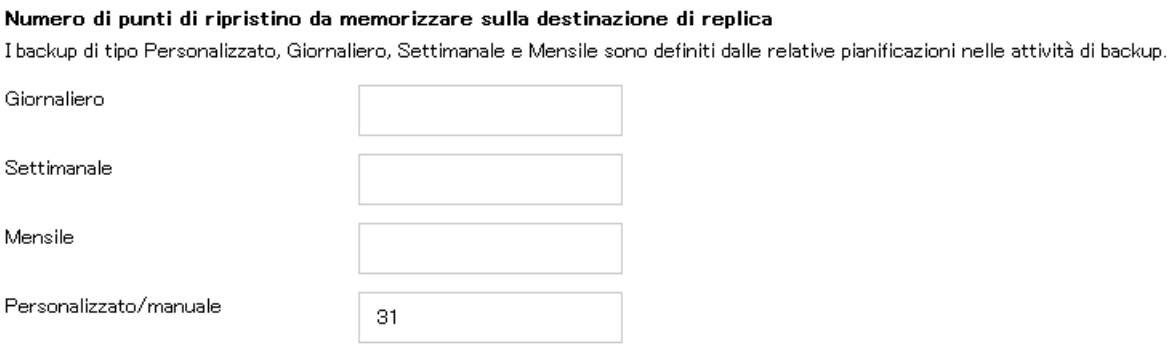


9. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di unione di replica**.

   La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.
10. Immettere la pianificazione di unione.

    Nota: per ulteriori informazioni sulle pianificazioni, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.
11. Fare clic su **Salva**.

    La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.
12. Immettere i dettagli di memorizzazione dei punti di ripristino.



13. Fare clic sulla scheda **Avanzate** e fornire i dettagli seguenti.

    Configurazione recupero

    Consente di eseguire il recupero dei punti di ripristino. Per attivare l'operazione, selezionare la casella di controllo **Consenti il recupero dei punti di ripristino**.

    Abilitazione degli avvisi di posta elettronica

    Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere mediante posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy.

Avvisi di processo

Consente di selezionare i tipi di avviso del processo che si desidera ricevere.

14. Fare clic su **Salva**.

Le modifiche vengono salvate e il piano viene creato.

Il piano di replica è stato creato correttamente. È inoltre possibile aggiungere al piano attività di Replica, Replica su server RPS gestito in remoto e Virtual Standby.

Mapping del piano sull'account utente

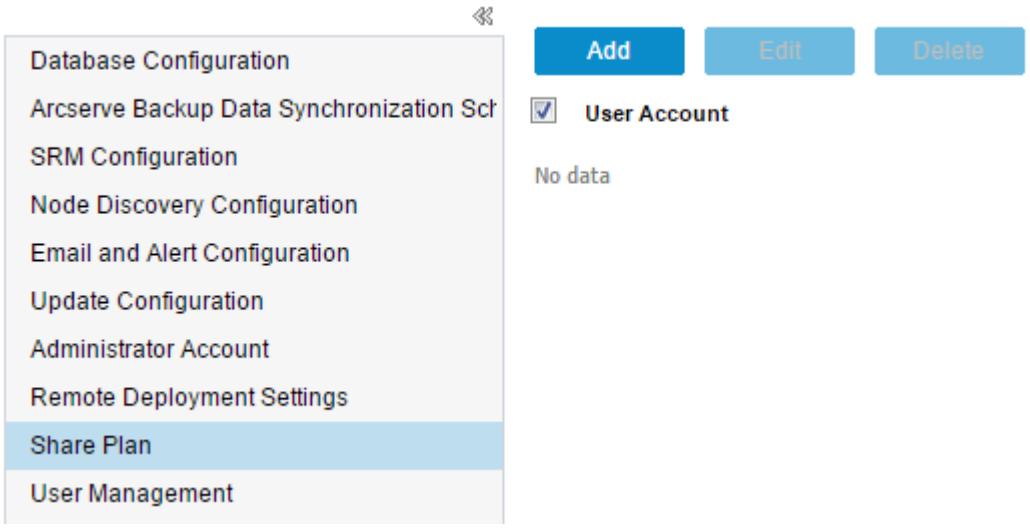
Amministratore della destinazione

L'account utente e il piano per la Console di origine sono stati creati precedentemente. Per identificare e gestire i dati replicati, assegnare il piano all'account utente.

Nota: è possibile assegnare più di un piano a un account utente. Tuttavia, due account diversi non possono condividere lo stesso piano. Si consiglia di assegnare un solo piano a ciascun account utente in modo da poter identificare e gestire facilmente i dati replicati.

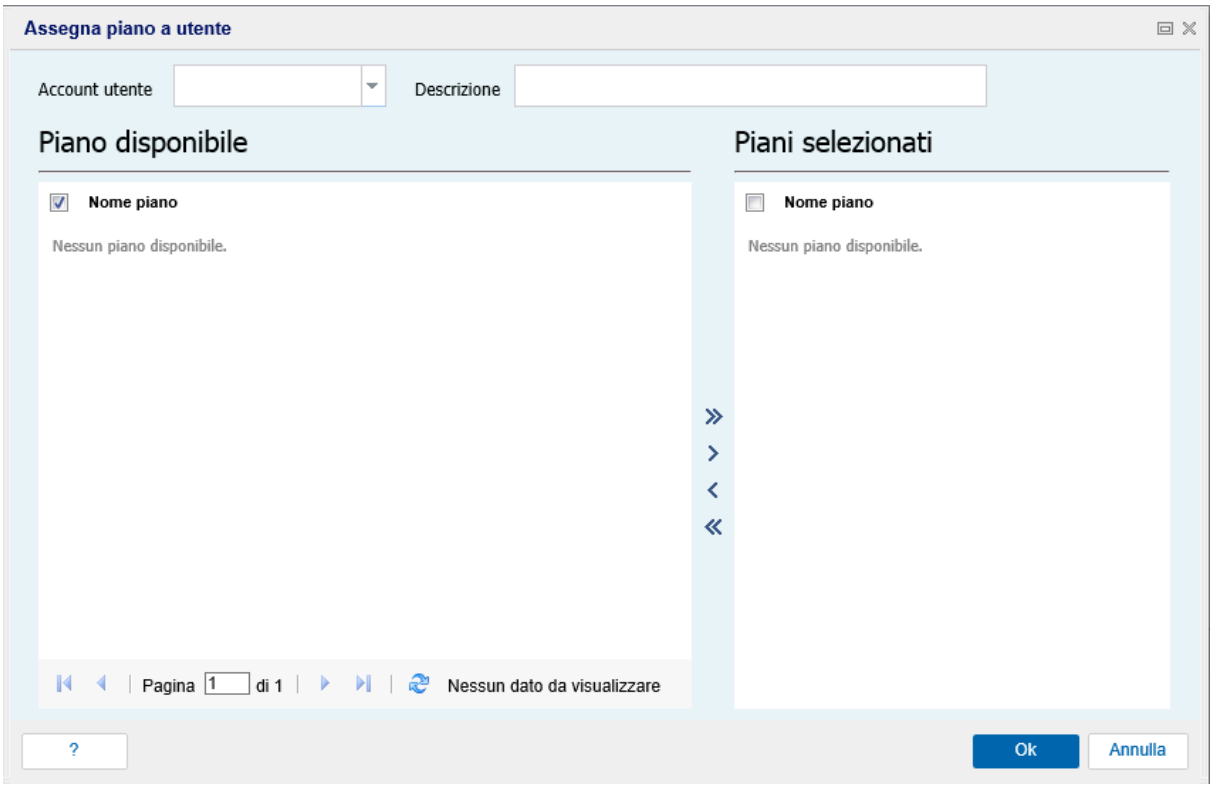
Effettuare le operazioni seguenti:

1. Dalla console, fare clic sulla scheda **Impostazioni**.
2. Dal riquadro sinistro, fare clic su **Condividi piano**.



3. Dal riquadro centrale, fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo **Assegna piano a utente**.



4. Selezionare l'**account utente**.
5. Selezionare un piano dalla colonna **Piano disponibile**.

   Nota: Se un piano è già stato aggiunto a un nome utente, tale piano non viene visualizzato nella colonna **Piano disponibile**.
6. Fare clic su **Aggiungi tutti i piani** o **Aggiungi i piani selezionati** per aggiungere i piani nella colonna **Piani selezionati**.
7. Fare clic su **OK**.

   La finestra di dialogo **Assegna piano a utente** viene chiusa. Il nome utente e i piani associati vengono visualizzati nella pagina **Condividi piano**.

   Viene eseguito il mapping dell'account utente sul piano creato la Console di origine.

   È possibile utilizzare l'opzione **Modifica** per modificare la configurazione utente oppure l'opzione **Elimina** per rimuovere l'utente dall'elenco.

Invio del piano e dei dettagli dell'account utente all'amministratore dell'origine

Amministratore della destinazione

Dopo aver associato il piano all'account utente, inviare il piano e i dettagli dell'account utente all'amministratore dell'origine. L'amministratore dell'origine utilizza questi dettagli per effettuare la connessione alla Console di destinazione.

L'amministratore della destinazione ha completato tutte le attività corrispondenti.

Ricezione del piano e dei dettagli dell'account utente dall'amministratore della destinazione

Amministratore dell'origine

Per eseguire la replica dei dati sulla Console di origine, è necessario che l'amministratore della destinazione fornisca i dettagli utente, il piano e il server di destinazione. Tali dettagli vengono forniti dall'amministratore della destinazione. Verificare i dettagli e richiedere eventuali chiarimenti all'amministratore della destinazione prima di procedere alla creazione dei piani di replica.

Creazione di un piano di replica per l'invio dei dati alla Console di destinazione

Amministratore dell'origine

Per eseguire la replica dei dati di backup sul Recovery Point Server di destinazione gestito da una Console differente, creare un piano di replica. Il piano di replica include un'attività di backup e un'attività di replica gestita in remoto. Nell'attività di replica, specificare il server remoto e i dettagli del piano, quindi connettersi al server remoto. Se la connessione viene eseguita correttamente, selezionare il piano creato appositamente dall'amministratore della destinazione.

Effettuare le operazioni seguenti:

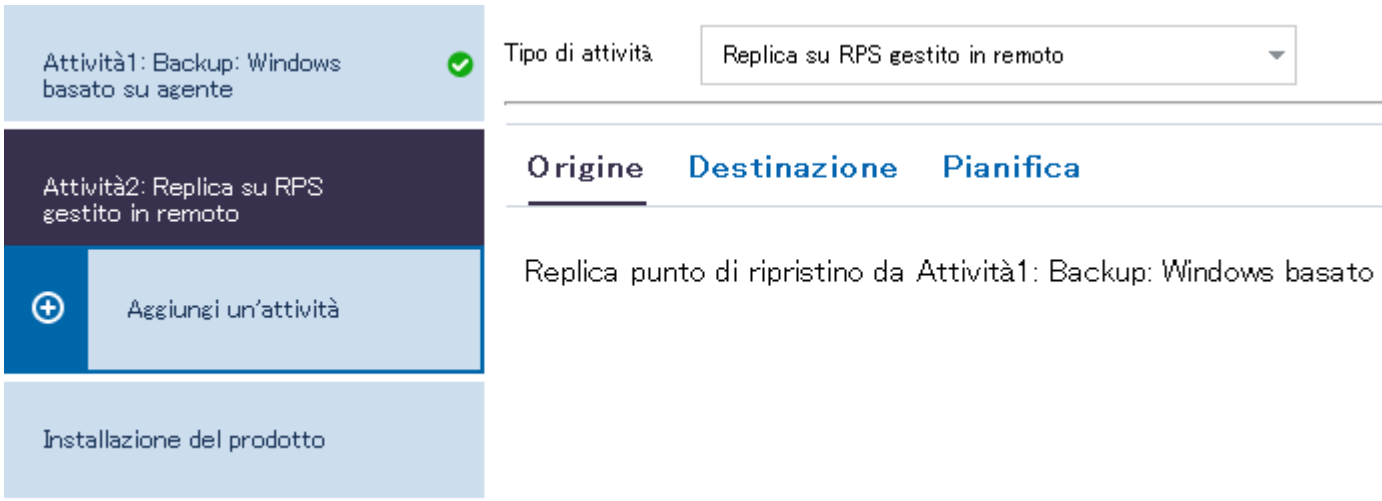
1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.
3. Fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina **Aggiungi un piano**.
4. Immettere il nome del piano, selezionare una delle attività di backup seguenti e creare l'attività:
   - **Backup: Windows basato su Agente**
   - **Backup: senza Agente basato su host**
   - **Backup: Linux basato su agente**

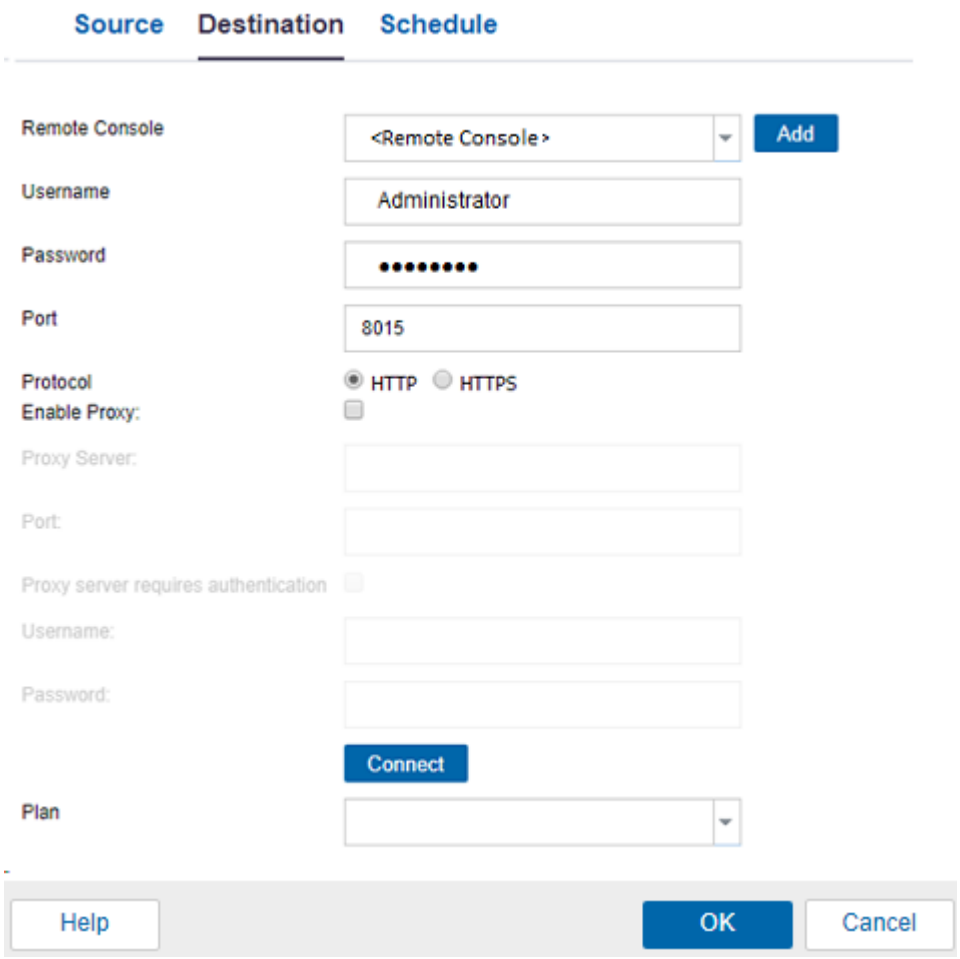
     Nota: Per ulteriori informazioni sulla creazione di un'attività di backup, consultare gli argomenti seguenti:
     - Creazione di un piano di backup di Windows
     - Creazione di un piano di backup del computer virtuale basato su host
     - Creazione di un piano di backup di Linux
5. Nel riquadro a sinistra, fare clic su **Aggiungi un'attività**.

   Viene aggiunta una nuova attività al riquadro sinistro.
6. Dall'elenco a discesa **Tipo di attività**, selezionare **Replica su RPS gestito in remoto**.

   L'attività Replica viene aggiunta e viene visualizzata la pagina **Origine.** Nella scheda **Origine**, la destinazione dell'attività di backup (ad esempio, Backup: Windows basato su Agente) corrisponde all'origine dell'attività **Replica su RPS gestito in remoto**.



7. Fare clic sulla scheda **Destinazione** e immettere i seguenti dettagli.



Console remota

Selezionare un account di console remota dall'elenco a discesa o aggiungere un nuovo account di console remota facendo clic sul pulsante **Aggiungi**.

Per ulteriori informazioni, fare clic su Aggiungi console remota.

Nome utente

Specificare il nome utente creato dall'amministratore di destinazione. Il nome utente viene fornito dall'amministratore della destinazione.

Password

Specificare la password creata dall'amministratore della destinazione. La password viene fornita dall'amministratore della destinazione.

Porta

Specificare il numero di porta della Console di destinazione. Il numero di porta della Console di destinazione viene fornito dall'amministratore della destinazione.

Protocollo

Specificare il protocollo utilizzato dall'amministratore della destinazione per la connessione alla Console di destinazione.

Abilita proxy

Selezionare la casella di controllo per abilitare la selezione del server proxy.

Server proxy

Specifica l'indirizzo del server proxy.

Porta

Specifica del numero della porta del server di backup.

Il server proxy richiede l'autenticazione

Selezionare la casella di controllo per abilitare i campi di autenticazione per il server proxy.

Nome utente

Specificare il nome utente per la connessione al server proxy.

Password

Specificare la password per autenticare la connessione al server proxy.

Connetti

Verifica la connessione tra la Console di origine e la Console di destinazione. Se la connessione viene stabilita correttamente, il nome del piano viene visualizzato nel campo **Piano.** Il nome del piano viene assegnato alla Console dall'amministratore della destinazione.

Piano

Specificare il piano creato dall'amministratore della destinazione per l'utente. Se l'elenco contiene più piani, contattare l'amministratore della destinazione per conoscere il piano corretto.

Avvia nuovo tentativo

In caso di errore, ripete il processo di replica dopo l'intervallo di tempo specificato. Immettere un valore compreso tra 1 e 60 e il tempo viene definito in minuti.

Riprova

Specificare il numero di nuovi tentativi che si desidera eseguire in caso di un errore di processo. Una volta superato il numero di tentativi, il processo di replica viene eseguito solo all'ora pianificata successiva. Immettere un valore compreso tra 1 e 99.

8. Fare clic sulla scheda **Pianificazione** e fornire la pianificazione del processo di replica e la pianificazione del limite di velocità di replica.

   Pianificazione processo di replica

   Specificare la data e l'ora di avvio dei processi di replica. È possibile modificare o eliminare una pianificazione del processo di replica.

   Pianificazione del limite delle risorse di replica

   Specificare la velocità massima (Mbps) di esecuzione della replica. È possibile limitare la velocità di replica per ridurre l'utilizzo della CPU o della rete. Nel caso di un processo di replica, la scheda **Jobs** (Processi) mostra la velocità media di lettura e scrittura del processo in corso e il valore limite configurato.

   È possibile modificare o eliminare una pianificazione del processo del limite di velocità.

9. Fare clic su **Salva**.

   Il piano viene salvato ed eseguito in base alla pianificazione.

   Il piano di replica è stato creato correttamente e distribuito in automatico. Durante l'esecuzione del piano, la replica dei dati viene eseguita dalla posizione di origine alla posizione di destinazione di dati, su una rete.

   Nota: una volta completato il processo di replica, i dettagli del nodo replicato vengono aggiunti automaticamente alla Console di destinazione.

   La replica dei dati tra due archivi dati gestiti da Console UPD diverse è stata eseguita correttamente.

Verifica della replica dei dati

Amministratore della destinazione

Una volta completato il processo di replica verificare che sia stato eseguito correttamente.

Effettuare le operazioni seguenti:

1. Dalla Console di destinazione, accedere all'archivio dati di destinazione del Recovery Point Server.
2. Verificare che le dimensioni dei dati replicati corrispondano a quelle dei dati di origine.

   La replica dei dati tra due archivi dati gestiti da Console UDP diverse è stata eseguita correttamente.

Esecuzione di una replica di dati non in linea utilizzando JumpStart RPS

La replica di archivi dati di grandi dimensioni su un Recovery Point Server diverso (gestito da una Console UDP differente) eseguita su rete (LAN, WAN, Internet) richiede tempi lunghi. Per eseguire rapidamente la replica di un archivio dati di grandi dimensioni, Arcserve UDP fornisce un metodo di replica di dati non in linea. Questo metodo è denominato JumpStart RPS.

Jumpstart RPS è un metodo di replica non in linea che utilizza una periferica di archiviazione esterna, ad esempio un'unità di unità di memoria flash USB, per la replica di un archivio dati. La replica viene eseguita tra due archivi dati gestiti da Console UDP diverse. Ad esempio, un provider di servizi offre i propri servizi di replica a più clienti. Il cliente esegue la replica dei dati su una periferica di archiviazione e invia la periferica di archiviazione al provider dei servizi. Il provider dei servizi esegue la replica dei dati dalla periferica di archiviazione al server di destinazione. È necessario che Arcserve UDP sia installato presso il provider di servizi e presso il cliente.

La replica non in linea richiede che entrambi gli amministratori (dell'origine e della destinazione) completino le operazioni seguenti nella rispettiva posizione.

Importante. Se è in corso la replica da una cartella condivisa in un archivio dati selezionato sul Recovery Point Server, consultare la sezione Migrazione dei punti di ripristino di Arcserve r16.5 ad Arcserve UDP.

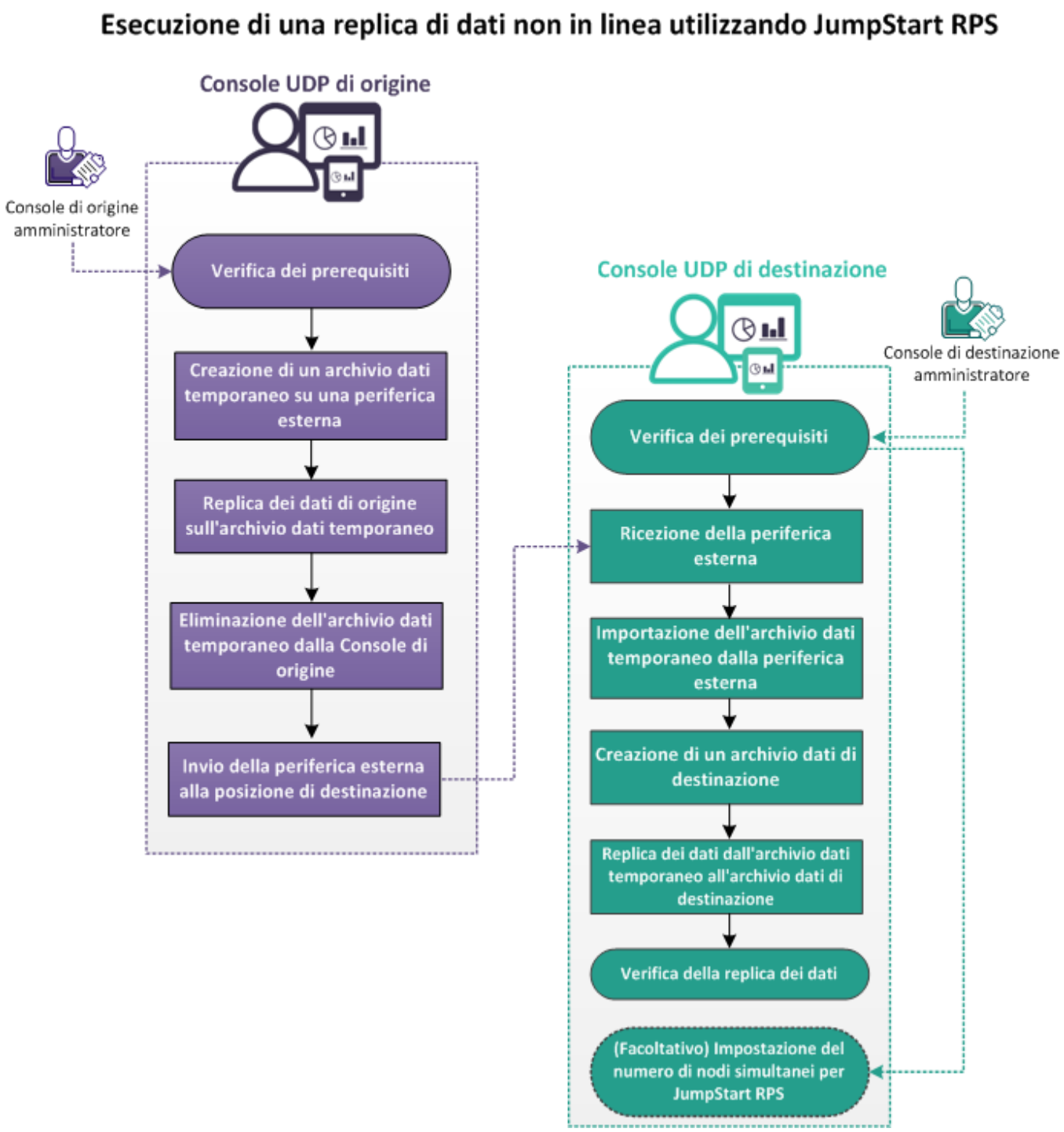
Amministratore dell'origine

1. Replica dell'archivio dati di origine su una periferica esterna.
2. Invio della periferica esterna alla posizione di destinazione.

Amministratore della destinazione

1. Ricezione della periferica esterna.
2. Replica dell'archivio dati di origine dalla periferica esterna al Recovery Point Server.

Il diagramma seguente descrive il processo di replica non in linea dei dati mediante Jumpstart RPS.



Come procedere?

- Verifica dei prerequisiti
- Creazione di un archivio dati temporaneo su una periferica esterna
- Replica dei dati di origine sull'archivio dati temporaneo
- Eliminazione dell'archivio dati temporaneo dalla Console di origine

- Invio della periferica esterna alla posizione di destinazione
- Ricezione della periferica esterna
- Importazione dei dati temporanei dalla periferica esterna
- Creazione di un archivio dati di destinazione
- Replica dei dati dall'archivio dati temporaneo all'archivio dati di destinazione
- Verifica della replica dei dati
- (Facoltativo) Impostazione del numero di nodi simultanei per JumpStart RPS

Verifica dei prerequisiti

Prima di eseguire la replica non in linea dei dati, verificare i seguenti prerequisiti:

- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.
- Se l'origine è un archivio dati con deduplicazione abilitata, anche la destinazione deve essere un archivio dati con deduplicazione abilitata.
- Se l'origine è un archivio dati con crittografia abilitata, anche la destinazione dovrà essere un archivio dati con crittografia abilitata.

Amministratore - Console di origine

- Verificare che l'archivio dati di origine sia stato creato.
- Verificare che sia stato completato almeno un backup completo su un archivio dati.
- (Facoltativo) Verificare che il numero di nodi simultanei per JumpStart RPS sia stato configurato. Per ulteriori informazioni sulla configurazione del numero di nodi simultanei, consultare la sezione Impostazione del numero di nodi simultanei per JumpStart RPS.

Amministratore - Console di destinazione

- Verificare di disporre dello spazio disponibile necessario per la replica.
- Verificare di disporre dei privilegi richiesti per la periferica esterna.

Creazione di un archivio dati temporaneo su una periferica esterna

Amministratore dell'origine

Per importare i dati da un archivio dati esistente a una periferica esterna, creare un archivio dati temporaneo sulla periferica esterna. Per creare l'archivio dati temporaneo, connettere la periferica esterna al computer.

Effettuare le operazioni seguenti:

1. Accedere alla Console UDP.
2. Accedere a **Destinazioni**, **Recovery Point Server**.
3. Selezionare il Recovery Point Server.
4. Fare clic con il tasto destro del mouse e selezionare **Aggiungi archivio dati**.
5. Immettere i dettagli nella pagina **Aggiungi archivio dati**.

   Nota: Verificare che le cartelle di destinazione di backup siano sulla periferica esterna.
6. Salvare l'archivio dati.

   L'archivio dati temporaneo viene creato sulla periferica esterna.

Replica dei dati di origine sull'archivio dati temporaneo

Amministratore dell'origine

Dopo avere creato l'archivio dati temporaneo sulla periferica esterna, è possibile replicare i dati di origine sulla periferica esterna mediante Jumpstart RPS.

Nota: Prima di avviare il processo Jumpstart RPS, sospendere il piano correlato. La sospensione del piano garantisce che nessun processo di replica pianificato venga avviato durante l'esecuzione del processo Jumpstart.

Effettuare le operazioni seguenti:

1. Fare clic su **Azioni**, quindi su **JumpStart RPS**.

   Viene visualizzata la **Procedura di installazione guidata di RPS.**

2. Selezionare se eseguire la migrazione dallo stesso archivio dati o da una posizione condivisa.
3. Selezionare il Recovery Point Server di origine, l'archivio dati di origine e il piano.

   Vengono visualizzati i nodi che appartengono al piano.

4. Selezionare i nodi di cui si desidera eseguire la migrazione.
5. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Selezione dell'archivio dati di destinazione.** Se l'archivio dati di origine è crittografato, nell'elenco a discesa vengono mostrati soltanto gli archivi dati crittografati.

6. Selezionare l'archivio dati di destinazione. L'archivio dati di destinazione deve trovarsi sulla periferica esterna.
7. Fare clic su **Fine**.

   La sezione **Eventi recenti** del riquadro di destra mostra il progresso del processo di replica.

   Una volta completato il processo, la replica dei dati è disponibile sull'archivio dati temporaneo. È possibile verificare la dimensione di entrambi gli archivi dati nella pagina **Destinazioni: Recovery Point Server**.

Eliminazione dell'archivio dati temporaneo dalla Console di origine

Amministratore dell'origine

Ai fini dell'integrità dei dati sulla periferica esterna, eliminare l'archivio dati temporaneo della Console UDP prima di rimuovere la periferica esterna.

Nota: L'eliminazione dell'archivio dati temporaneo dalla console UDP di origine non elimina i file dell'archivio dati dalla periferica esterna.

Effettuare le operazioni seguenti:

1. Fare clic con il tasto destro del mouse sull'archivio dati temporaneo e fare clic su **Arresta**.

   L'archivio dati viene arrestato.

2. Fare clic con il tasto destro del mouse sull'archivio dati temporaneo e fare clic su **Elimina**.

   Viene visualizzata una finestra di dialogo di conferma.

3. Fare clic su **Sì**.

   L'archivio dati è stato eliminato.

   Ora è possibile rimuovere la periferica esterna dal computer.

Invio della periferica esterna alla posizione di destinazione

Amministratore dell'origine

Dopo avere rimosso la periferica esterna, inviare la periferica alla posizione di destinazione.

Ricezione della periferica esterna

Amministratore della destinazione

L'amministratore riceve la periferica esterna contenente i dati di origine e la connette al server di destinazione.

Importazione dell'archivio dati temporaneo dalla periferica esterna

Amministratore della destinazione

Prima di eseguire la replica dei dati di origine sull'archivio dati di destinazione, importare l'archivio dati temporaneo sul Recovery Point Server di destinazione.

Effettuare le operazioni seguenti:

1. Accedere alla scheda **Risorse** e selezionare il Recovery Point Server in cui si desidera importare l'archivio dati.
2. Fare clic con il tasto destro del mouse sul Recovery Point Server e selezionare **Importa archivio dati**.

   Viene visualizzata la schermata **Importa archivio dati**.
3. Selezionare la cartella di destinazione di backup dalla periferica esterna.
4. Fare clic su **Avanti**.

   Vengono visualizzati i dettagli dell'archivio dati temporaneo. Se necessario, modificare il percorso di dati, indice e hash.
5. Fare clic su **Salva**.

   L'archivio dati è stato importato ed è possibile visualizzare l'archivio dati sulla Console di destinazione.

Creazione di un archivio dati di destinazione

Amministratore della destinazione

Per eseguire la replica dei dati dall'archivio dati temporaneo, creare un archivio dati di destinazione. Per ulteriori informazioni, consultare la sezione Aggiunta di un Archivio dati.

Nota: è possibile utilizzare un archivio dati esistente come archivio dati di destinazione.

Replica dei dati dall'archivio dati temporaneo all'archivio dati di destinazione

Dopo avere creato l'archivio dati di destinazione, replicare i dati dall'archivio dati temporaneo sull'archivio dati di destinazione. Una volta completata la replica sull'archivio dati di destinazione, è possibile eliminare l'archivio dati temporaneo.

Effettuare le operazioni seguenti:

1. Fare clic su **Azioni**, quindi su **JumpStart RPS**.

   Viene visualizzata la **Procedura di installazione guidata di RPS.**

2. Selezionare il Recovery Point Server di origine e l'archivio dati di origine. Il piano deve essere selezionato qui.

   Vengono visualizzati i nodi.

3. Selezionare i nodi di cui si desidera eseguire la migrazione.

4. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Selezione dell'archivio dati di destinazione.** Se l'archivio dati di origine è crittografato, nell'elenco a discesa vengono mostrati soltanto gli archivi dati crittografati.

5. Selezionare l'archivio dati di destinazione. L'archivio dati di destinazione deve trovarsi sulla periferica esterna.

6. Fare clic su **Fine**.

   La sezione **Eventi recenti** del riquadro di destra mostra il progresso del processo di replica.

   Una volta completato il processo, la replica dei dati è disponibile sull'archivio dati temporaneo. È possibile verificare la dimensione di entrambi gli archivi dati nella pagina **Destinazioni: Recovery Point Server**.

   La replica dei dati viene eseguita sul archivio dati di destinazione.

Verifica della replica dei dati

Amministratore della destinazione

Una volta completato il processo di replica verificare che sia stato eseguito correttamente.

Effettuare le operazioni seguenti:

1. Dalla Console di destinazione, accedere all'archivio dati di destinazione del Recovery Point Server.
2. Verificare che le dimensioni dei dati replicati corrispondano a quelle dei dati di origine.

   La replica dei dati tra due archivi dati gestiti da Console UDP diverse è stata eseguita correttamente.

(Facoltativo) Impostazione del numero di nodi simultanei per JumpStart RPS

Amministratore dell'origine

Quando si avvia un processo Jumpstart RPS, per impostazione predefinita il valore del numero di nodi simultanei per l'archivio dati corrisponde a 4. Per specificare il numero di nodi simultanei, creare la chiave e aggiungere manualmente un valore DWORD per impostare il conteggio.

Effettuare le operazioni seguenti:

1. Effettuare l'accesso al Recovery Point Server.
2. Accedere alla posizione seguente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
3. Creare una chiave nella directory del modulo, quindi denominare la chiave *JumpStart RPS*.
4. Aggiungere il seguente valore DWORD alla chiave JumpStart RPS:

   JumpStartConCurrencyCount
5. Fornire un valore per DWORD.

   Esempio: Se si desidera impostare un numero massimo di 10 nodi per il processo JumpStart RPS, aggiungere il seguente elemento come DWORD:

   JumpStartConCurrencyCount=10

   Il numero dei nodi simultanei è impostato per JumpStart RPS.

Esecuzione della replica inversa

L'utilizzo di questa funzionalità consente di eseguire la replica dei dati (punto di ripristino) da Cloud, MSP o un server RPS gestito in remoto su UDP o un server RPS on-premise. Per recuperare i dati replicati sul server UDP locale o on-premise da un Recovery Point Server gestito da una console Arcserve UDP diversa, ad esempio Cloud, MSP o un server RPS gestito in remoto, è necessario eseguire la replica inversa. Nella replica inversa, i dati vengono replicati da un archivio dati di destinazione (sulla console di destinazione) su un archivio dati di origine (sulla console di origine).

La presente sezione descrive i seguenti argomenti:

Verifica dei prerequisiti

Verificare i prerequisiti seguenti prima di eseguire la replica dei dati:

- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Amministratore - Console di destinazione

- Verificare che Arcserve UDP sia stato installato sul server di destinazione.
- Verificare di disporre dei privilegi completi per la creazione di account utenti Windows sul server di destinazione.
- Verificare di aver attivato la casella di controllo **Consenti il recupero dei punti di ripristino** nelle Impostazioni avanzate durante la creazione della replica da un piano RPS gestito in remoto.

  Nota: se non si attiva la casella di controllo **Consenti il recupero dei punti di ripristino** e si avvia il processo di replica inversa per la console remota, viene richiesto di attivare il flag Consenti il recupero dei punti di ripristino per la replica inversa.

Amministratore - Console di origine UDP

- Verificare che Arcserve UDP sia stato installato sul server di origine.
- Verificare che sia stato completato almeno un backup completo su un archivio dati.

Esecuzione della replica ad hoc

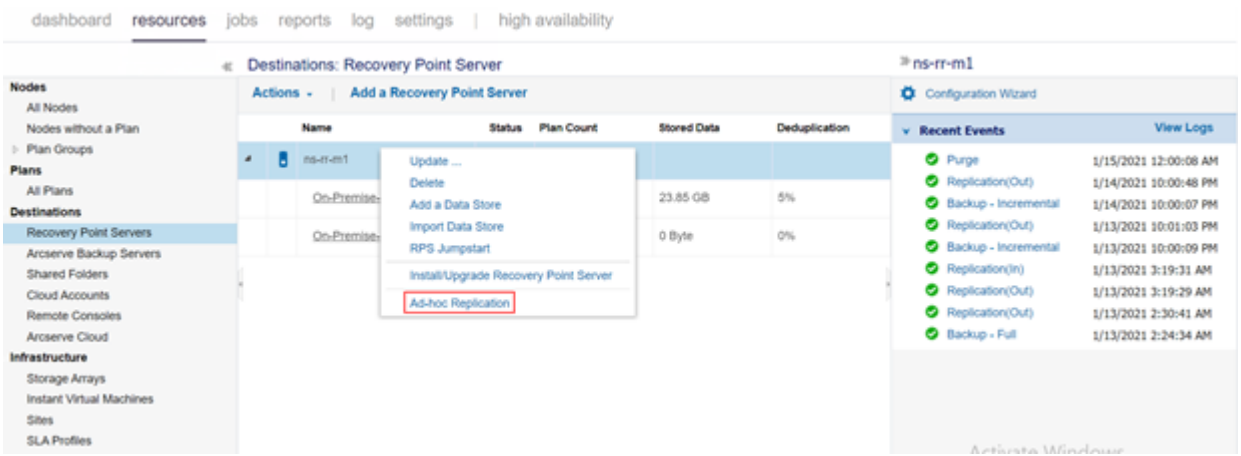
In questa sezione viene descritta la modalità di avvio della replica ad hoc.

Nota: prima di eseguire la replica ad hoc, assicurarsi che la replica diretta sia stata eseguita correttamente. Per verificare se la replica diretta è stata eseguita correttamente, consultare la sezione Verifica della replica dei dati.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

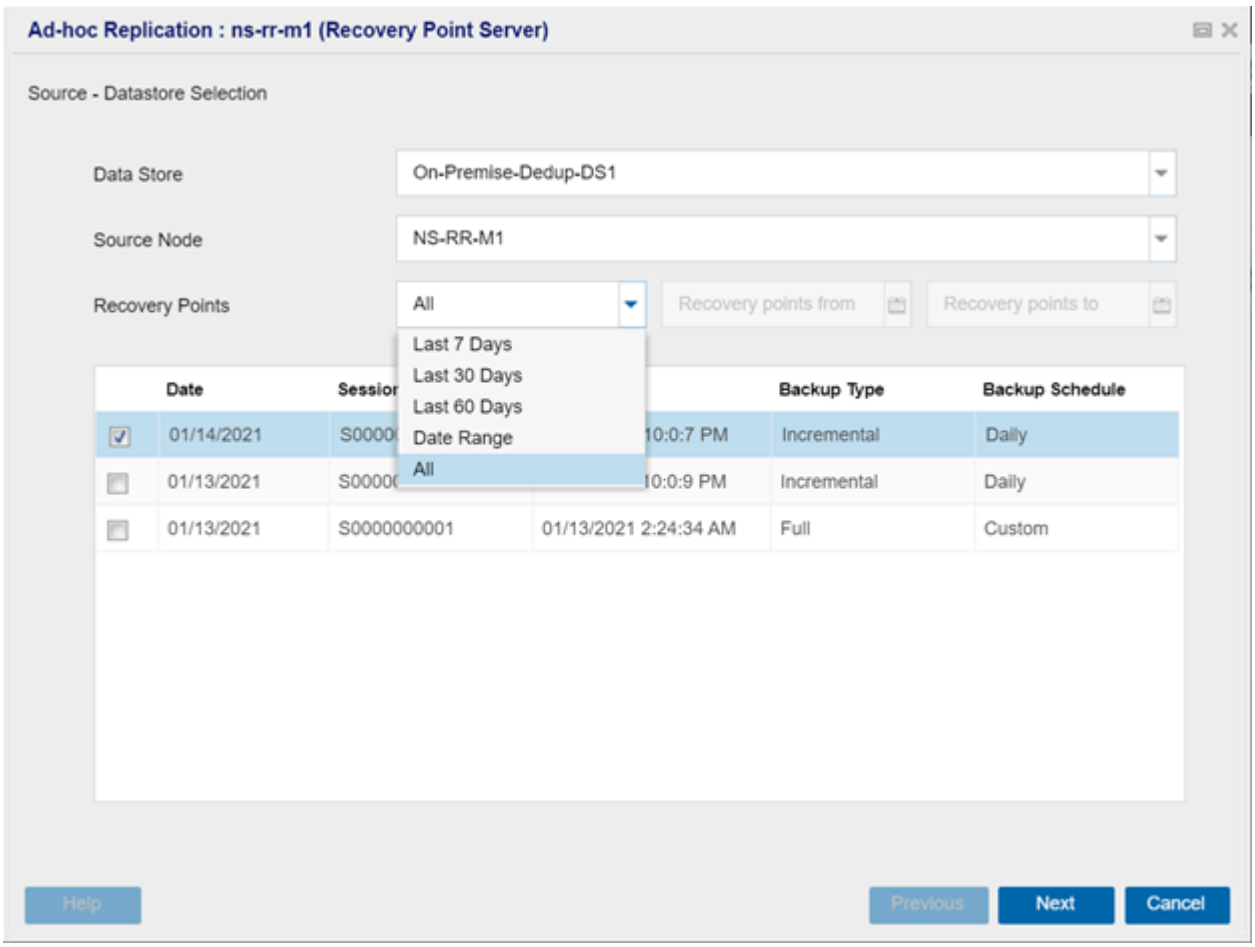
   L'elenco dei Recovery Point Server viene visualizzato nel riquadro centrale.
3. Fare clic con il pulsante destro del mouse sul Recovery Point Server, quindi selezionare **Replica ad hoc**.



Attendere la connessione al Recovery Point Server.

Viene visualizzata la finestra di dialogo Replica ad hoc: xx-xx-xx (Recovery Point Server).

4. Nella pagina Origine - Selezione archivio dati, procedere come segue:



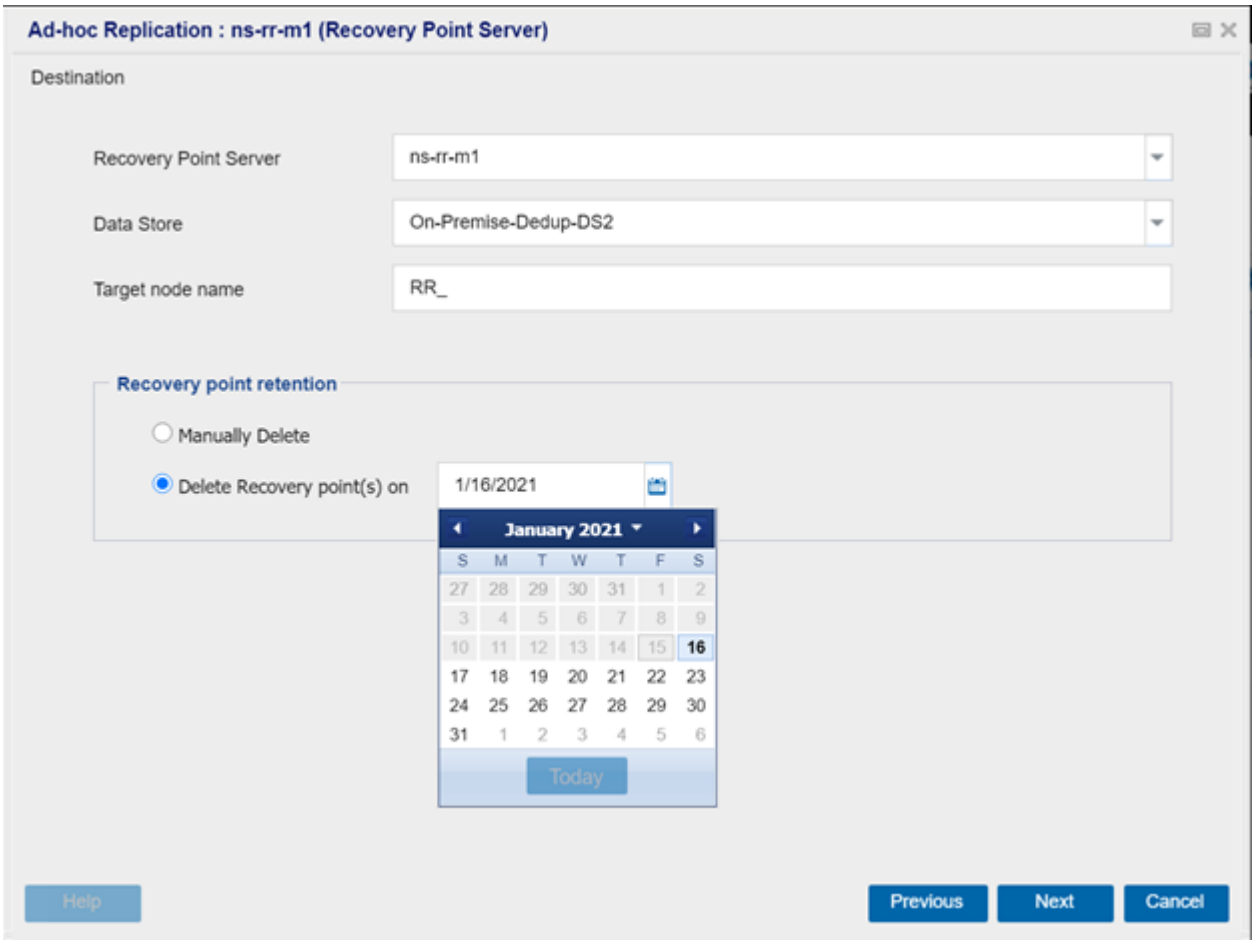
- Archivio dati: selezionare l'archivio dati di origine dall'elenco a discesa.
- Nodo di origine: selezionare il nodo di origine dall'elenco a discesa.

- Punti di ripristino: eseguire una delle seguenti operazioni:
  - Se si desidera visualizzare tutti i punti di ripristino di cui è stato eseguito il backup, selezionare **Tutto** dall'elenco a discesa.
  - Se si desidera visualizzare i punti di ripristino per una durata specifica, selezionare una delle opzioni seguenti dall'elenco a discesa:
    - Ultimi 7 giorni
    - Ultimi 30 giorni
    - Ultimi 60 giorni
    - Intervallo date

    Nota: se è stato selezionato **Intervallo date**, impostare la data nei campi **Punti di ripristino da** e **Punti di ripristino a**.

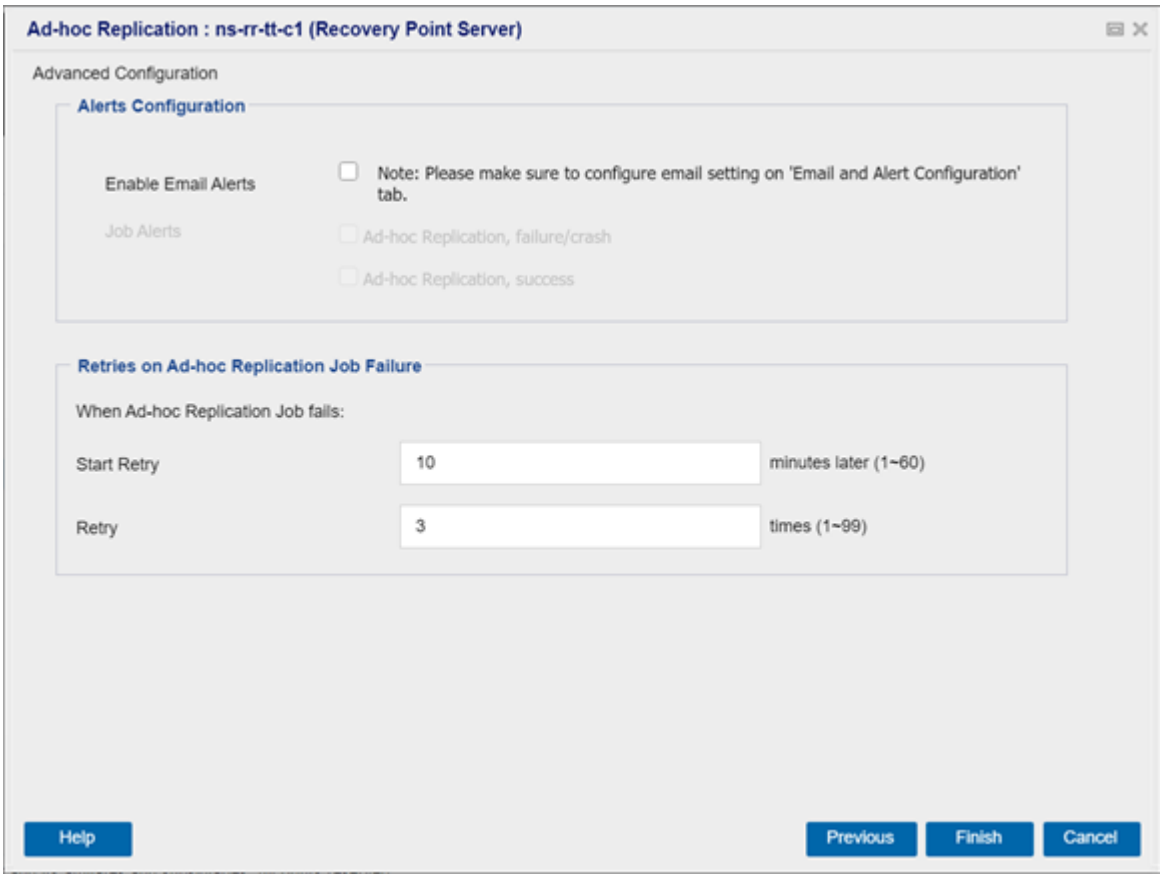
  Verranno visualizzati tutti i punti di ripristino associati per la durata specificata.
- Dalla tabella, fare clic sulle caselle di controllo per selezionare uno o più punti di ripristino.

5. Fare clic su **Avanti**.
6. Nella pagina Destinazione, eseguire le seguenti operazioni:



- Recovery Point Server: selezionare il Recovery Point Server di destinazione dall'elenco a discesa.
- Archivio dati: selezionare l'archivio dati di destinazione dall'elenco a discesa.
- Nome nodo di destinazione: immettere un nome per il nodo di destinazione.
- Conservazione punto di ripristino: eliminare i punti di ripristino in uno dei seguenti modi:
  - Per eliminare manualmente i punti di ripristino, selezionare l'opzione **Elimina manualmente**.
  - Se si desidera che i punti di ripristino vengano eliminati automaticamente, selezionare l'opzione **Elimina punti di ripristino**, quindi specificare la data. Tutti i punti di ripristino corrispondenti a tale data vengono eliminati automaticamente.

7. Fare clic su **Avanti**.
8. Nella pagina Configurazione avanzata, procedere come segue:



- Per la configurazione degli avvisi

  Abilitazione degli avvisi di posta elettronica

  Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere in un messaggio di posta elettronica. Quando si seleziona la casella di controllo **Nota: assicurarsi di configurare le impostazioni di posta elettronica nella scheda Configurazione posta elettronica e avvisi**, la seguente opzione è abilitata per la selezione:

  Avvisi di processo

  Consente di selezionare i tipi di messaggi di posta elettronica di avviso del processo che si desidera ricevere.

  - Se si desidera ricevere avvisi di posta elettronica in caso di errore o arresto anomalo della replica ad hoc, selezionare la casella di controllo **Replica ad hoc, errore/arresto anomalo**.

    Nota: questo avviso di posta elettronica viene inviato con priorità alta. Gli avvisi di posta elettronica associati a un'impostazione di

priorità alta vengono contrassegnati mediante da punto esclamativo nella casella di posta elettronica.

- Se si desidera ricevere avvisi di posta elettronica per la corretta esecuzione della replica ad hoc, selezionare la casella di controllo **Replica ad hoc, riuscita**.

- Per i nuovi tentativi in caso di errore del processo di replica ad hoc

  Quando il processo di replica ad hoc non riesce, procedere come segue:

  Avvia nuovo tentativo

  Consente di specificare il tempo (in minuti) per il riavvio del processo di replica in seguito all'errore del processo. Ad esempio, se si specificano 10 minuti, il processo di replica verrà riavviato 10 minuti dopo l'errore.

  Limite: da 1 a 60

  Riprova

  Consente di specificare il numero di tentativi che si desidera eseguire nel caso in cui il processo di replica non riesca. Il processo di replica verrà eseguito fino a quando il processo avrà esito positivo, oppure fino al raggiungimento del limite. Una volta superato il numero di tentativi, il processo di replica viene eseguito solo all'ora pianificata successiva.

  Limite: da 1 a 99

9. Fare clic su **Fine**.

   Nota: se si desidera modificare le impostazioni delle schermate precedenti, fare clic su **Precedente**, quindi modificare le impostazioni in base alle esigenze.

   Viene visualizzata la finestra di dialogo Informazioni e viene visualizzato il messaggio *Processo di replica ad hoc inoltrato correttamente*.

10. Fare clic su **OK** per chiudere la finestra di dialogo Informazioni.

    La replica ad hoc è stata eseguita correttamente.

Monitoraggio dello stato della replica ad hoc

Amministratore dell'origine

Una volta completata correttamente la replica ad hoc, è possibile monitorare lo stato del processo di replica ad hoc.

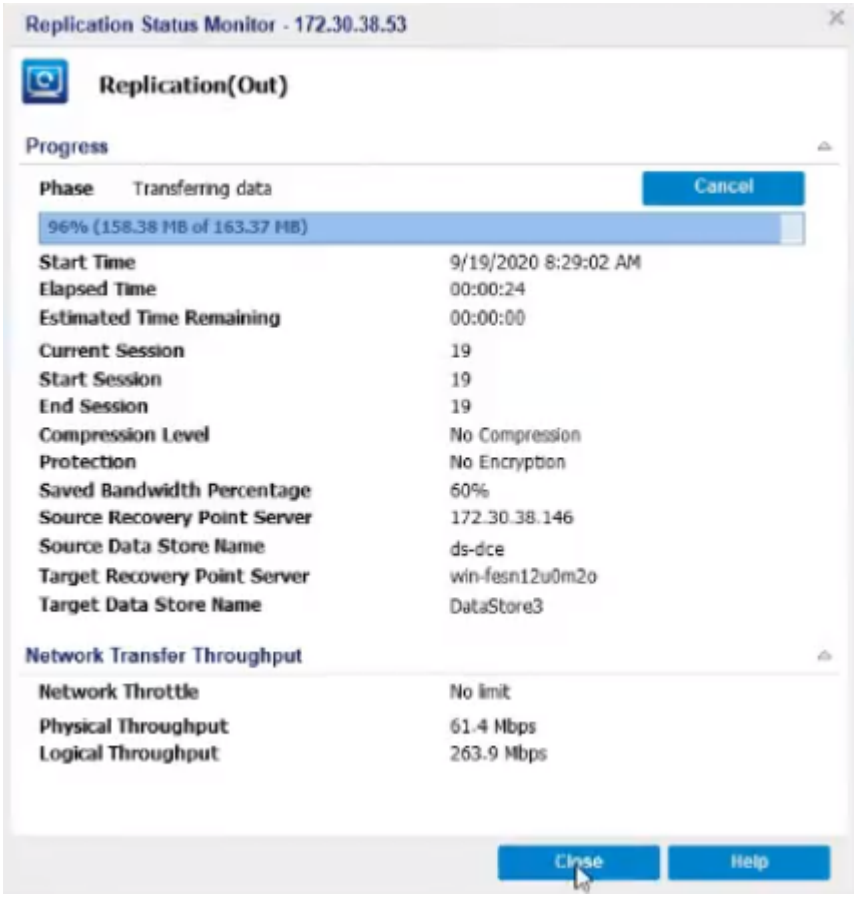
Effettuare le operazioni seguenti:

1. Accedere a **Processi** > **Processi in corso**.

   I processi di replica (in uscita) e di replica (in entrata) in corso vengono visualizzati nel riquadro centrale.

2. Per monitorare lo stato di un processo specifico, fare clic su **Dettagli** accanto alla barra di avanzamento corrispondente al processo.

   Viene visualizzata la finestra di dialogo Monitoraggio dello stato di replica – xx.xx.xx.xx.



3. Attendere il completamento al 100% del trasferimento dei dati, quindi fare clic su **Chiudi**.

Lo stato della replica ad hoc è stato monitorato correttamente.

Verifica della corretta esecuzione della replica ad-hoc

Amministratore dell'origine

Una volta completato il processo di replica, verificare che la replica ad-hoc sia stata eseguita correttamente.

Effettuare le operazioni seguenti:

1. Nella console di origine, accedere a **Processi** > **Processi completati correttamente**.

   Nel riquadro centrale viene visualizzato un elenco di processi completati.

2. Fare clic sul processo di replica inversa completato. Il riquadro destro viene aggiornato.
3. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
4. Verificare che la replica dei dati sia stata eseguita correttamente.

La replica ad hoc è stata verificata correttamente.

Esecuzione della replica inversa dalla console remota sul server RPS on-premise

In questa sezione viene descritta la modalità di esecuzione della replica inversa dalla console remota al server UDP locale o al server RPS on-premise.

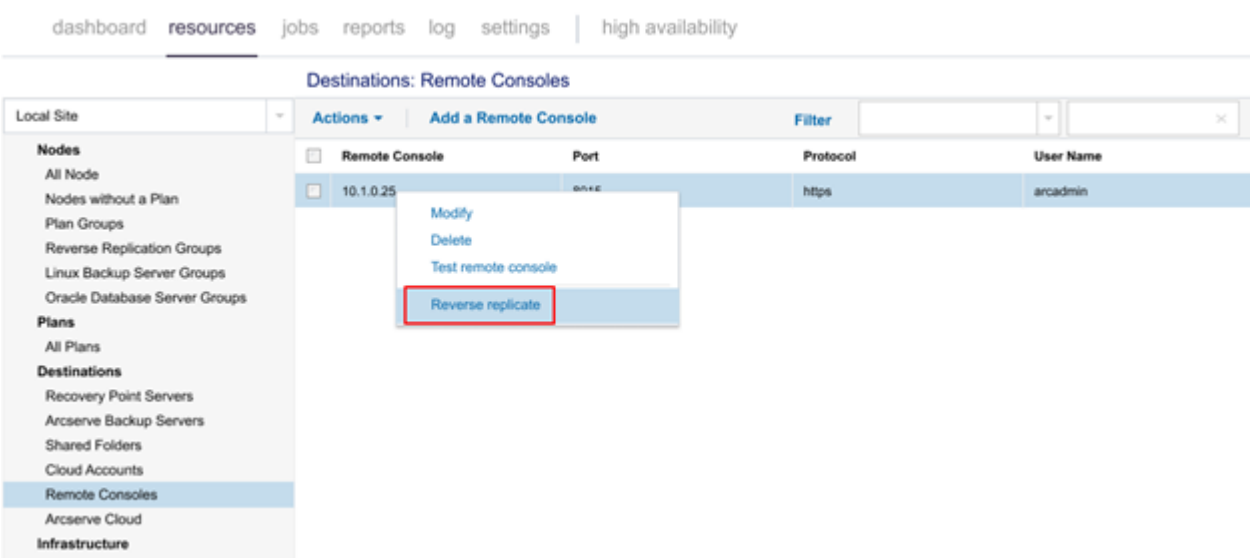
Nota: prima di eseguire la replica inversa, assicurarsi che la replica diretta sia stata eseguita correttamente. Per verificare se la replica diretta è stata eseguita correttamente, consultare la sezione Verifica della replica dei dati.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni** > **Console remota**.

   L'elenco delle console remote viene visualizzato nel riquadro centrale.

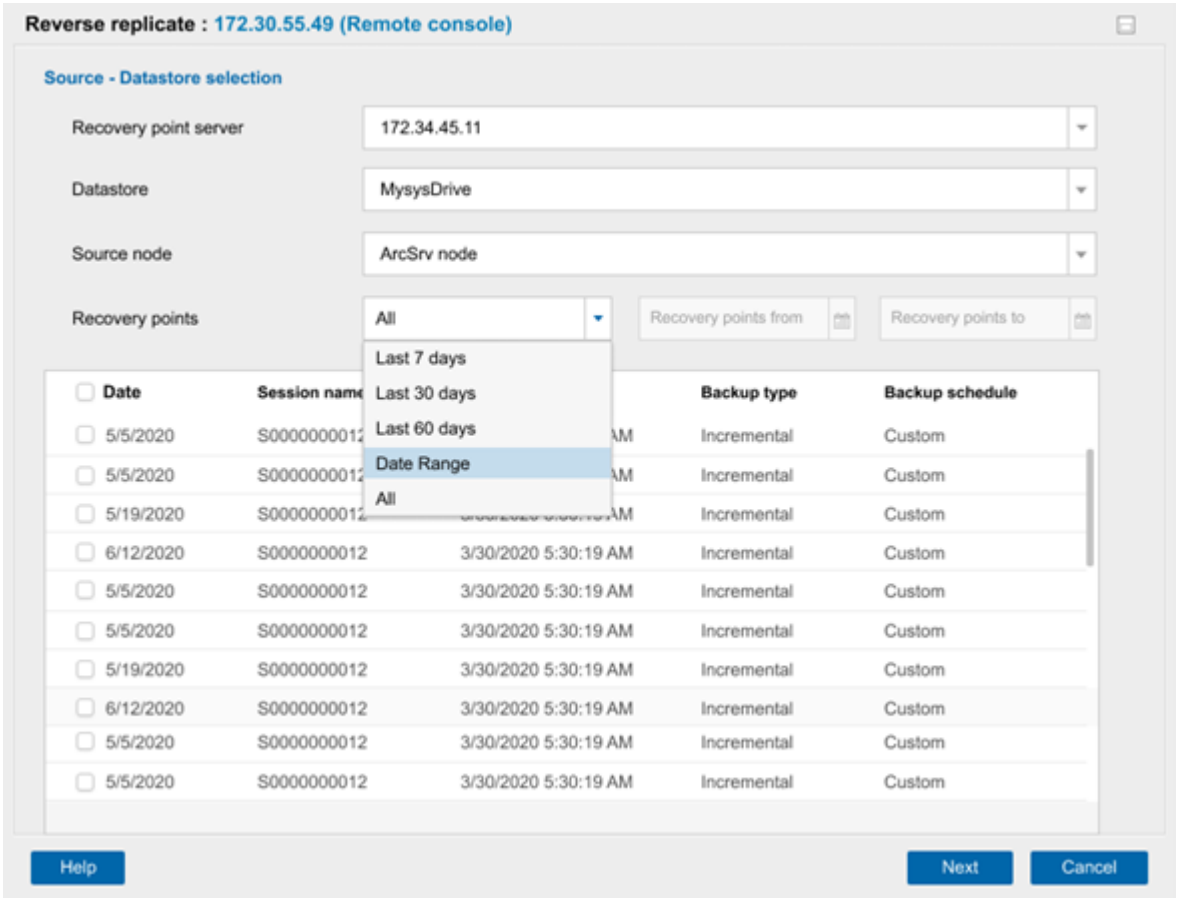
3. Fare clic con il pulsante destro del mouse sulla console remota, quindi selezionare **Replica inversa**.



Attendere la connessione alla console remota.

Viene visualizzata la finestra di dialogo Replica inversa: xxx.xx.xx.xxx (Console remota).

4. Nella pagina Origine - Selezione archivio dati, procedere come segue:

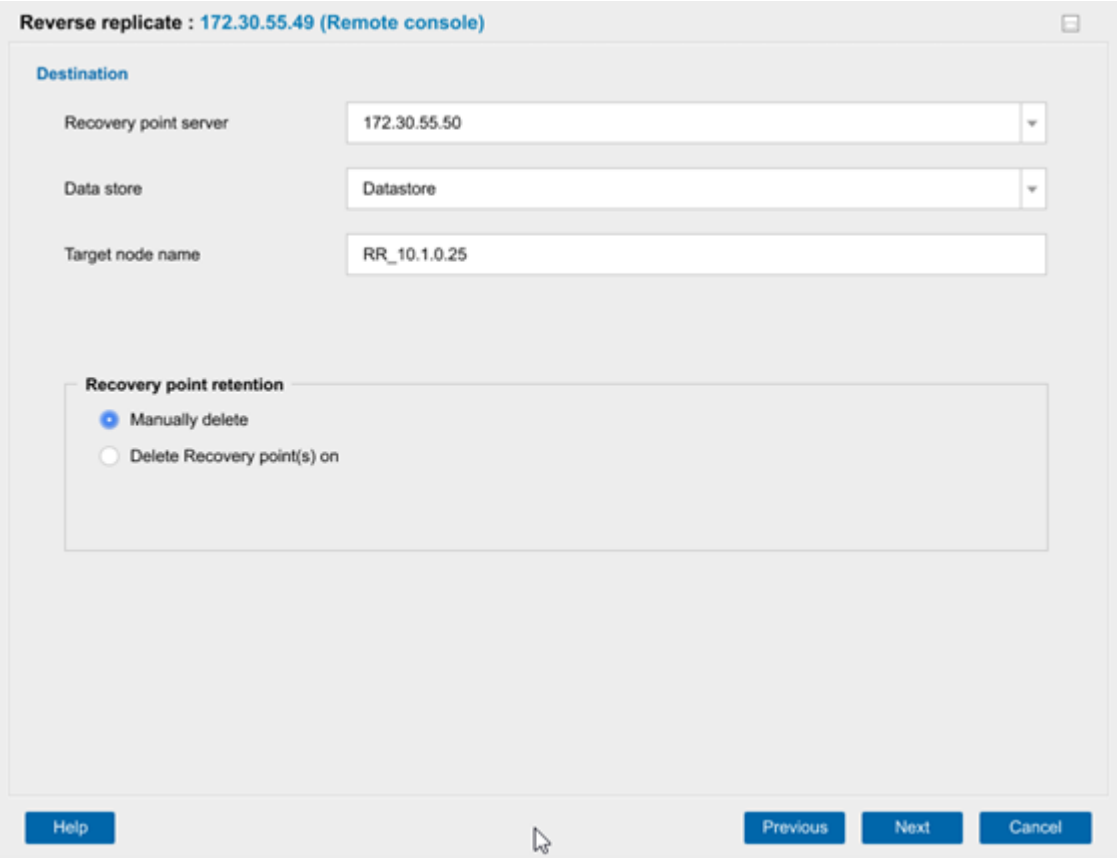


- Recovery Point Server: selezionare il Recovery Point Server di origine dall'elenco a discesa.
- Archivio dati: selezionare l'archivio dati di origine dall'elenco a discesa.
- Nodo di origine: selezionare il nodo di origine dall'elenco a discesa.
- Punti di ripristino: eseguire una delle seguenti operazioni:
  - Se si desidera visualizzare tutti i punti di ripristino di cui è stato eseguito il backup, selezionare **Tutto** dall'elenco a discesa.
  - Se si desidera visualizzare i punti di ripristino per una durata specifica, selezionare una delle opzioni seguenti dall'elenco a discesa:
    - Ultimi 7 giorni
    - Ultimi 30 giorni
    - Ultimi 60 giorni
    - Intervallo date

    Nota: se è stato selezionato **Intervallo date**, impostare la data nei campi **Punti di ripristino da** e **Punti di ripristino a**.

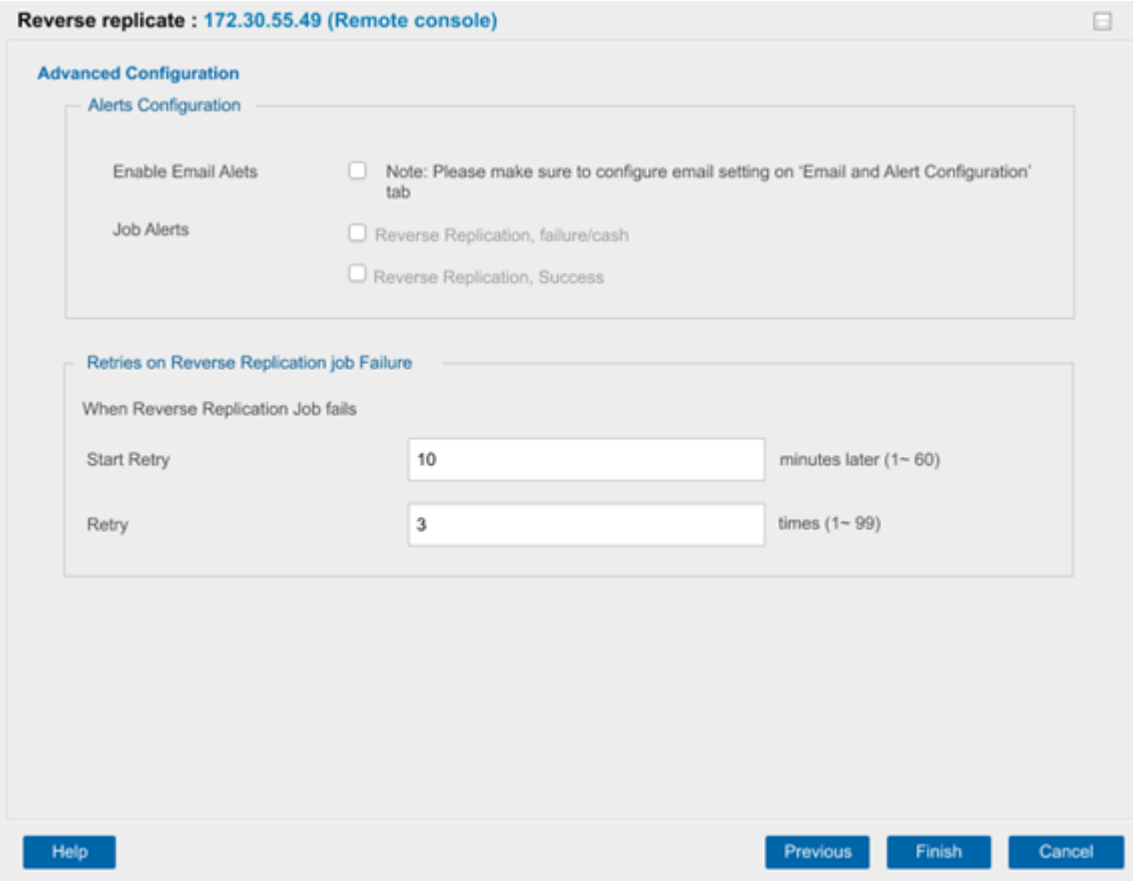
  Verranno visualizzati tutti i punti di ripristino associati per la durata specificata.
- Dalla tabella, fare clic sulle caselle di controllo per selezionare uno o più punti di ripristino.

5. Fare clic su **Avanti**.
6. Nella pagina Destinazione, eseguire le seguenti operazioni:



- Recovery Point Server: selezionare il Recovery Point Server di destinazione dall'elenco a discesa.
- Archivio dati: selezionare l'archivio dati di destinazione dall'elenco a discesa.
- Nome nodo di destinazione: immettere un nome per il nodo di destinazione.
- Conservazione punto di ripristino: eliminare i punti di ripristino in uno dei seguenti modi:
  - Per eliminare manualmente i punti di ripristino, selezionare l'opzione **Elimina manualmente**.
  - Se si desidera che i punti di ripristino vengano eliminati automaticamente, selezionare l'opzione **Elimina punti di ripristino**, quindi specificare la data. Tutti i punti di ripristino corrispondenti a tale data vengono eliminati automaticamente.

7. Fare clic su **Avanti**.
8. Nella pagina Configurazione avanzata, procedere come segue:



- Per la configurazione degli avvisi

  Abilitazione degli avvisi di posta elettronica

  Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere in un messaggio di posta elettronica. Quando si seleziona la casella di controllo **Nota: assicurarsi di configurare le impostazioni di posta elettronica nella scheda Configurazione posta elettronica e avvisi**, la seguente opzione è abilitata per la selezione:

  Avvisi di processo

  Consente di selezionare i tipi di messaggi di posta elettronica di avviso del processo che si desidera ricevere.

  - Se si desidera ricevere avvisi di posta elettronica in caso di errore o arresto anomalo della replica inversa, selezionare la casella di controllo **Replica inversa, errore/arresto anomalo**.

    Nota: questo avviso di posta elettronica viene inviato con priorità alta. Gli avvisi di posta elettronica associati a un'impostazione di

priorità alta vengono contrassegnati mediante da punto esclamativo nella casella di posta elettronica.

- Se si desidera ricevere avvisi di posta elettronica per la corretta esecuzione della replica inversa, selezionare la casella di controllo **Replica inversa, riuscita**.

- Per i nuovi tentativi in caso di errore del processo di replica inversa

  Quando il processo di replica inversa non riesce, procedere come segue:

  Avvia nuovo tentativo

  Consente di specificare il tempo (in minuti) per il riavvio del processo di replica in seguito all'errore del processo. Ad esempio, se si specificano 10 minuti, il processo di replica verrà riavviato 10 minuti dopo l'errore.

  Limite: da 1 a 60

  Riprova

  Consente di specificare il numero di tentativi che si desidera eseguire nel caso in cui il processo di replica non riesca. Il processo di replica verrà eseguito fino a quando il processo avrà esito positivo, oppure fino al raggiungimento del limite. Una volta superato il numero di tentativi, il processo di replica viene eseguito solo all'ora pianificata successiva.

  Limite: da 1 a 99

9. Fare clic su **Fine**.

   Nota: se si desidera modificare le impostazioni delle schermate precedenti, fare clic su **Precedente**, quindi modificare le impostazioni in base alle esigenze.

   Viene visualizzata la finestra di dialogo Informazioni, contenente il messaggio *Processo di replica inversa inoltrato correttamente*.

10. Fare clic su **OK** per chiudere la finestra di dialogo Informazioni.

    La replica inversa è stata completata correttamente dalla console remota al server UDP locale o al server UDP on premise.

Monitoraggio dello stato della replica inversa

Amministratore dell'origine

Una volta completata correttamente la replica inversa, è possibile monitorare lo stato del processo di replica inversa.

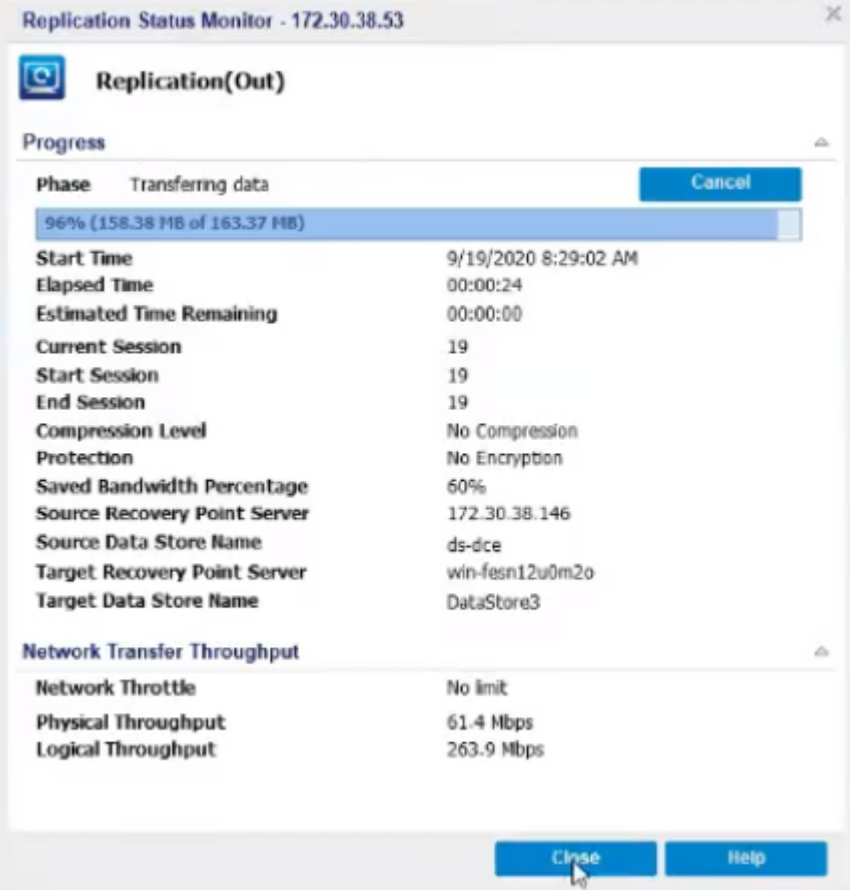
Effettuare le operazioni seguenti:

1. Accedere a **Processi** > **Processi in corso**.

   I processi di replica (in uscita) e di replica (in entrata) in corso vengono visualizzati nel riquadro centrale.

2. Per monitorare lo stato di un processo specifico, fare clic su **Dettagli** accanto alla barra di avanzamento corrispondente al processo.

   Viene visualizzata la finestra di dialogo Monitoraggio dello stato di replica – xx.xx.xx.xx.



3. Attendere il completamento al 100% del trasferimento dei dati, quindi fare clic su **Chiudi**.

Lo stato della replica inversa è stato monitorato correttamente.

Verifica della corretta esecuzione della replica inversa

Amministratore dell'origine

Una volta completato il processo di replica dei dati, verificare che sia stato eseguito correttamente.

Effettuare le operazioni seguenti:

1. Nella console di origine, accedere a **Processi** > **Processi completati correttamente**.

   Nel riquadro centrale viene visualizzato un elenco di processi completati.
2. Fare clic sul processo di replica inversa completato. Il riquadro destro viene aggiornato.
3. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
4. Verificare che la replica dei dati sia stata eseguita correttamente.

La replica inversa dei dati è stata verificata correttamente dalla console remota al server UDP locale o al server RPS on-premise.

Creazione di un piano di copia dei punti di ripristino

Arcserve Unified Data Protection consente di copiare i punti di ripristino in una cartella condivisa o in un volume locale per proteggere i punti di ripristino. Questo processo consente di disporre di una copia aggiuntiva dei punti di ripristino se i punti di ripristino originali vengono eliminati accidentalmente. L'attività Copia punti di ripristino copia i punti di ripristino dalla destinazione di backup solo nel cloud, in una cartella condivisa o in un volume locale. Non è possibile copiare il punto di ripristino in un Recovery Point Server.

È possibile aggiungere solamente una attività di copia dei punti di ripristino in un piano.

Note:

- Nella versione corrente, i processi di copia del punto di ripristino non sono supportati se **Backup: Linux basato su agente** viene creato come Attività1.
- I processi di copia del punto di ripristino vengono sempre eseguiti sull'agente, anche nel caso in cui il backup è configurato sul Recovery Point Server.

  Per il backup del computer virtuale senza agente, è il proxy dell'agente UDP utilizzato in Attività1 a elaborare il processo di copia del punto di ripristino.

Risoluzione dei problemi: Congestione della larghezza di banda con i processi di copia del punto di ripristino su cloud

Come procedere?

- Verifica delle considerazioni e dei prerequisiti
- Creazione di un piano con un'attività di
- Aggiunta di un'attività di copia dei punti di ripristino al piano
- Verifica del piano

Verifica delle considerazioni e dei prerequisiti

Verificare se i prerequisiti seguenti sono stati completati:

- Accedere alla console.
- Installare il componente server e creare gli archivi dati qualora si desideri archiviare i dati di backup nei Recovery Point Server.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Creazione di un piano con un'attività di backup

Un piano include diversi tipi di attività da eseguire. Per creare un'attività Copia punti di ripristino, è necessario innanzitutto disporre di un punto di ripristino valido. Per ottenere un punto di ripristino valido, è necessario creare un'attività di backup.

Un'attività di backup esegue un backup dei nodi di origine e archivia i dati nella destinazione specificata. L'attività Copia punti di ripristino è supportata sia per il backup Windows basato su agente, sia per il backup senza agente basato su host. La procedura seguente illustra le fasi per creare l'attività di backup Windows basata su agente. Non è possibile eseguire la copia del punto di ripristino per i piani di backup basati sull'agente Linux.

Nota: Per ulteriori informazioni sul backup senza agente basato su host, consultare la sezione Creazione di un piano di backup di un computer virtuale basato su host.

Per ulteriori informazioni sul backup del percorso UNC, consultare la sezione Creazione di un piano di backup del percorso UNC.

Per ulteriori informazioni sul backup di Exchange Online, consultare la sezione Creazione di un piano di backup di Exchange Online.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

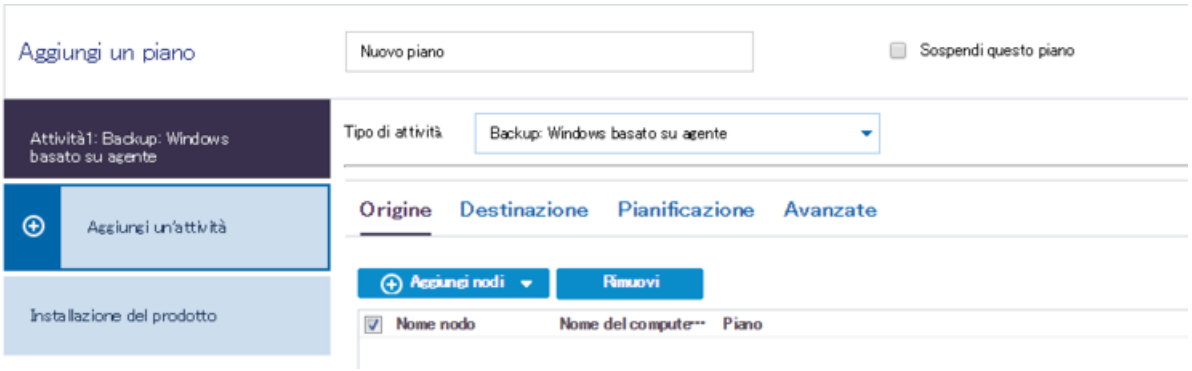
   Viene visualizzata la finestra di dialogo **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano** per sospendere il piano.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di

replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.

6. Dall'elenco a discesa **Tipo di attività**, selezionare **Backup, Windows basato su agente**.



Specificare quindi i dettagli per i campi Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine che si desidera proteggere. È possibile selezionare più di un nodo per un piano. Se non sono stati aggiunti nodi alla console, è possibile aggiungerli in fase di creazione o modifica di un piano dalla pagina Origine. È inoltre possibile salvare un piano senza aggiungere nessun nodo di origine. Il piano viene distribuito soltanto dopo l'aggiunta dei nodi di origine.

Effettuare le operazioni seguenti:

1. Nella scheda Origine, fare clic su **Aggiungi**.
2. Selezionare una delle seguenti opzioni:

   Selezionare i nodi da proteggere in Arcserve UDP

   Consente di visualizzare la finestra di dialogo Selezionare i nodi da proteggere in Arcserve UDP. Selezionare i nodi dall'elenco visualizzato. Selezionare questa opzione se sono stati già aggiunti nodi alla Console.

   Aggiungi nodo Windows

   Viene visualizzata la finestra di dialogo Aggiungi nodi a un piano. Selezionare questa opzione se non sono stati aggiunti nodi e si desidera aggiungere manualmente i nodi da proteggere.

   Rileva nodi da Active Directory

   Consente di aprire la finestra di dialogo Aggiungi nodi alla Console Arcserve UDP. Selezionare questa opzione se si desidera rilevare e aggiungere nodi da Active Directory.
3. Se è stata selezionata l'opzione **Selezionare i nodi da proteggere in Arcserve UDP**, nella finestra di dialogo Selezionare i nodi da proteggere, procedere come segue:
   a. (Facoltativo) Selezionare un filtro dall'elenco a discesa Gruppi per filtrare i nodi. Immettere parole chiave per applicare ulteriori filtri ai nodi.

      I nodi vengono visualizzati nella colonna Nodi disponibili.

   b. Selezionare i nodi dalla colonna Nodi disponibili, quindi fare clic sulla freccia destra singola (>) o sulla freccia destra doppia (>>) per spostare rispettivamente i nodi selezionati o tutti i nodi nella colonna Nodi selezionati.

      I nodi vengono visualizzati nella colonna Nodi selezionati.

   c. Fare clic su **OK** per chiudere la finestra di dialogo.



4. Per scegliere il Tipo di protezione, selezionare una delle seguenti opzioni:

   Backup di tutti i volumi

   Prepara una snapshot del backup di tutti i volumi.

   Backup dei volumi selezionati

   Prepara una snapshot del backup del volume selezionato.

   L'origine viene specificata.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Selezionare un **Tipo di destinazione** tra quelli elencati di seguito:

   Disco locale o cartella condivisa

   Specifica che la destinazione di backup è una destinazione locale o una cartella condivisa. Se si seleziona questa opzione, è possibile salvare i dati come punti di ripristino o set di ripristino. Le opzioni dei punti di ripristino e dei set di ripristino sono disponibili nella scheda **Pianificazione.**

   Recovery Point Server di Arcserve UDP

   Specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono memorizzati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.

2. Se è stato selezionato il **Recovery Point Server di Arcserve UDP**, immettere i seguenti dettagli:
   a. Selezionare un Recovery Point Server
   b. Selezionare un archivio dati. L'elenco mostra tutti gli archivi dati creati sul Recovery Point Server specificato.
   c. Fornire una password di sessione.
   d. Confermare la password di sessione.
3. Se è stata selezionata l'opzione **Utilizza il disco locale o la cartella condivisa**, fornire i dettagli seguenti:
   a. Fornire il percorso completo della destinazione locale o di rete. Per la destinazione di rete, specificare le credenziali con l'accesso di scrittura.
   b. Selezionare l'algoritmo di crittografia. Per ulteriori informazioni, consultare la sezione Impostazioni di crittografia.
   c. Facoltativamente, fornire una password di crittografia.
   d. Confermare la password di crittografia.
   e. Selezionare un tipo di compressione. Per ulteriori informazioni, consultare la sezione Tipo di compressione.

Note:

- La copia del punto di ripristino (CRP) non supporta i backup personalizzati anche quando viene aggiunta la pianificazione CRP. Inoltre, l'attività CRP non supporta la pianificazione di backup personalizzata.
- Il processo CRP su cloud è supportato solo da una console. Non supporta un agente standalone.
- Sia i *dischi locali che le cartelle condivise*, nonché i *backup archiviati su RPS* supportano le attività CRP.

La destinazione viene specificata.

Definizione della pianificazione

La pagina di pianificazione consente di definire una pianificazione per il backup. La copia dei punti di ripristino supporta backup giornalieri, settimanali e mensili dalla console. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni giornaliere, settimanali e mensili, oltre alla possibilità di specificare impostazioni di memorizzazione.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

Effettuare le operazioni seguenti:

1. (Facoltativo) Selezionare l'opzione per la gestione dei punti di ripristino. Questa opzione è visibile solamente se sono state selezionate le cartelle Locale o Condivisa come destinazione di backup.

   Conserva per punti di ripristino

   I dati di backup vengono archiviati come punti di ripristino.

   Conserva per set di ripristino

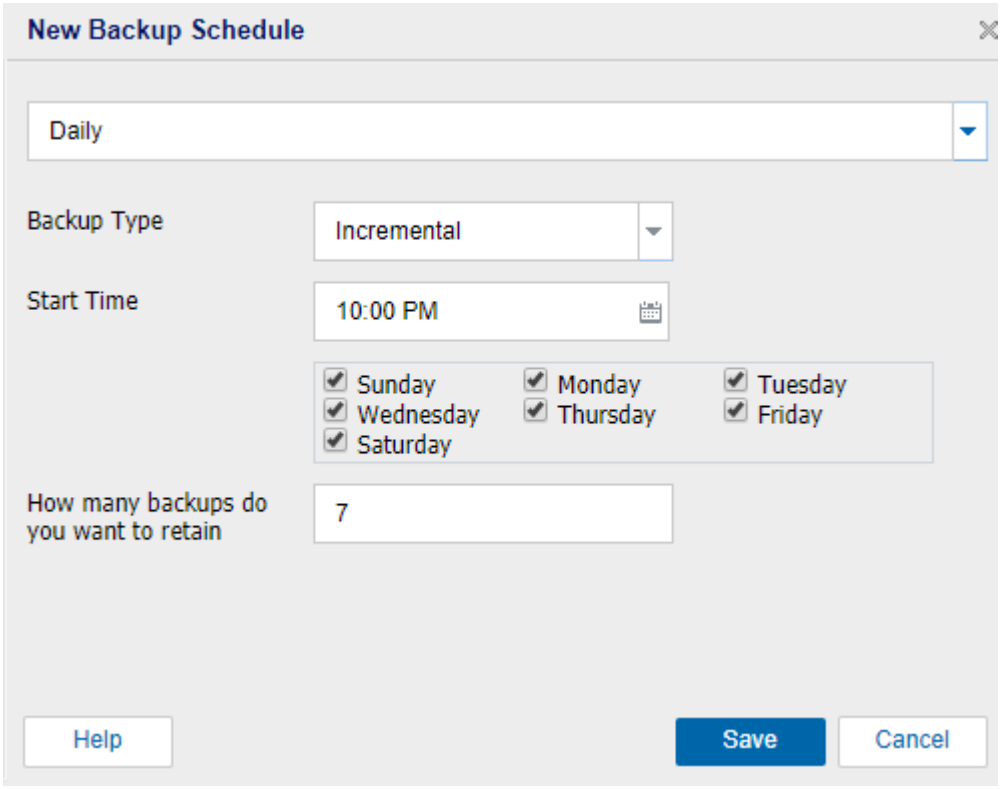
   I dati di backup vengono archiviati come set di ripristino.

   Nota: l'opzione Mantieni per set di ripristino non è supportata per la copia dei punti di ripristino.

2. Aggiungere una pianificazione di backup.

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni di backup.

Incrementale

Specifica la pianificazione dei backup incrementali.

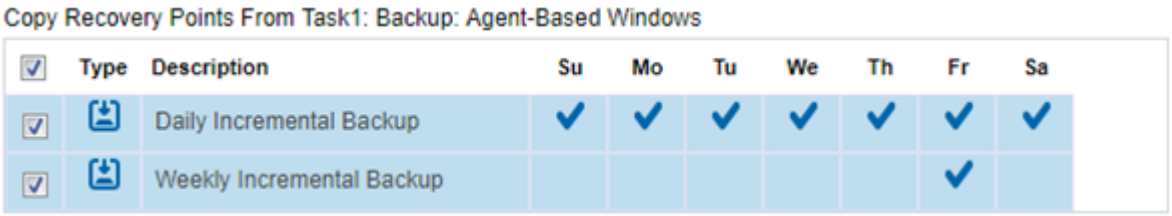
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup con dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

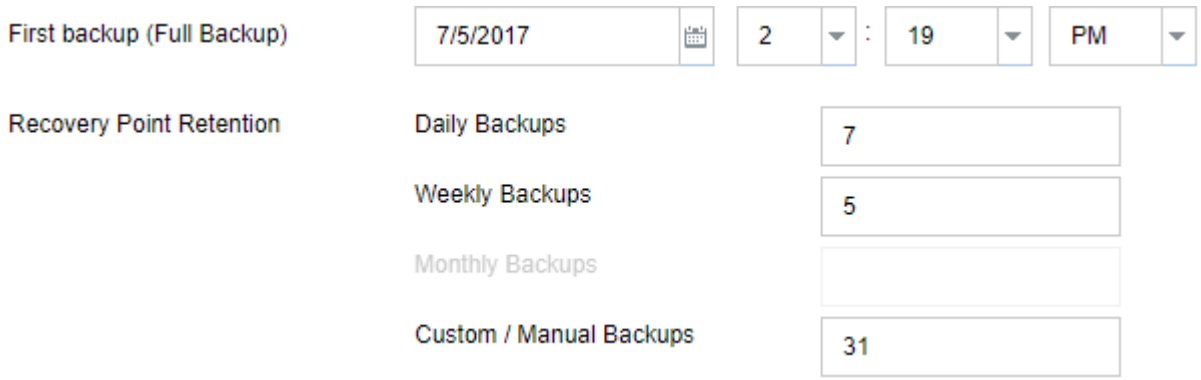
e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



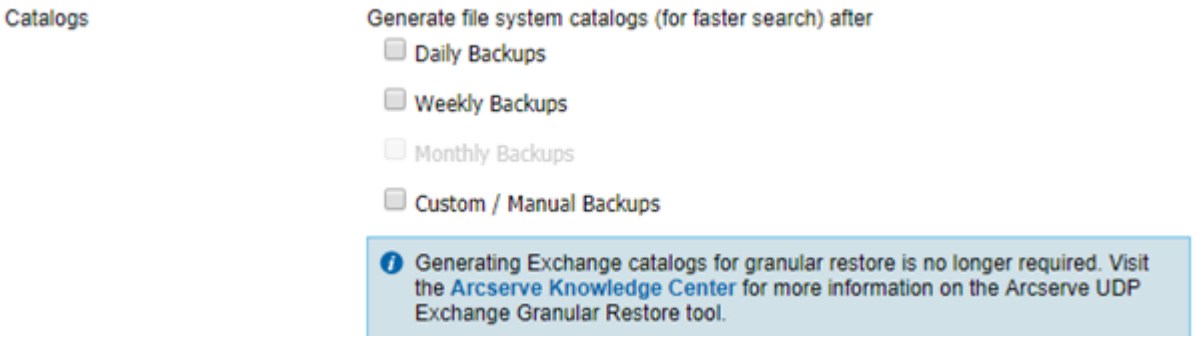
3. Specificare l'ora di inizio per il backup pianificato.



4. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione giornaliera, settimanale o mensile.

Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo Pianificazione di backup.

5. Specificare i dettagli relativi al catalogo.



I cataloghi permettono di generare il catalogo file system. Il catalogo file system è necessario per migliorare e velocizzare la ricerca. Se si selezionano le caselle di controllo del catalogo, i cataloghi verranno abilitati in base al tipo di backup specificato. Deselezionare una casella di controllo per disattivare la generazione del catalogo.

Viene specificata la pianificazione.

Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione

L'opzione di pianificazione consente di specificare una pianificazione personalizzata o una pianificazione giornaliera/settimanale/mensile o entrambe. Nella pianificazione personalizzata è possibile configurare la pianificazione del backup per ciascun giorno della settimana e aggiungere fino a quattro pianificazioni di backup ogni giorno. È possibile selezionare un giorno specifico di una settimana e creare un intervallo di tempo per definire quando eseguire il backup e la frequenza.

Pianificazione	Processo supportato	Commenti
Backup	Processo di backup	Definire gli intervalli di tempo per eseguire i processi di backup.
Limitazione della velocità di backup	Processo di backup	Definire gli intervalli di tempo per controllare la velocità di backup.
Unione	Processo di unione	Definire quando unire i processi.
Pianificazione quotidiana	Processo di backup	Definire quando eseguire processi di backup quotidiani.
Pianificazione settimanale	Processo di backup	Definire quando eseguire processi di backup settimanali.
Pianificazione mensile	Processo di backup	Definire quando eseguire processi di backup mensili.

È inoltre possibile specificare le impostazioni di memorizzazione per i punti di ripristino.

Nota: All'interno di ogni piano è necessario configurare le impostazioni di conservazione per controllare il modo in cui i nodi assegnati a tale piano vengono memorizzati nell'archivio dati di destinazione.

Le pianificazioni per i backup giornalieri/settimanali/mensili sono indipendenti dalla pianificazione personalizzata e gli uni dagli altri. È possibile configurare di eseguire solo il backup giornaliero, il backup settimanale o il backup mensile senza configurare la pianificazione personalizzata.

Pianificazione del processo di backup

È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del backup. Un intervallo di tempo valido è dalle 00:00 alle 23:59. Non è possibile specificare un intervallo di tempo come ad esempio dalle 18:00 alle 06:00. In tali casi, si devono specificare manualmente due intervalli di tempo diversi.

Per ogni intervallo di tempo l'ora di inizio è inclusa e l'ora di fine è esclusa. Ad esempio, si è configurato il backup incrementale da eseguire ogni ora tra le 06:00 e le 09:00 e il backup inizierà alle 06:00. Ciò significa che il backup verrà eseguito alle 06:00, alle 07:00 e 08:00, ma NON alle 09:00.

Nota: Se si desidera eseguire il processo di backup ripetutamente fino al termine della giornata, impostare la pianificazione fino alle 00:00. Ad esempio, per eseguire un processo di backup ogni 15 minuti per l'intera giornata, impostare la pianificazione dalle 00:00 alle 00:00 ogni 15 minuti.

Pianificazione del limite delle risorse di backup

La pianificazione del limite delle risorse di backup consente di controllare la velocità effettiva di backup, che a sua volta controlla l'utilizzo delle risorse (I/O del disco, CPU, larghezza di banda della rete) del server di cui si esegue il backup. Questo è utile se non si desidera influire sulle prestazioni del server durante i normali orari di ufficio. È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del limite delle risorse di backup. Per ogni intervallo di tempo è possibile specificare un valore, in MB per minuto. Questo valore viene utilizzato per controllare la velocità effettiva di backup. I valori validi sono compresi tra 1 MB/minuto a 99999 MB/minuto.

Se un processo di backup si estende oltre il tempo specificato, il limite della velocità cambia in conformità all'intervallo di tempo specificato. Ad esempio, il limite delle risorse di backup definito è 500 MB/minuto dalle 08:00 alle 20:00 e 2500 MB/minuto dalle 20:00 alle 22:00. Se un processo di backup inizia alle 19:00 e viene eseguito per tre ore, dalle 19:00 alle 20:00 il limite della velocità è pari a 500 MB/minuto e dalle 20:00 alle 22:00 a 2500 MB/minuto.

Se non si definisce alcuna pianificazione del backup e della sua velocità effettiva, il backup viene eseguito il più rapidamente possibile.

Pianificazione di unione

Consente di unire i punti di ripristino in base alla pianificazione fornita.

Considerare i punti seguenti per il processo di unione:

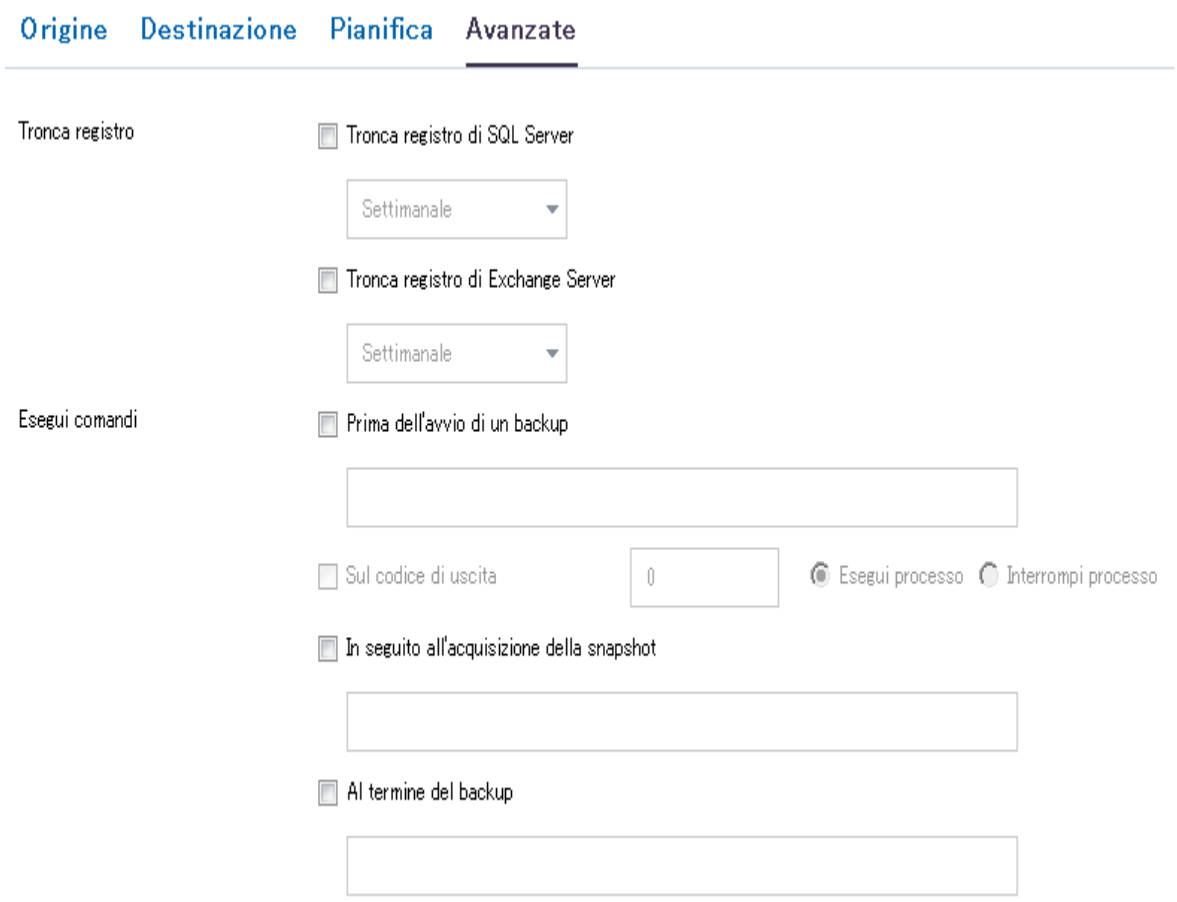
- In qualsiasi momento è possibile eseguire solo un processo di unione per un nodo.
- Se un processo di unione inizia, esso deve essere completato prima di poter avviare il processo di unione successivo. Ciò significa che se uno o più set di punti di ripristino vengono uniti, non è possibile aggiungere nuovi punti di ripristino a questo processo di unione finché il processo di unione dell'insieme corrente dei punti di ripristino non viene completato.

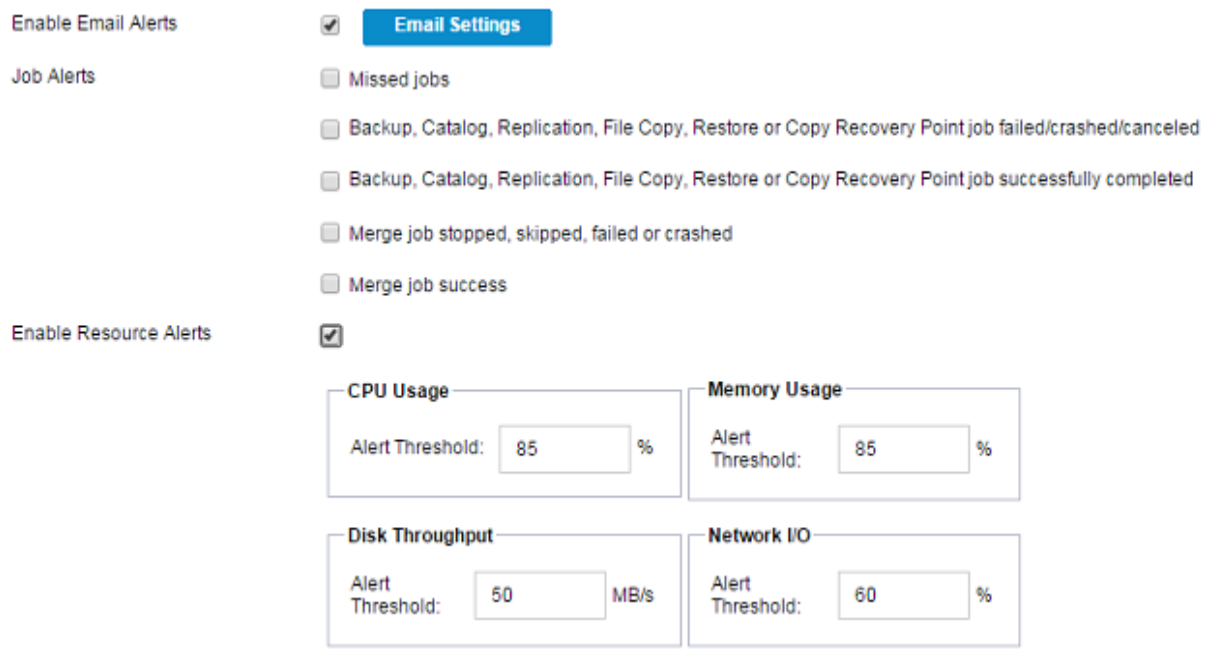
- Se un processo di unione sta elaborando più di un set di punti di ripristino (ad esempio set [1~4], set [5~11] e set [12~14] sono tre set distinti), il Recovery Point Server elabora tali set uno alla volta.
- Se un processo di unione viene ripreso dopo una pausa, il processo individua in quale punto era stato interrotto e riprende l'unione da tale punto.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione delle impostazioni per troncare i registri, l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda Avanzate:





Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

   Tronca registro

   Consente di specificare la pianificazione per troncare i registri per SQL Server ed Exchange Server. È possibile specificare la pianificazione come **Giornaliero**, **Settimanale** o **Mensile**.

   Nome utente

   Consente di specificare l'utente autorizzato per l'esecuzione di uno script.

   Password

   Consente di specificare la password dell'utente autorizzato all'esecuzione dello script.

   Esegui un comando prima dell'avvio del backup

   Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Esegui processo** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

   Esegui un comando dopo l'acquisizione della snapshot

Consente di eseguire uno script dopo l'acquisizione della snapshot del backup. Specificare il percorso di archiviazione dello script.

Esegui un comando al completamento del backup

Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso di archiviazione dello script.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere mediante posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

Abilita avvisi sulle risorse

Consente di specificare una soglia per Utilizzo CPU, Memoria, Velocità del disco, I/O di rete. È possibile fornire il valore in percentuale. Si riceve un messaggio di posta elettronica al superamento del valore Soglia di avviso.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su Salva.

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: Se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo.

Il piano di backup viene creato e distribuito automaticamente al nodo di origine. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

Aggiunta di un'attività di copia dei punti di ripristino al piano

L'attività Copia punti di ripristino copia i punti di ripristino dalla destinazione di backup nel cloud, in una cartella condivisa o in un volume locale.

Nota: se è in corso un processo di backup e il piano viene sospeso, il processo di backup verrà interrotto e il processo di copia dei punti di ripristino non verrà avviato. Quando il piano viene ripreso, il processo di copia dei punti di ripristino non viene ripreso automaticamente. Per attivare il processo di copia dei punti di ripristino è necessario eseguire un altro processo di backup manualmente.

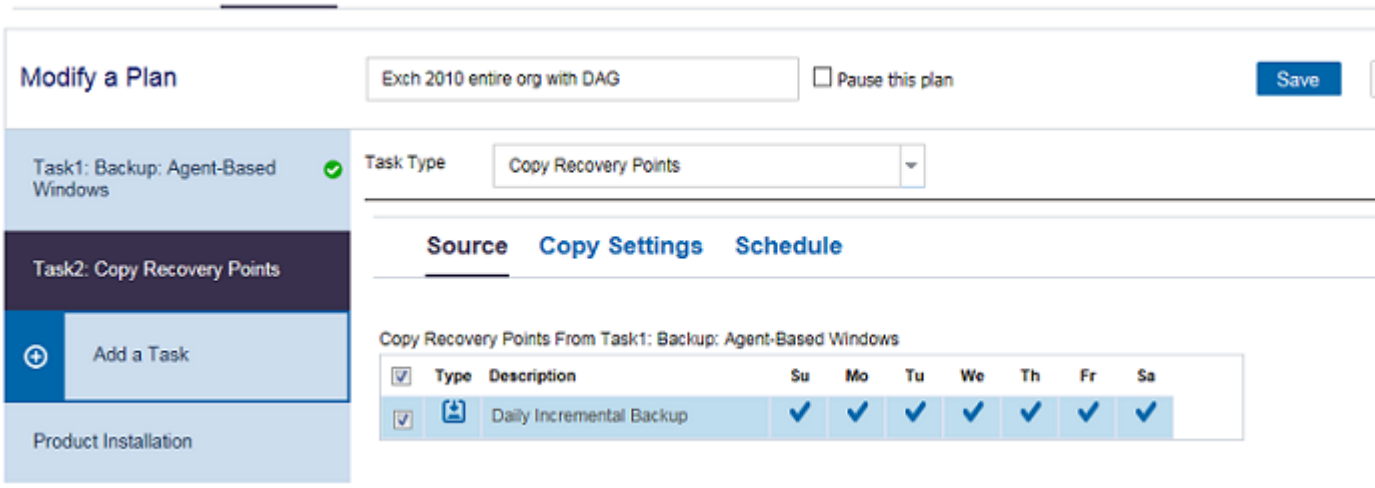
Effettuare le operazioni seguenti:

1. Nel riquadro a sinistra, fare clic su **Aggiungi un'attività**.

   Viene aggiunta una nuova attività al riquadro sinistro.

2. Dal menu a discesa **Tipo di attività**, selezionare **Copia punti di ripristino**.

   L'attività Copia punti di ripristino viene aggiunta. Non è necessario configurare la scheda **Origine** nell'attività Copia punti di ripristino (CRP). Inoltre, è possibile visualizzare la destinazione di backup dall'attività Backup.



Nota: È possibile configurare il percorso di copia del punto di ripristino in una posizione personalizzata utilizzando la chiave del Registro di sistema seguente.

Percorso: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession*

Nome chiave: *LocalTempPath*

Tipo di chiave: *REG_SZ (stringa)*

Valore chiave: *"Local_disk_path"*

3. Dalla scheda Origine, selezionare una pianificazione.
4. Nella scheda Impostazioni di copia, fornire i seguenti dettagli:

Tipo di destinazione

Specifica il tipo di destinazione. È possibile selezionare una delle opzioni disponibili dall'archiviazione cloud, da un disco locale o da una cartella condivisa. Non è possibile scegliere un server RPS come tipo di destinazione.

Disco locale o cartella condivisa

È necessario immettere i dettagli per la destinazione.

Destinazione

Specifica la destinazione in cui si desidera conservare la copia dei punti di ripristino.

Nota: Fare clic sulla freccia per convalidare la destinazione specificata. La freccia viene visualizzata con l'immissione della destinazione.

Archiviazione cloud

Selezionare il servizio cloud e aggiungere un'archiviazione cloud.

Per informazioni dettagliate sulla struttura di directory, consultare la sezione Struttura delle directory dei punti di ripristino nel bucket cloud S3.

Servizio cloud

Consente di selezionare una delle opzioni tra i vari servizi di archiviazione disponibili.

Archiviazione cloud

Consente di selezionare l'account cloud del servizio di archiviazione selezionato. Se l'elenco a discesa non contiene account, fare clic su **Aggiungi** per aggiungerne uno.

Abilita blocco degli oggetti

Consente di proteggere l'archiviazione cloud utilizzando la funzionalità Blocco oggetti. Quando si seleziona il seguente servizio cloud, viene visualizzata la casella di controllo Abilita blocco degli oggetti.

- Amazon S3
- Wasabi Hot Cloud Storage
- Nutanix Objects

Quando si seleziona la casella di controllo **Abilita blocco degli oggetti**, il pulsante Impostazioni di blocco degli oggetti viene abilitato. È necessario configurare le impostazioni di blocco degli oggetti dopo aver abilitato la casella di controllo Blocco degli oggetti. Per ulteriori informazioni sulla configurazione delle impostazioni di blocco degli oggetti, consultare la sezione Configurazione delle impostazioni di blocco degli oggetti per un servizio cloud.

Note:

- Per Amazon S3 e Wasabi Hot Cloud Storage:
  - È possibile attivare l'opzione di blocco per gli oggetti solo per i nuovi bucket.
  - Durante la modifica di un piano, considerare quanto segue:
    - Se un piano viene creato con il blocco degli oggetti abilitato, la casella di controllo *Abilita blocco degli oggetti* è disabilitata e il pulsante *Impostazioni di blocco oggetto degli oggetti* è abilitato. È possibile modificare la modalità e il periodo di conservazione utilizzando il pulsante *Impostazioni di blocco degli oggetti*.
    - Se un piano viene creato con il blocco degli oggetti disattivato, la casella di controllo *Abilita blocco degli oggetti* e il pulsante *Impostazioni di blocco degli oggetti sono disattivati*.
- Per Nutanix Objects:
  - È possibile attivare l'opzione di blocco degli oggetti per i bucket vecchi e nuovi.
  - Durante la modifica di un piano, considerare quanto segue:
    - Se un piano viene creato con il blocco degli oggetti abilitato, non è possibile disattivare la casella di controllo *Abilita blocco degli oggetti*. È possibile aumentare il periodo di conservazione solo utilizzando il pulsante *Impostazioni di blocco degli oggetti*.
    - Se un piano viene creato con il blocco degli oggetti disattivato, è possibile attivare la casella di controllo *Abilita blocco degli oggetti* e configurare le impostazioni di blocco degli oggetti.

- Quando si attiva l'opzione di blocco degli oggetti, le impostazioni di conservazione nella scheda Pianificazione non sono applicabili.

Compressione

Specifica la selezione di un livello di compressione per le copie dei punti di ripristino. La compressione consente solitamente di ridurre l'utilizzo dello spazio su disco. Tuttavia, può avere un effetto inverso e ridurre la velocità di backup a causa dell'aumento dell'utilizzo della CPU. Le opzioni disponibili sono:

Nessuna compressione - Non viene eseguito alcun tipo di compressione. I file sono di tipo VHD. L'opzione determina un utilizzo minimo della CPU (velocità massima) e un utilizzo massimo dello spazio su disco per la creazione dell'immagine di backup.

Nessuna compressione - VHD - Non viene eseguito alcun tipo di compressione. I file verranno convertiti direttamente in .vhd senza dover ricorrere ad operazioni manuali. L'opzione determina un utilizzo minimo della CPU (velocità massima) e un utilizzo massimo dello spazio su disco per la creazione dell'immagine di backup.

Compressione standard - Comporta un livello medio di compressione. Questa opzione fornisce un buon bilanciamento tra l'utilizzo della CPU e dello spazio su disco. Si tratta dell'impostazione predefinita.

Compressione massima - Verrà applicata la massima compressione. L'opzione implica un utilizzo massimo di CPU (velocità minima) ma utilizza anche una quantità minore di spazio su disco per l'immagine di backup.

Nota: Se l'immagine di backup contiene dati non comprimibili (ad esempio, immagini .jpg, file .zip, ecc.), potrebbe essere necessario allocare ulteriore spazio per la gestione di tali dati. Di conseguenza, se si seleziona una qualsiasi opzione di compressione e il backup contiene dati non comprimibili, l'utilizzo di spazio su disco potrebbe aumentare.

Algoritmo di crittografia

Specifica il tipo di algoritmo di crittografia utilizzato per le copie del punto di ripristino. Le opzioni di formato disponibili sono Nessuna crittografia, AES-128, AES-192 e AES-256.

Password di crittografia

Specifica di fornire una password di crittografia che verrà utilizzata per crittografare la sessione di destinazione. Quando si esegue il ripristino dalle copie dei punti di ripristino, si deve fornire questa password per confermare l'autenticazione.

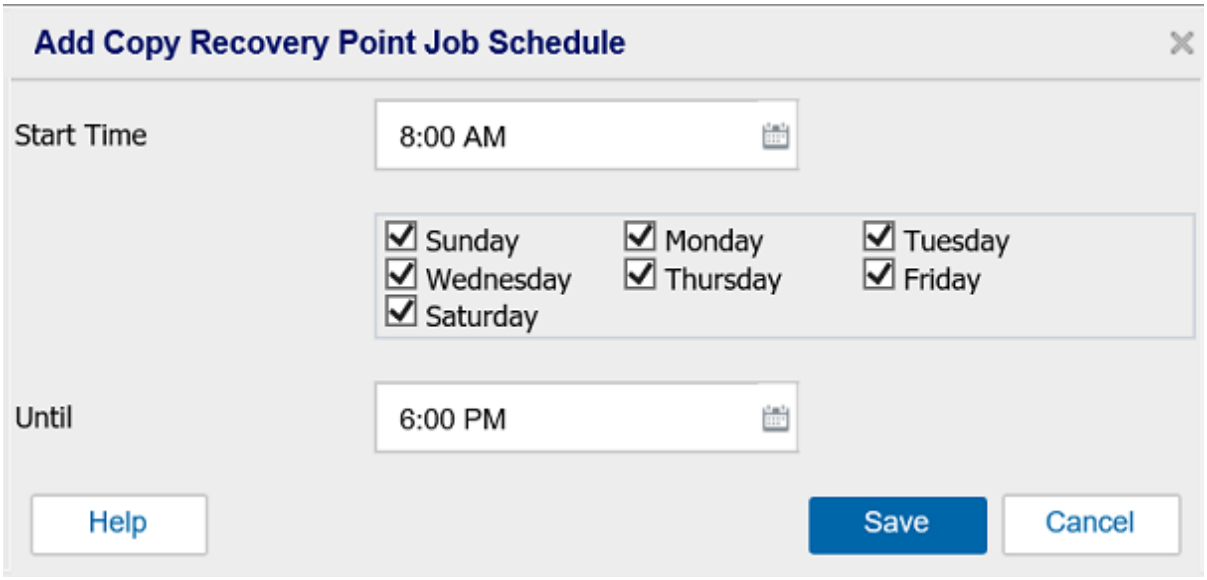
Conferma password di crittografia

Specifica di reimmettere la password.

5. Fare clic sulla scheda **Pianificazione** e specificare la pianificazione del processo.

   Se si utilizza l'opzione di pianificazione, è possibile aggiungere più pianificazioni per un punto di ripristino. Tenere inoltre presenti le seguenti considerazioni:

   - Se non viene configurata alcuna pianificazione, il processo Copia punti di ripristino viene eseguito immediatamente in seguito al completamento del processo di backup.
   - È inoltre possibile configurare il processo Copia punti di ripristino per l'ora di inizio e l'ora di fine.



   - Il processo Copia punti di ripristino verifica sempre la sessione disponibile per l'orario specificato.
   - Se durante l'orario specificato è disponibile una sessione di backup configurata nella scheda Origine, il processo Copia punti di ripristino copia la sessione della destinazione corrispondente.
   - È inoltre possibile configurare i punti di conservazione su base giornaliera, settimanale o mensile.

   Nota: Il numero di backup completati viene contato per ogni backup giornaliero, settimanale e mensile configurato.

6. Fare clic su **Salvare le modifiche**.

   Le modifiche vengono salvate e l'attività Copia punti di ripristino viene distribuita automaticamente al nodo.

   Il piano Copia punti di ripristino è stato creato e distribuito correttamente.

Configurazione delle impostazioni di blocco degli oggetti per un Servizio cloud

Questa sezione fornisce informazioni su come configurare le impostazioni di blocco degli oggetti per un Servizio cloud:

Effettuare le operazioni seguenti:

1. Selezionare la casella di controllo Abilita blocco degli oggetti.

   Il pulsante Impostazioni di blocco degli oggetti è abilitato.

2. Fare clic sul pulsante Impostazioni di blocco degli oggetti.

   Viene visualizzata la finestra di dialogo Impostazioni di blocco degli oggetti.

3. Nella finestra di dialogo Impostazioni di blocco degli oggetti, eseguire le seguenti operazioni:

   Nota: nella finestra di dialogo Impostazioni di blocco degli oggetti, le opzioni possono variare in base al servizio cloud selezionato durante la creazione di un piano.

   Amazon S3

   Modalità di conservazione predefinita

   Consente di attivare diversi livelli di protezione sulle versioni degli oggetti. Per attivarla, selezionare una delle seguenti opzioni:

   - **Governance**: se si dispone di autorizzazioni IAM speciali durante il periodo di conservazione, è possibile sovrascrivere o eliminare le versioni degli oggetti protetti oppure modificare le impostazioni di blocco.
   - **Conformità**: non è possibile sovrascrivere o eliminare le versioni degli oggetti protetti anche nel caso di un utente root nell'account AWS.

   Periodo di conservazione predefinito

   Consente di specificare un intervallo di tempo fisso per la protezione delle versioni degli oggetti. È possibile specificare il periodo di conservazione in giorni o anni.

   Wasabi Hot Cloud Storage

   Modalità di conservazione predefinita

   Consente di attivare diversi livelli di protezione sulle versioni degli oggetti. Per attivarla, selezionare una delle seguenti opzioni:

- **Governance**: se si dispone di autorizzazioni IAM speciali durante il periodo di conservazione, è possibile sovrascrivere o eliminare le versioni degli oggetti protetti oppure modificare le impostazioni di blocco.
- **Conformità**: non è possibile sovrascrivere o eliminare le versioni degli oggetti protetti anche nel caso di un utente root nell'account AWS.

Periodo di conservazione predefinito

Consente di specificare un intervallo di tempo fisso per la protezione delle versioni degli oggetti. È possibile specificare il periodo di conservazione in giorni o anni.

Nutanix Objects

Periodo di conservazione predefinito

Consente di specificare un intervallo di tempo fisso per la protezione delle versioni degli oggetti. È possibile specificare il periodo di conservazione in giorni o anni.

Nota: quando il blocco degli oggetti è abilitato durante la creazione di un piano per Nutanix Objects, vengono abilitati anche i seguenti elementi:

- **Write-Once-Read-Many (WORM)**: non è possibile sovrascrivere o eliminare gli oggetti esistenti per un periodo di conservazione specificato.
- **Controllo delle versioni**: è possibile conservare più versioni di Nutanix Objects in un bucket.

4. Fare clic su **OK**.

Struttura delle directory dei punti di ripristino nel bucket cloud/contenitore

Tutti i punti di ripristino dei nodi con un singolo piano CRP e un account cloud (creati nella console di gestione di Arcserve) come destinazione vengono archiviati in un bucket cloud.

Di seguito è riportata la struttura della directory dei punti di ripristino nel bucket cloud/contenitore:

arcserve-{random-generated-id}-<BucketName>

ca_root_arcserve-recovery-points_<NodeName1>

Set0

<YYYY-MM-DD_HH-MM-SS_<ScheduleType>>

<NodeName1>

<YYYY-MM-DD_HH-MM-SS_<ScheduleType>>

<NodeName1>

.....

<YYYY-MM-DD_HH-MM-SS_<ScheduleType>>

<NodeName1>

ca_root_arcserve-recovery-points_<NodeName2>

.....

ca_root_arcserve-recovery-points_<NodeNameN>

Note:

- Le modifiche al nuovo prefisso arcserve-{random-generated-id}- non hanno effetto sui piani esistenti.
- Il prefisso arcserve-{random-generated-id}- viene aggiunto al nome del bucket configurato nell'account cloud.
- Il nome del nodo è simile a quello visualizzato nella destinazione di backup.
- YYYY-MM-DD: Formato di data (Y: anno, M: mese, D: giorno)
- HH-MM-SS: Formato di ora (H: ore, M: minuti, S: secondi)
- <ScheduleType> indica il tipo di pianificazione di backup e si riferisce a una delle seguenti opzioni:

  - Giornaliero: punto di ripristino di backup giornaliero
  - Settimanale: punto di ripristino di backup settimanale
  - Mensile: punto di ripristino di backup mensile
  - Personalizzato: punto di ripristino caricato utilizzando l'opzione Carica punto di ripristino su cloud (copia ad hoc del punto di ripristino)

- I punti di ripristino dei nodi con lo stesso nome vengono archiviati all'interno della stessa directory se sono destinati allo stesso account cloud. Di conseguenza, si consiglia di utilizzare account cloud diversi per i nodi con lo stesso nome in modo da archiviarli in bucket differenti.

Verifica del piano

Per verificare la funzionalità Copia punti di ripristino, confermare di aver creato correttamente il piano. Dopo avere verificato che il piano è stato creato correttamente, verificare se il processo di backup sia in esecuzione in base alla pianificazione. Dopo la corretta conclusione del processo di backup, viene eseguito il processo Copia punti di ripristino. È possibile verificare lo stato del processo di backup e del processo Copia punti di ripristino dalla scheda **Jobs** (Processi).

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Seguire questi passaggi per verificare i processi Copia punti di ripristino:

1. Fare clic sulla scheda **Jobs** (Processi).
2. Dal riquadro sinistro, fare clic su **Tutti i Processi**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare la corretta esecuzione del processo di backup e del processo Copia punti di ripristino.

Creazione di un piano di copia file

Arcserve Unified Data Protection consente di copiare o spostare i file di origine selezionati in una destinazione. La destinazione può essere un'archiviazione cloud o una rete condivisa. Il file di origine deve provenire dallo stesso volume di cui è già stato eseguito il backup. Ad esempio, è stato eseguito il backup dell'intero volume D:\ del nodo di origine. Si desidera copiare un file specifico dal volume D:\ del nodo di origine. È possibile creare un'attività di copia file per eseguire questa operazione.

È possibile utilizzare l'opzione Copia file per eseguire la copia di dati critici in posizioni secondarie o come soluzione di archiviazione.

Vantaggi della copia file:

- Maggior efficienza: i processi di backup e di ripristino vengono eseguiti più rapidamente mediante la copia e lo spostamento dei dati non modificati, riducendo in tal modo il volume dei dati reali per cui è necessario eseguire il backup e l'archiviazione su nastro o su disco.
- Conformità normativa: consente di conservare documenti, messaggi di posta elettronica e altri dati critici in conformità con i regolamenti interni ed esterni.
- Riduzione dei costi di archiviazione: consente di recuperare la capacità di archiviazione mediante la migrazione dei dati meno recenti o dei dati usati raramente contenuti nei sistemi primari su percorsi di archiviazione più adeguati.
- Gestione di più versioni file: consente di risalire alle versioni precedenti dei file di cui è stato eseguito il backup (se necessario) oppure di gestire più versioni dello stesso file in destinazioni diverse.

Come procedere?

- Verifica dei prerequisiti
- Creazione di un piano con un'attività di backup
- Aggiunta di un'attività di copia file al piano
- (Facoltativo) Esecuzione di una copia file manuale
- Verifica del piano

Verifica delle considerazioni e dei prerequisiti

Verificare se i prerequisiti seguenti sono stati completati:

- Accedere alla console.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Considerazioni:

- Nella tabella seguente sono riportati i limiti per la lunghezza del nome file per un processo di copia file. I file che superano tali limiti vengono ignorati.

Destinazione	Limite
Condivisione di rete	240
Cloud	245

- Se è in esecuzione la copia file da una sessione replicata e l'*origine* di replica comprende più sessioni di backup, il processo di copia file viene eseguito separatamente per ciascuna sessione. Ad esempio, se sono disponibili **cinque** *sessioni di backup* nella destinazione di backup e si aggiunge un'attività di replica, questa esegue la replica di tutte le sessioni di backup in *un unico processo*. A questo punto, se si aggiunge un'attività di copia file e l'origine di copia file corrisponde alla destinazione di replica, vengono eseguiti **cinque** *processi di copia file* per replicare ogni sessione.

Creazione di un piano con un'attività di backup

Un piano include diversi tipi di attività da eseguire. Per creare un'attività Copia file, prima si deve disporre di un punto di ripristino valido. Per ottenere un punto di ripristino valido, è necessario creare un'attività di backup.

Un'attività di backup esegue un backup dei nodi di origine e archivia i dati nella destinazione specificata. L'attività Copia file è supportata solo per il backup Windows basato su agente. La procedura seguente illustra le fasi per creare l'attività di backup Windows basata su agente.

Effettuare le operazioni seguenti:

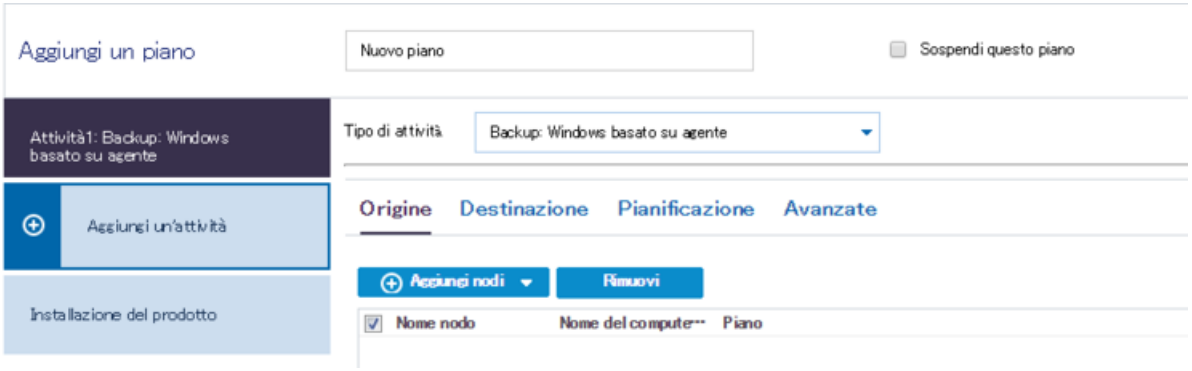
1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la finestra di dialogo **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa **Tipo di attività**, selezionare **Backup, Windows basato su agente**.



Specificare i dettagli Origine, Destinazione, Pianificazione e Impostazioni avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine che si desidera proteggere. È possibile selezionare più di un nodo per un piano. Se non sono stati aggiunti nodi alla console, è possibile aggiungerli in fase di creazione o modifica di un piano dalla pagina Origine. È inoltre possibile salvare un piano senza aggiungere nessun nodo di origine. Il piano viene distribuito soltanto dopo l'aggiunta dei nodi di origine.

Effettuare le operazioni seguenti:

1. Nella scheda Origine, fare clic su **Aggiungi**.
2. Selezionare una delle seguenti opzioni:

   Selezionare i nodi da proteggere in Arcserve UDP

   Consente di visualizzare la finestra di dialogo Selezionare i nodi da proteggere in Arcserve UDP. Selezionare i nodi dall'elenco visualizzato. Selezionare questa opzione se sono stati già aggiunti nodi alla Console.

   Aggiungi nodo Windows

   Viene visualizzata la finestra di dialogo Aggiungi nodi a un piano. Selezionare questa opzione se non sono stati aggiunti nodi e si desidera aggiungere manualmente i nodi da proteggere.

   Rileva nodi da Active Directory

   Consente di aprire la finestra di dialogo Aggiungi nodi alla Console Arcserve UDP. Selezionare questa opzione se si desidera rilevare e aggiungere nodi da Active Directory.

3. Se è stata selezionata l'opzione **Selezionare i nodi da proteggere in Arcserve UDP**, nella finestra di dialogo Selezionare i nodi da proteggere, procedere come segue:

   a. (Facoltativo) Selezionare un filtro dall'elenco a discesa Gruppi per filtrare i nodi. Immettere parole chiave per applicare ulteriori filtri ai nodi.

      I nodi vengono visualizzati nella colonna Nodi disponibili.

   b. Selezionare i nodi dalla colonna Nodi disponibili, quindi fare clic sulla freccia destra singola (>) o sulla freccia destra doppia (>>) per spostare rispettivamente i nodi selezionati o tutti i nodi nella colonna Nodi selezionati.

      I nodi vengono visualizzati nella colonna Nodi selezionati.

   c. Fare clic su **OK** per chiudere la finestra di dialogo.



4. Per scegliere il Tipo di protezione, selezionare una delle seguenti opzioni:

   Backup di tutti i volumi

   Prepara una snapshot del backup di tutti i volumi.

   Backup dei volumi selezionati

   Prepara una snapshot del backup del volume selezionato.

   L'origine viene specificata.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Selezionare un **Tipo di destinazione** tra quelli elencati di seguito:

   Disco locale o cartella condivisa

   Specifica che la destinazione di backup è una destinazione locale o una cartella condivisa. Se si seleziona questa opzione, è possibile salvare i dati come punti di ripristino o set di ripristino. Le opzioni dei punti di ripristino e dei set di ripristino sono disponibili nella scheda **Pianificazione.**

   Recovery Point Server di Arcserve UDP

   Specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono memorizzati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.

2. Se è stato selezionato il **Recovery Point Server di Arcserve UDP**, immettere i seguenti dettagli:
   a. Selezionare un Recovery Point Server.
   b. Selezionare un archivio dati. L'elenco mostra tutti gli archivi dati creati sul Recovery Point Server specificato.
   c. Fornire una password di sessione.
   d. Confermare la password di sessione.
3. Se è stata selezionata l'opzione **Utilizza il disco locale o la cartella condivisa**, fornire i dettagli seguenti:
   a. Fornire il percorso completo della destinazione locale o di rete. Per la destinazione di rete, specificare le credenziali con l'accesso di scrittura.
   b. Selezionare l'algoritmo di crittografia. Per ulteriori informazioni, consultare la sezione Impostazioni di crittografia.
   c. Facoltativamente, fornire una password di crittografia.
   d. Confermare la password di crittografia.
   e. Selezionare un tipo di compressione. Per ulteriori informazioni, consultare la sezione Tipo di compressione.

Nota: Se si archiviano i dati in un disco locale o in una cartella condivisa, non è possibile replicare i dati in un altro Recovery Point Server. La replica è supportata solo se si archiviano i dati in un Recovery Point Server.

La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

Effettuare le operazioni seguenti:

1. (Facoltativo) Selezionare l'opzione per la gestione dei punti di ripristino. Questa opzione è visibile solamente se sono state selezionate le cartelle Locale o Condivisa come destinazione di backup.

   Conserva per punti di ripristino

   I dati di backup vengono archiviati come punti di ripristino.

   Conserva per set di ripristino

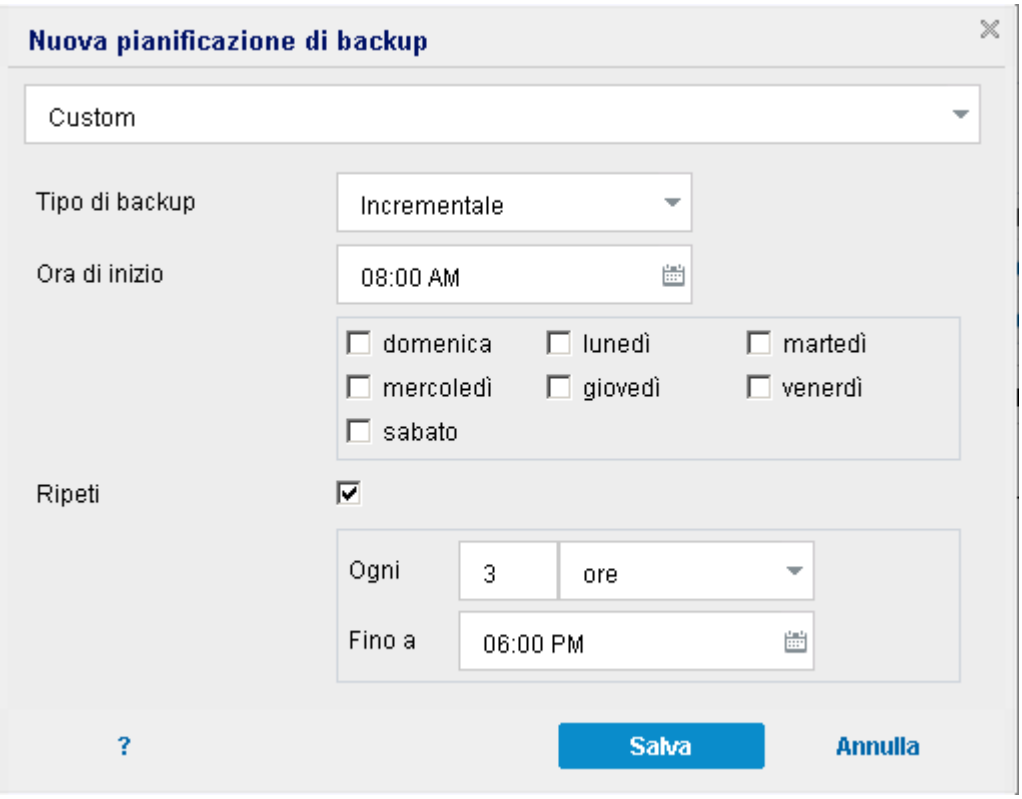
   I dati di backup vengono archiviati come set di ripristino.

2. Aggiungere le pianificazioni di backup, di unione e di definizione del limite di velocità

   Aggiunta di una pianificazione di backup

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base

alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni di backup.

Verifica

Specifica la pianificazione dei backup di verifica.

Arcserve UDP controlla che i dati protetti siano validi e completi eseguendo una verifica di affidabilità dell'immagine di backup archiviata sull'origine di backup. Se necessario esegue la risincronizzazione dell'immagine. Un backup di verifica controlla il backup più recente di ogni blocco e lo confronta con il contenuto e le informazioni di origine. Questo confronto consente di verificare che le informazioni corrispondenti all'origine siano contenute nel blocco di backup più recente. Se l'immagine di backup di un blocco non corrisponde all'origine (probabilmente a causa di modifiche apportate al sistema dall'ultimo backup), Arcserve UDP aggiorna (risincronizza) il backup del blocco non corrispondente. Sebbene si tratti di una procedura poco frequente, il backup di verifica può essere utilizzato per ottenere le stesse garanzie di un backup completo, ma senza occupare lo stesso spazio.

Vantaggi: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.

Svantaggi: il backup di verifica richiede tempi di esecuzione più lunghi, in quanto esegue il confronto di tutti i blocchi originali con i blocchi del backup più recente.

Incrementale

Specifica la pianificazione dei backup incrementali.

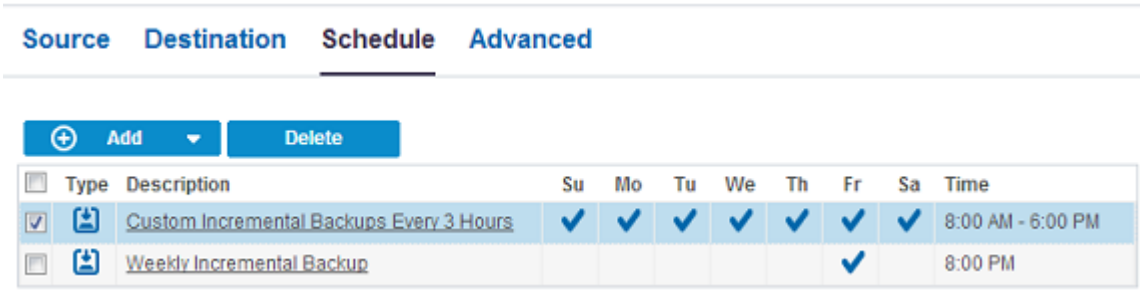
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su Aggiungi e selezionare Aggiungi pianificazione di unione.

   La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

b. Specificare l'ora di inizio per l'avvio del processo di unione.

c. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

d. Fare clic su **Salva**.

   La Pianificazione di unione viene specificata e visualizzata nella pagina **Pianificazione.**

Aggiungi pianificazione del limite delle risorse

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

   Viene visualizzata la finestra di dialogo Aggiungi nuova pianificazione del limite delle risorse.

b. Specificare il limite di velocità effettiva in MB per unità di minuti.

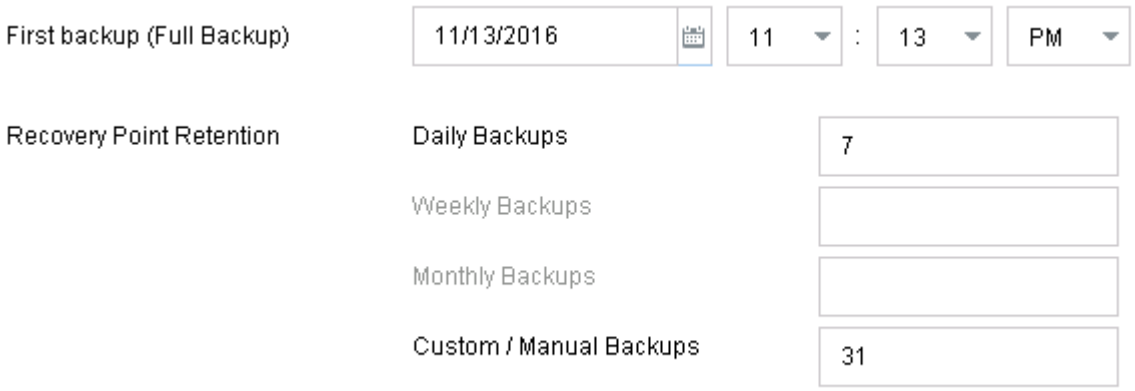
c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

   La pianificazione del limite delle risorse specificata viene visualizzata nella pagina **Pianificazione**.

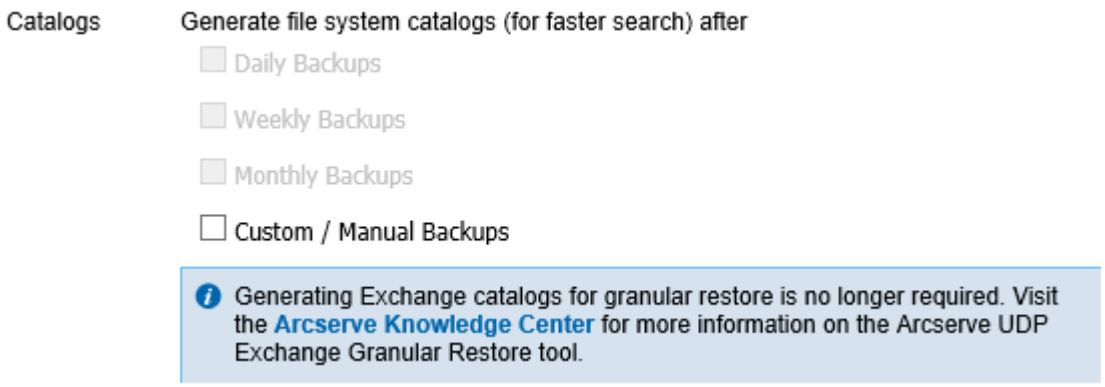
3. Specificare l'ora di inizio per il backup pianificato.



4. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo Pianificazione di backup.

5. Specificare i dettagli relativi al catalogo.



   I cataloghi permettono di generare il catalogo file system. Il catalogo file system è necessario per migliorare e velocizzare la ricerca. Se si selezionano le caselle di controllo del catalogo, i cataloghi verranno abilitati in base al tipo di backup specificato. Deselezionare una casella di controllo per disattivare la generazione del catalogo.

   Viene specificata la pianificazione.

Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione

L'opzione di pianificazione consente di specificare una pianificazione personalizzata o una pianificazione giornaliera/settimanale/mensile o entrambe. Nella pianificazione personalizzata è possibile configurare la pianificazione del backup per ciascun giorno della settimana e aggiungere fino a quattro pianificazioni di backup ogni giorno. È possibile selezionare un giorno specifico di una settimana e creare un intervallo di tempo per definire quando eseguire il backup e la frequenza.

Pianificazione	Processo supportato	Commenti
Backup	Processo di backup	Definire gli intervalli di tempo per eseguire i processi di backup.
Limitazione della velocità di backup	Processo di backup	Definire gli intervalli di tempo per controllare la velocità di backup.
Unione	Processo di unione	Definire quando unire i processi.
Pianificazione quotidiana	Processo di backup	Definire quando eseguire processi di backup quotidiani.
Pianificazione settimanale	Processo di backup	Definire quando eseguire processi di backup settimanali.
Pianificazione mensile	Processo di backup	Definire quando eseguire processi di backup mensili.

È inoltre possibile specificare le impostazioni di memorizzazione per i punti di ripristino.

Nota: All'interno di ogni piano è necessario configurare le impostazioni di conservazione per controllare il modo in cui i nodi assegnati a tale piano vengono memorizzati nell'archivio dati di destinazione.

Le pianificazioni per i backup giornalieri/settimanali/mensili sono indipendenti dalla pianificazione personalizzata e gli uni dagli altri. È possibile configurare di eseguire solo il backup giornaliero, il backup settimanale o il backup mensile senza configurare la pianificazione personalizzata.

Pianificazione del processo di backup

È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del backup. Un intervallo di tempo valido è dalle 00:00 alle 23:59. Non è possibile specificare un intervallo di tempo come ad esempio dalle 18:00 alle 06:00. In tali casi, si devono specificare manualmente due intervalli di tempo diversi.

Per ogni intervallo di tempo l'ora di inizio è inclusa e l'ora di fine è esclusa. Ad esempio, si è configurato il backup incrementale da eseguire ogni ora tra le 06:00 e le 09:00 e il backup inizierà alle 06:00. Ciò significa che il backup verrà eseguito alle 06:00, alle 07:00 e 08:00, ma NON alle 09:00.

Nota: Se si desidera eseguire il processo di backup ripetutamente fino al termine della giornata, impostare la pianificazione fino alle 00:00. Ad esempio, per eseguire un processo di backup ogni 15 minuti per l'intera giornata, impostare la pianificazione dalle 00:00 alle 00:00 ogni 15 minuti.

Pianificazione del limite delle risorse di backup

La pianificazione del limite delle risorse di backup consente di controllare la velocità effettiva di backup, che a sua volta controlla l'utilizzo delle risorse (I/O del disco, CPU, larghezza di banda della rete) del server di cui si esegue il backup. Questo è utile se non si desidera influire sulle prestazioni del server durante i normali orari di ufficio. È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del limite delle risorse di backup. Per ogni intervallo di tempo è possibile specificare un valore, in MB per minuto. Questo valore viene utilizzato per controllare la velocità effettiva di backup. I valori validi sono compresi tra 1 MB/minuto a 99999 MB/minuto.

Se un processo di backup si estende oltre il tempo specificato, il limite della velocità cambia in conformità all'intervallo di tempo specificato. Ad esempio, il limite delle risorse di backup definito è 500 MB/minuto dalle 08:00 alle 20:00 e 2500 MB/minuto dalle 20:00 alle 22:00. Se un processo di backup inizia alle 19:00 e viene eseguito per tre ore, dalle 19:00 alle 20:00 il limite della velocità è pari a 500 MB/minuto e dalle 20:00 alle 22:00 a 2500 MB/minuto.

Se non si definisce alcuna pianificazione del backup e della sua velocità effettiva, il backup viene eseguito il più rapidamente possibile.

Pianificazione di unione

Consente di unire i punti di ripristino in base alla pianificazione fornita.

Considerare i punti seguenti per il processo di unione:

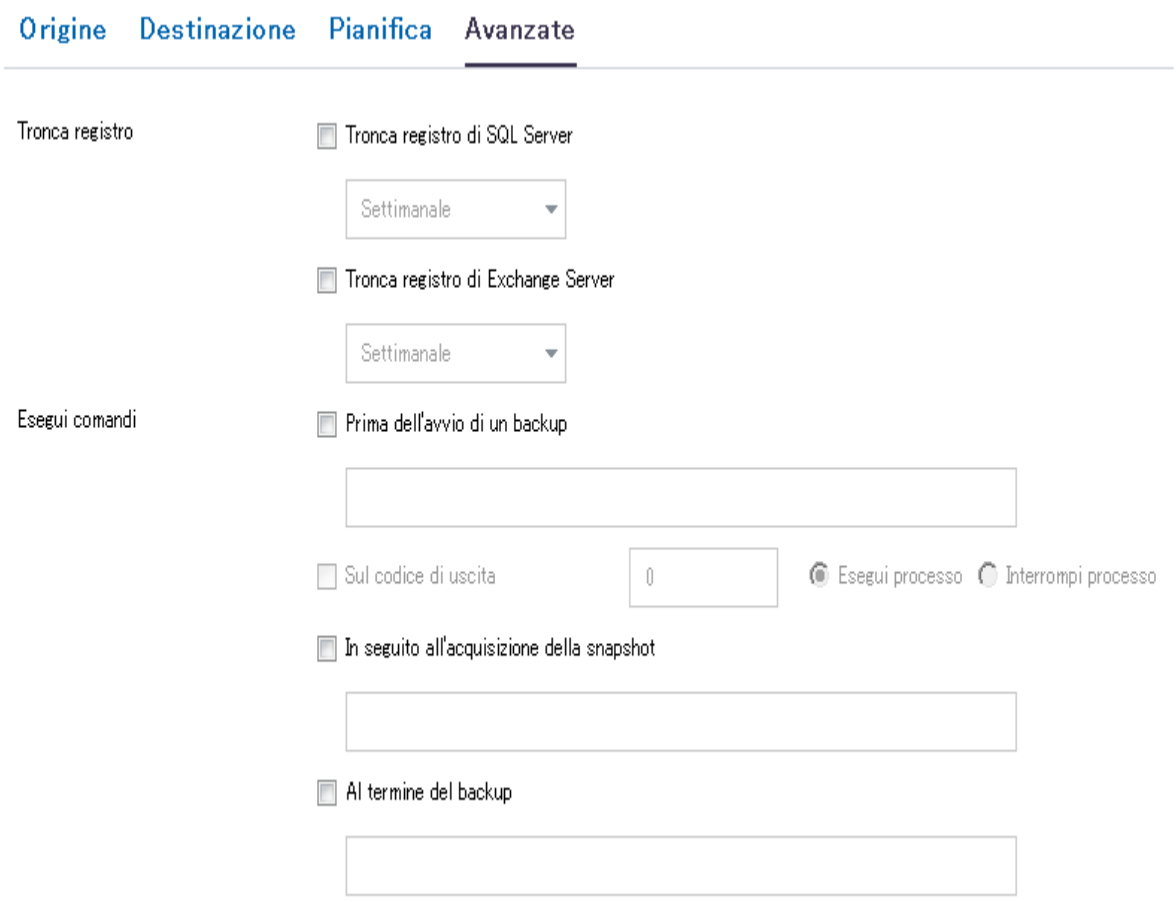
- In qualsiasi momento è possibile eseguire solo un processo di unione per un nodo.
- Se un processo di unione inizia, esso deve essere completato prima di poter avviare il processo di unione successivo. Ciò significa che se uno o più set di punti di ripristino vengono uniti, non è possibile aggiungere nuovi punti di ripristino a questo processo di unione finché il processo di unione dell'insieme corrente dei punti di ripristino non viene completato.

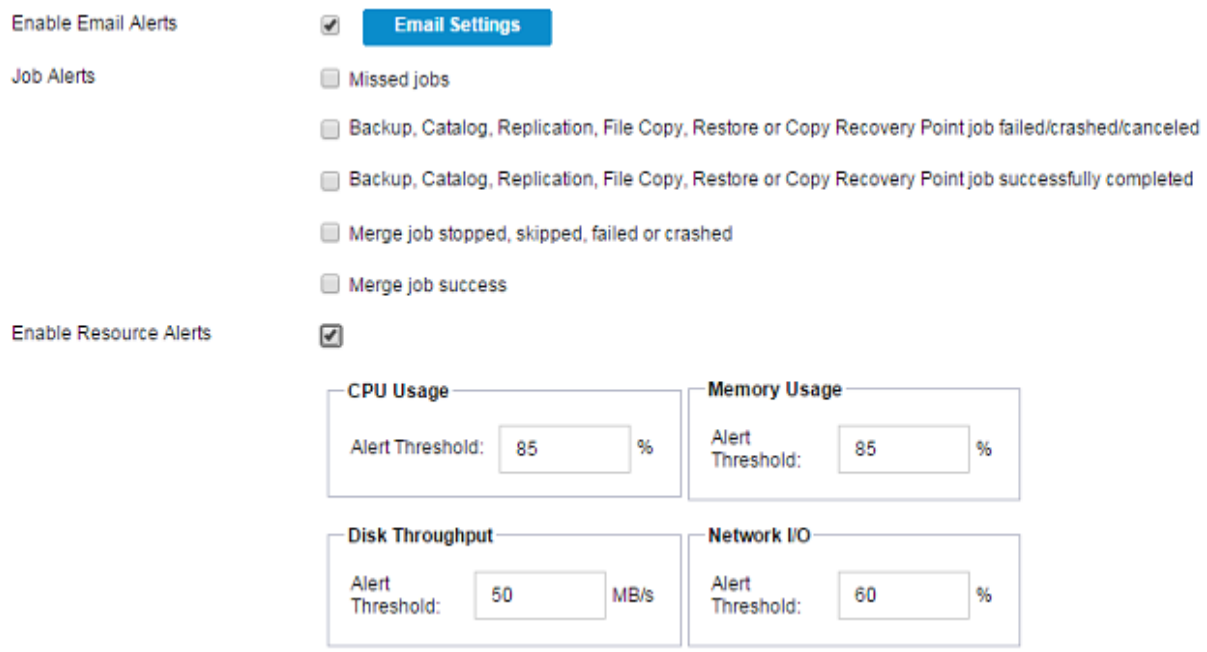
- Se un processo di unione sta elaborando più di un set di punti di ripristino (ad esempio set [1~4], set [5~11] e set [12~14] sono tre set distinti), il Recovery Point Server elabora tali set uno alla volta.
- Se un processo di unione viene ripreso dopo una pausa, il processo individua in quale punto era stato interrotto e riprende l'unione da tale punto.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione delle impostazioni per troncare i registri, l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda Avanzate:





Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

   Tronca registro

   Consente di specificare la pianificazione per troncare i registri per SQL Server ed Exchange Server. È possibile specificare la pianificazione come **Giornaliero**, **Settimanale** o **Mensile**.

   Nome utente

   Consente di specificare l'utente autorizzato per l'esecuzione di uno script.

   Password

   Consente di specificare la password dell'utente autorizzato all'esecuzione dello script.

   Esegui un comando prima dell'avvio del backup

   Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Esegui processo** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

   Esegui un comando dopo l'acquisizione della snapshot

Consente di eseguire uno script dopo l'acquisizione della snapshot del backup. Specificare il percorso di archiviazione dello script.

Esegui un comando al completamento del backup

Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso di archiviazione dello script.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere mediante posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

Abilita avvisi sulle risorse

Consente di specificare una soglia per Utilizzo CPU, Memoria, Velocità del disco, I/O di rete. È possibile fornire il valore in percentuale. Si riceve un messaggio di posta elettronica al superamento del valore Soglia di avviso.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su Salva.

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: Se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo.

Il piano di backup viene creato e distribuito automaticamente al nodo di origine. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

Aggiunta di un'attività di copia file al piano

L'attività Copia file consente di copiare singoli file nella destinazione specificata. La copia originale viene memorizzata dopo aver copiato i file nella destinazione specificata. Il processo di copia file non dipende dai processi di catalogo. Se la destinazione di backup è un archivio dati di deduplicazione o di non deduplicazione, la cartella Catalogo viene spostata nella destinazione di backup. Il processo di catalogo è compreso nel processo di copia file. Il processo di copia file viene eseguito sul Recovery Point Server per consentire a Arcserve UDP di eseguire l'offload dell'attività degli agenti.

Arcserve UDP supporta la copia file da un archivio dati di deduplicazione.

Verifica preliminare per i nodi Copia file: è inoltre possibile eseguire la verifica preliminare per la copia di file. Solo i nodi che sono stati aggiunti per la copia file sono idonei per la verifica preliminare. Per eseguire la verifica preliminare per la copia file, fare clic con il pulsante destro del mouse sul nodo da Tutti i nodi e selezionare Verifica preliminare di copia file.

Nota: se è in corso un processo di backup e il piano viene sospeso, il processo di backup verrà interrotto e il processo di copia file non verrà avviato. Quando il piano viene ripreso, il processo di copia file non viene ripreso automaticamente. Per avviare il processo di copia file è necessario eseguire un altro processo di backup manualmente.

Effettuare le operazioni seguenti:

1. Fare clic su **Aggiungi un'attività** dal riquadro sinistro.

   Viene aggiunta una nuova attività al riquadro sinistro.

2. Dal menu a discesa **Tipo di attività**, selezionare **Copia file**.

   L'attività Copia file viene aggiunta.

3. Fare clic sulla scheda **Origine** e specificare i dettagli.

   Origine punti di ripristino per copia file

   Consente di selezionare l'origine dei punti di ripristino. Se è presente una sola origine, questa viene visualizzata automaticamente. Se sono presenti più origini, è necessario selezionare l'origine corretta dall'elenco a discesa.

   Tipi di punti di ripristino

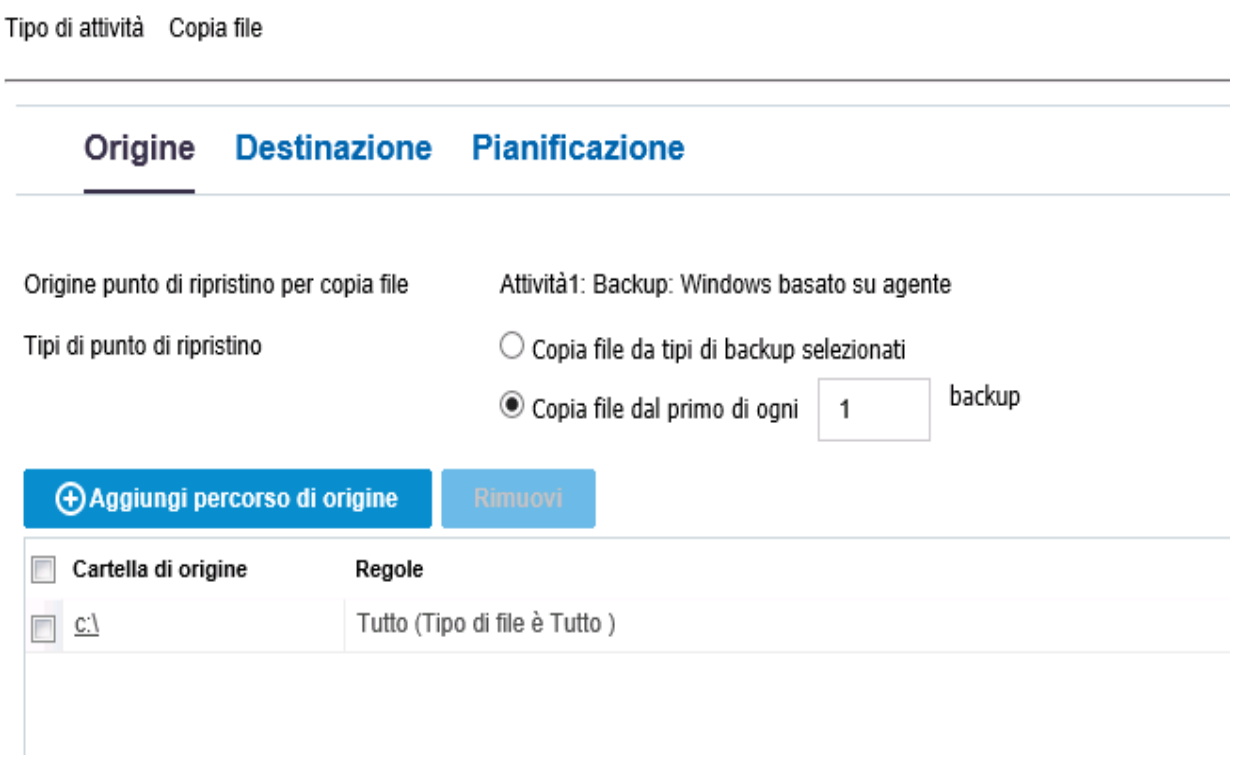
   Consente di selezionare i punti di ripristino per la copia file. È possibile selezionare una delle due opzioni seguenti:

   Copia file da tipi di backup selezionati

È possibile selezionare **Backup giornalieri**, **Backup settimanali** e **Backup mensili**. Le opzioni relative alla frequenza giornaliera, settimanale o mensile sono abilitate in base alla pianificazione del backup di origine. Ad esempio, se per il backup di origine è pianificato soltanto un backup mensile, per l'opzione **Copia file da tipi di backup selezionati** sono attivi soltanto i **backup mensili**.

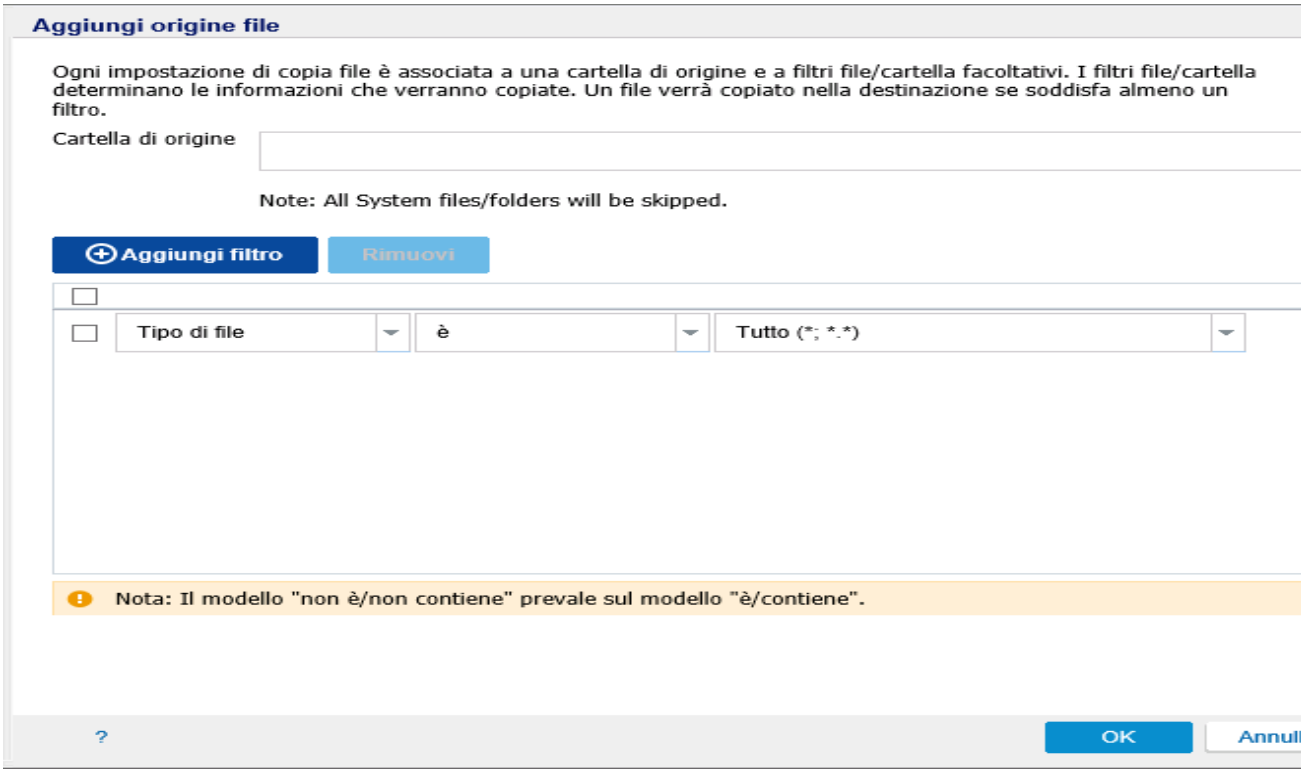
Copia file dal primo di ogni backup

È possibile specificare il numero di backup che si desidera copiare. Ad esempio, se si specifica 3, viene copiato il terzo backup. Il processo di copia file supporta fino a 700 punti di ripristino da cui avviare la copia.



4. Fare clic su **Aggiungi percorso di origine**.

   Viene visualizzata la finestra di dialogo **Aggiungi origine file**.



È possibile evitare l'omissione delle directory di sistema di Windows (C:\Windows) e dei programmi (C:\Programmi, C:\Programmi (x86)) utilizzando la seguente configurazione:

Aggiungere il seguente tag XML se non ancora presente, oppure aggiornarlo nel file FileCopyDebugSetting.xml dalla directory $UDPHome\Engine\Configuration:

<SkipWindowsFolders>0</SkipWindowsFolders>

Il file XML avrà l'aspetto seguente:

<?xml version="1.0" encoding="UTF-8"?>

<HKLM>

<AFArchiveDLL>

.....

<SkipWindowsFolders>0</SkipWindowsFolders>

</AFArchiveDLL>

</HKLM>

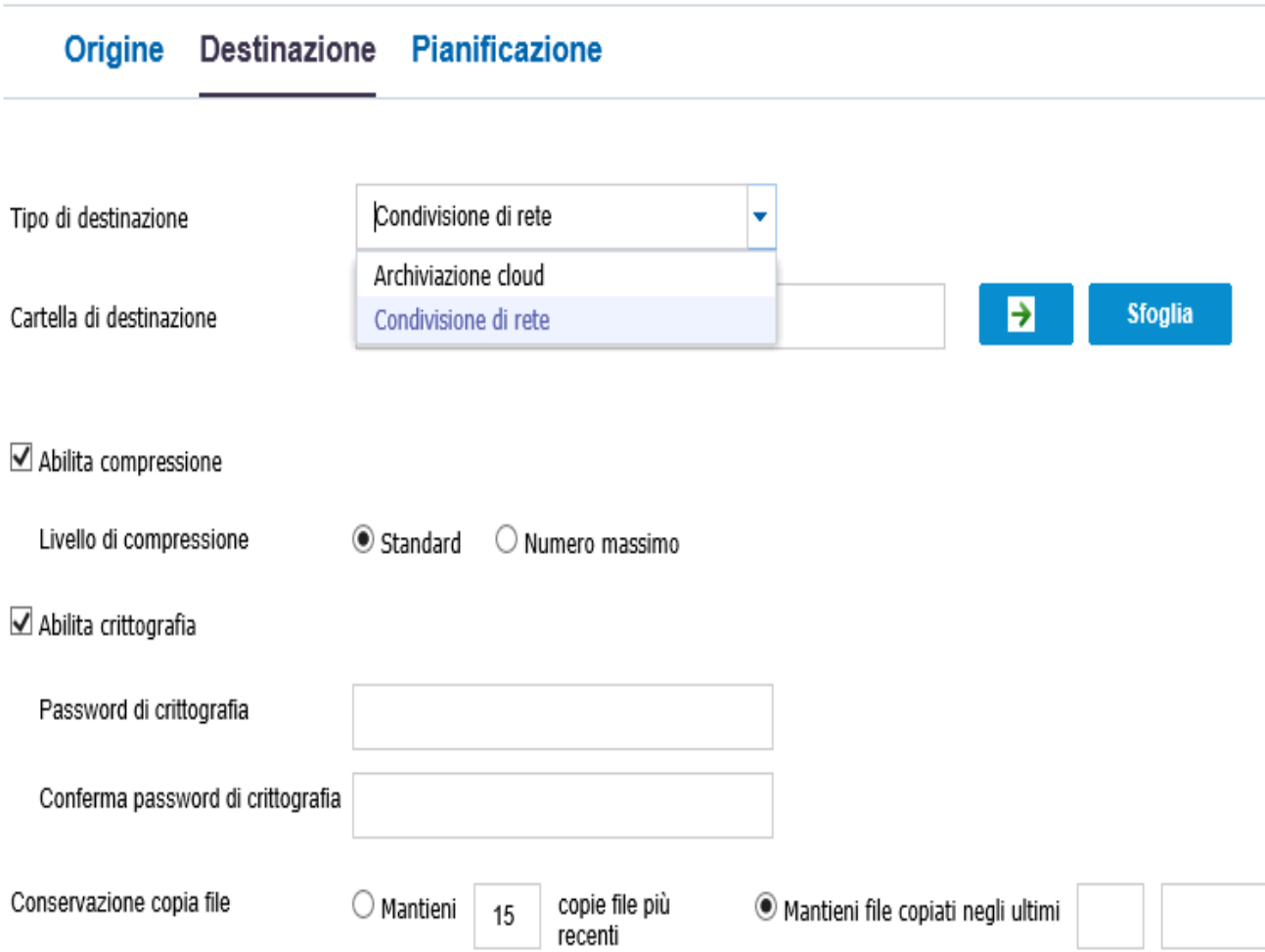
5. Specificare il percorso della cartella di origine che si desidera copiare.
6. Fare clic su **Aggiungi filtro**.

Il filtro viene aggiunto sotto al pulsante **Aggiungi filtro.** È possibile aggiungere e rimuovere più filtri. Per ulteriori informazioni, consultare la sezione relativa all'aggiunta dei filtri di copia file.

7. Selezionare il filtro dall'elenco e fare clic su **OK**.

   La finestra di dialogo **Aggiungi origine file** viene chiusa.

8. Fare clic sulla scheda **Destinazione** e specificare i dettagli della destinazione.



Tipo di destinazione

Specifica che il tipo di destinazione è una condivisione di rete o un'archiviazione cloud. Per entrambe le opzioni di destinazione, se la connessione alla destinazione specificata viene persa o interrotta, Arcserve UDP esegue più tentativi di completamento del processo di copia file. Nel caso in cui non sia possibile completare il processo, viene eseguito un processo di riparazione a partire dal punto in cui si è verificato l'errore. Inoltre, il registro attività viene aggiornato con il messaggio di errore corrispondente e viene inviata una notifica di posta elettronica (se configurata).

Condivisione di rete

Specifica che la destinazione è una cartella condivisa. Se selezionata, questa opzione consente di specificare il percorso completo della posizione in cui si desidera spostare o copiare i file o le cartelle di origine.

Cartella di destinazione

Specifica la destinazione in cui vengono archiviati i file copiati. La destinazione può corrispondere a un volume o a una cartella locale oppure a una condivisione file accessibile mediante un percorso conforme al formato UNC (Uniform Naming Convention). Questo campo è disponibile quando si seleziona Condivisione di rete come tipo di destinazione. È anche possibile cercare la cartella di destinazione.

Archiviazione cloud

Specifica che sono i file copiati vengono archiviati in un ambiente cloud. Arcserve UDP attualmente supporta la copia di file su più fornitori cloud, come Amazon S3 (Simple Storage Service), le versioni compatibili con Amazon S3, Windows Azure, le versioni compatibili con Windows Azure, Eucalyptus-Walrus e FUJITSU Hybrid IT Service FJcloud-O. Questi fornitori cloud sono servizi Web disponibili al pubblico che consentono di archiviare e recuperare qualsiasi quantità di dati in qualsiasi momento da ogni punto del Web in un ambiente protetto e sicuro.

Nota: per eliminare eventuali errori di sfasamento orario durante la connessione all'ambiente cloud, verificare sul computer in uso che il fuso orario sia stato impostato correttamente e che l'orologio sia sincronizzato con l'orario globale. Si consiglia di confrontare l'ora del computer con l'ora GMT. Se l'orario del computer in uso non è sincronizzato con l'ora globale corretta (con uno scarto di 5-10 minuti), non sarà possibile utilizzare la connessione cloud. Se necessario, reimpostare l'ora corretta per il computer ed eseguire di nuovo il processo di copia file.

Periferica di archiviazione

Selezionare il tipo di periferica dall'elenco a discesa.



Archiviazione cloud

Selezionare il percorso di archiviazione cloud dall'elenco a discesa. L'elenco a discesa è disponibile se i dettagli di archiviazione cloud sono stati specificati. Se si specifica l'account di archiviazione cloud per la prima volta, fare clic su Aggiungi per aggiungere l'account cloud. Se si seleziona Archiviazione cloud dalla volta successiva, l'account viene visualizzato nell'elenco a discesa Archiviazione cloud.

Nota: Per ulteriori informazioni sull'aggiunta di un account cloud, consultare la sezione Aggiunta account cloud.

Compressione

Specifica il tipo di compressione da utilizzare per i processi di copia file.

Generalmente, la compressione viene utilizzata per ridurre lo spazio di archiviazione nella destinazione di copia file, tuttavia comporta la riduzione della velocità di copia file a causa del maggiore utilizzo della CPU.

Nota: per i processi di copia file compressi, il registro attività visualizza solamente la dimensione non compressa.

Le opzioni disponibili sono:

Compressione standard

Verrà eseguito un certo livello di compressione. L'opzione determina un equilibrio di utilizzo della CPU e dello spazio di archiviazione richiesto. Si tratta dell'impostazione predefinita.

Compressione massima

Verrà eseguita la compressione massima. L'opzione determina un utilizzo massimo della CPU (velocità minima) e un utilizzo minimo dello spazio di archiviazione per la copia file.

Enable Encryption (Abilita crittografia)

Specifica l'utilizzo della crittografia per la copia file.

La crittografia dei dati corrisponde alla conversione di dati in un modulo incomprensibile senza un meccanismo di decifratura. La protezione dei dati di Arcserve UDP utilizza algoritmi di crittografia AES-256 (Advanced Encryption Standard) per ottenere la massima protezione e riservatezza dei dati. Nel caso in cui venga selezionata l'opzione di crittografia, è necessario specificare e confermare una password di crittografia.

Nota: Se si modifica un'attività di copia file, non è possibile modificare la crittografia o la compressione.

Conservazione file

Conserva i file nella destinazione di copia file se i criteri specificati vengono soddisfatti.

File creati negli ultimi

Specifica la durata (anni, mesi, giorni) di memorizzazione dei dati archiviati nel percorso di destinazione. Al termine del periodo di memorizzazione specificato, i dati archiviati verranno eliminati dalla destinazione.

Importante! Al termine del periodo di conservazione specificato i dati vengono eliminati dalla destinazione. Pertanto, non sarà più possibile archiviare o salvare i dati eliminati.

Nota: il processo di eliminazione del periodo di memorizzazione viene attivato solamente se l'opzione di pianificazione della copia file viene abilitata.

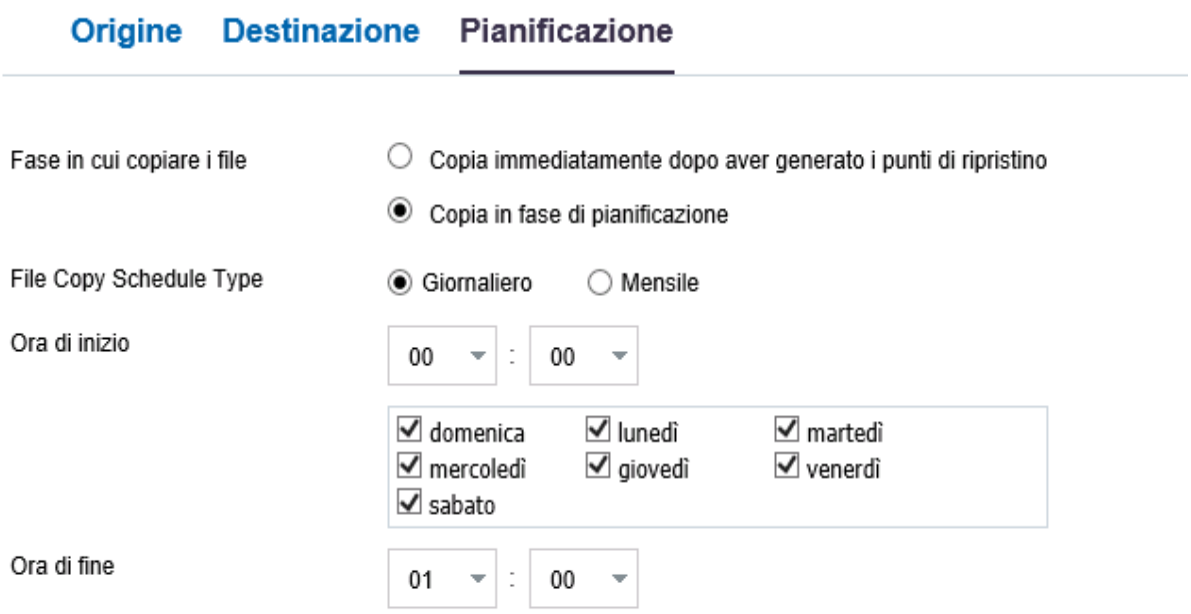
Versione file precedente a

Specifica il numero di copie memorizzate e archiviate nel percorso di destinazione. Quando questo numero viene raggiunto, la versione meno recente viene eliminata. Il processo di eliminazione della versione archiviata meno recente viene ripetuto con l'aggiunta delle nuove versioni alla destinazione mantenendo in questo modo il numero di versioni archiviate specificato.

Ad esempio, se il valore delle versioni di file da memorizzare viene impostato su cinque e vengono eseguite cinque copie del file alle ore t1, t2, t3, t4 e t5, tali versioni costituiscono le cinque copie di file memorizzate e disponibili per il recupero. Quando viene eseguita la sesta copia (con il salvataggio della nuova versione), Arcserve UDP rimuove la copia t1 e le cinque versioni disponibili per il ripristino sono t2, t3, t4, t5 e t6.

Per impostazione predefinita, il numero di copie memorizzate nel percorso di destinazione è 15.

9. Fare clic sulla scheda **Pianificazione** e specificare la pianificazione di copia file.



Se un processo di copia file viene eseguito oltre l'ora di fine, il processo rimane in esecuzione fino al completamento. Il processo di copia file successivo non viene eseguito finché il processo di copia file precedente non è completo, anche se un processo pianificato si sovrappone al processo in esecuzione.

Il processi di copia file viene eseguito come specificato nella pianificazione.

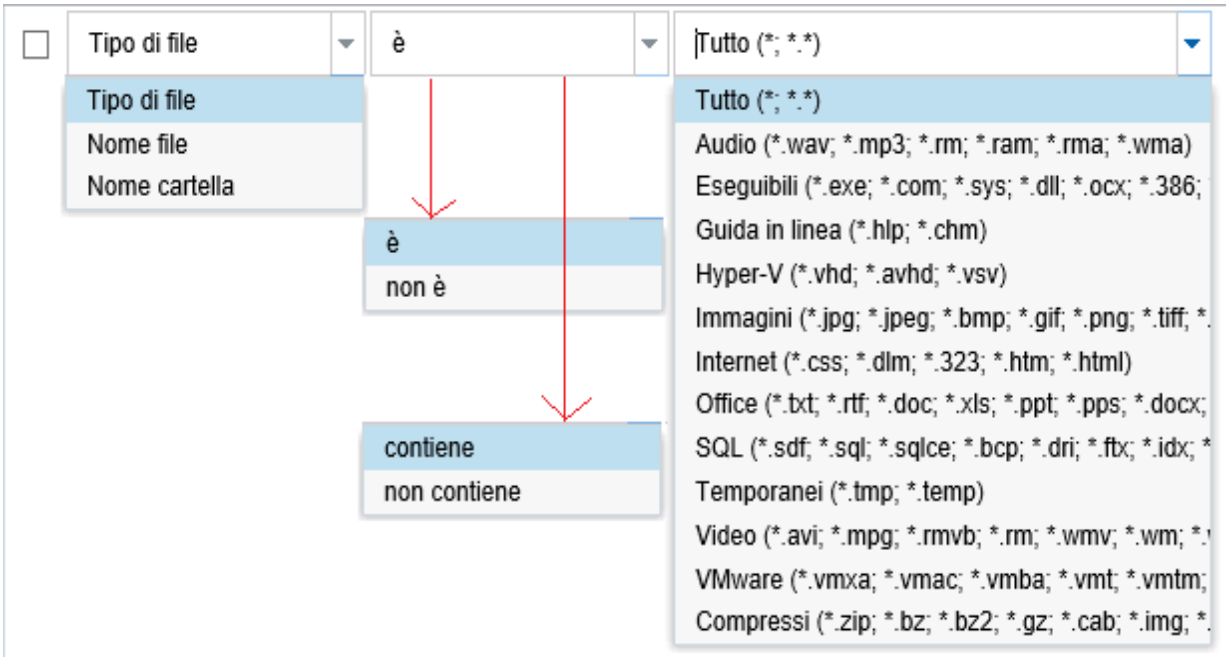
10. Fare clic su **Salva**.

    Le modifiche vengono salvate e l'attività di copia file viene distribuita automaticamente al nodo.

Aggiunta di filtri di copia file

Aggiungi filtro

Consente di aggiungere un filtro. I filtri consentono di limitare il numero di oggetti di copia file ai tipi e valori specificati.



Categoria di filtri

Sono disponibili tre categorie di filtri: **Tipo di file**, **Nome file** e **Nome cartella**. I campi Variabile di filtro e Valore di filtro cambiano in base alla categoria di filtri.

Variabile di filtro

Se la categoria di filtri è **Tipo di file**, le opzioni Variabile di filtro sono **è** e **non è**. Se la categoria di filtri è **Nome file o Nome di cartella**, le opzioni Variabile di filtro sono **contiene** o **non contiene**.

È possibile specificare più filtri all'interno della stessa richiesta di copia file. È possibile specificare la stessa categoria di filtri ma una diversa variabile di filtro.

Nota: Quando si verifica un conflitto relativo alla variabile di filtro per la stessa categoria di filtri, alla variabile **non è** o **non contiene** viene sempre assegnata una priorità più alta e ne viene forzata l'applicazione.

Valore di filtro

Il valore di filtro consente di limitare le informazioni di copia file selezionando solamente le informazioni di parametro specificate, ad esempio file txt.

Arcserve UDP supporta l'utilizzo dei caratteri jolly per la selezione di più oggetti da includere in un'unica richiesta di copia file. Un carattere jolly è un carattere speciale che può essere utilizzato per rappresentare un carattere singolo o una stringa di testo.

Il campo Valore supporta i caratteri asterisco e punto di domanda. Se non si è a conoscenza del valore completo del criterio file/cartella, è possibile semplificare i risultati del filtro specificando un carattere jolly.

"*": utilizzare l'asterisco per sostituire uno, nessuno o più caratteri del valore.

"?" : utilizzare il punto interrogativo per sostituire un carattere del valore.

Ad esempio, immettere * .txt per escludere tutti i file con estensione .txt, nel caso in cui non si conosca il nome di un file specifico. È possibile specificare il nome parzialmente ed utilizzare i caratteri jolly per completare le parti mancanti.

Nota: Se si seleziona **Tipo di file** come tipo di filtro, viene visualizzato un elenco a discesa contenente i filtri predefiniti per i tipi di file più utilizzati (file MS-Office, file Image, file eseguibili, file temporanei ecc.). Dopo aver selezionato uno dei filtri predefiniti, è possibile aggiungere o modificare i valori corrispondenti.

Evitare l'omissione delle cartelle di sistema

Il processo di copia dei file ignora le cartelle di sistema per impostazione predefinita se il processo viene eseguito sui volumi che contengono le cartelle di sistema. Per proteggere tali cartelle e copiarle nella destinazione, è possibile modificare il testo predefinito aggiungendo una voce di configurazione.

Aggiungere la seguente voce tag XML nel file FileCopyDebugSetting.xml dalla directory $UDPHome\Engine\Configuration:

FileName : FileCopyDebugSetting.xml

TagName: SkipWindowsFolders

DefaultValue: 1

Per proteggerle impostare il valore su 0

Nota: questa opzione interessa esclusivamente il processo di copia dei file. L'archiviazione dei file ignora tutte le cartelle di sistema indipendentemente dal valore di TagValue configurato.

(Facoltativo) Esecuzione di una copia file manuale

In genere, la copia file viene eseguita automaticamente ed è controllata dalle relative impostazioni di pianificazione. In aggiunta alla copia file pianificata, quella manuale permette di eseguire la copia dei file importanti a seconda delle proprie esigenze.

Quando si esegue una copia file manuale, il processo corrispondente viene eseguito solo per la prima sessione di backup, qualificato per la copia file. Le sessioni di backup sono adatte per la copia file in base alla pianificazione di backup e se sono incluse in una coda. Ad esempio, se si sceglie di eseguire la copia file per ogni secondo backup, soltanto ogni secondo backup sarà adatto per la copia file, non tutti i backup. Al termine della copia file, la prima sessione viene rimossa e la seconda a seguire diventa la prima. Ad esempio, se sono presenti tre sessioni di backup (S1, S2 ed S3) e si esegue una copia file manuale, il processo di copia file viene eseguito solo per S1. Il processo di copia file non interessa S2 ed S3. Quando si ripete il processo di copia file manuale, verrà copiata S2.

Si può eseguire la copia file manualmente dalle visualizzazioni Nodi e Piani facendo clic sul menu **Azioni** o sul menu di scelta rapida.

Attenersi alla procedura descritta per eseguire la copia file manuale dalla visualizzazione Nodi:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   I nodi vengono visualizzati nel riquadro centrale.
3. Selezionare i nodi per il processo di copia file. I nodi devono disporre di un piano di copia file assegnato.
4. Nel riquadro centrale, fare clic su **Azioni**, **Copia file ora**.

   Viene visualizzata la finestra di dialogo **Run File copy now (Esegui copia file ora)**.
5. Fare clic su **OK**.

   Il processo di copia file viene eseguito.

   La copia file manuale viene completata correttamente.

Verifica del piano

Per verificare il piano di copia file, confermare di aver creato correttamente il piano. Dopo avere verificato che il piano è stato creato correttamente, verificare se il processo di backup sia in esecuzione in base alla pianificazione. In seguito al completamento del processo di backup, il processo di copia file viene eseguito in base alla pianificazione. È possibile verificare lo stato del processo di backup e del processo Copia file dalla scheda **Jobs** (Processi).

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Seguire questi passaggi per verificare i processi Copia file:

1. Fare clic sulla scheda **Jobs** (Processi).
2. Dal riquadro sinistro, fare clic su **Tutti i processi completati**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare la corretta esecuzione del processo di backup e del processo Copia file.

Creazione di un piano di archiviazione file

Arcserve Unified Data Protection consente di archiviare i file di origine selezionati in una destinazione. La destinazione può essere un account cloud o una rete condivisa. Il file di origine deve provenire dallo stesso volume di cui è già stato eseguito il backup. Ad esempio, è stato eseguito il backup dell'intero volume D:\ del nodo di origine. Si desidera copiare un file specifico (ad esempio .htm) dal volume D:\ del nodo di origine. Dopo aver copiato il file, si desidera eliminare tale file dal nodo di origine. È possibile archiviare un piano di copia file per eseguire questa operazione.

L'archiviazione file consente di eliminare in modo sicuro i dati di origine una volta copiati in un repository di archiviazione secondario o remoto.

I vantaggi dell'archiviazione file sono:

- Maggior efficienza: i processi di backup e di ripristino vengono eseguiti più rapidamente mediante l'archiviazione dei dati non modificati, riducendo in tal modo il volume dei dati reali per cui è necessario eseguire il backup e l'archiviazione su nastro o su disco.
- Conformità normativa: consente di conservare documenti, messaggi di posta elettronica e altri dati critici in conformità con i regolamenti interni ed esterni.
- Riduzione dei costi di archiviazione: consente di recuperare la capacità di archiviazione mediante la migrazione dei dati meno recenti o dei dati usati raramente contenuti nei sistemi primari su percorsi di archiviazione più adeguati.
- Gestione di più versioni file: consente di risalire alle versioni precedenti dei file di cui è stato eseguito il backup (se necessario) oppure di gestire più versioni dello stesso file in destinazioni diverse.

Come procedere?

Verifica delle considerazioni e dei prerequisiti

Verificare se i prerequisiti seguenti sono stati completati:

- Accedere alla console.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Tenere presenti le seguenti considerazioni:

- Il processo di archiviazione dei file viene eseguito dalla sessione di backup più recente disponibile.
- Il processo di archiviazione dei file viene eseguito solo una volta al giorno in base alla pianificazione.
- Il processo di eliminazione dell'archiviazione dei file viene eseguito come nuovo processo per l'eliminazione dei file di origine.
- Nella tabella seguente sono riportati i limiti per la lunghezza del nome file per un processo di archiviazione dei file. I file che superano tali limiti vengono ignorati.

Destinazione	Limite
Condivisione di rete	240
Cloud	245

Creazione di un piano con un'attività di backup

Un piano include diversi tipi di attività da eseguire. Per creare un'attività di archiviazione file, è necessario prima disporre di un punto di ripristino valido. Per ottenere un punto di ripristino valido, è necessario creare un'attività di backup.

Un'attività di backup esegue un backup dei nodi di origine e archivia i dati nella destinazione specificata. L'archiviazione file è supportata solo per il backup Windows basato su agente. La procedura seguente illustra le fasi per creare l'attività di backup Windows basata su agente.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

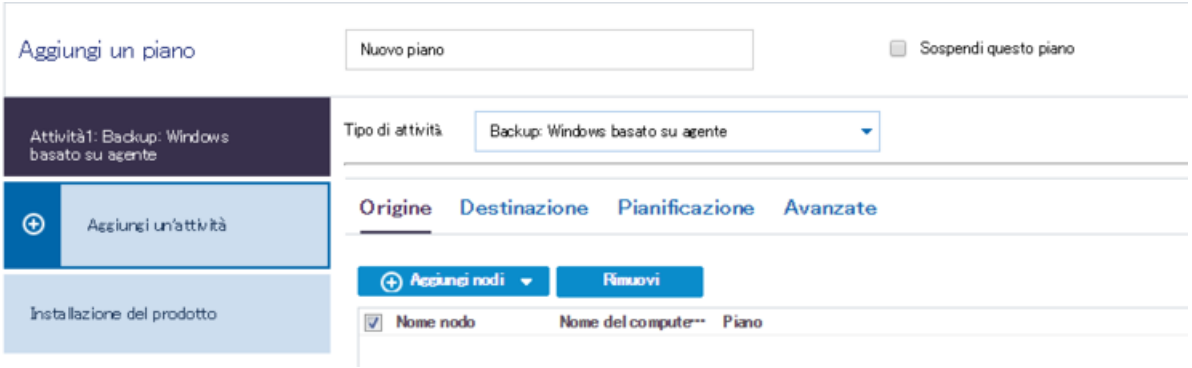
   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la finestra di dialogo **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa **Tipo di attività**, selezionare **Backup, Windows basato su**

agente.



Specificare i dettagli Origine, Destinazione, Pianificazione e Impostazioni avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine che si desidera proteggere. È possibile selezionare più di un nodo per un piano. Se non sono stati aggiunti nodi alla console, è possibile aggiungerli in fase di creazione o modifica di un piano dalla pagina Origine. È inoltre possibile salvare un piano senza aggiungere nessun nodo di origine. Il piano viene distribuito soltanto dopo l'aggiunta dei nodi di origine.

Effettuare le operazioni seguenti:

1. Nella scheda Origine, fare clic su **Aggiungi**.
2. Selezionare una delle seguenti opzioni:

   Selezionare i nodi da proteggere in Arcserve UDP

   Consente di visualizzare la finestra di dialogo Selezionare i nodi da proteggere in Arcserve UDP. Selezionare i nodi dall'elenco visualizzato. Selezionare questa opzione se sono stati già aggiunti nodi alla Console.

   Aggiungi nodo Windows

   Viene visualizzata la finestra di dialogo Aggiungi nodi a un piano. Selezionare questa opzione se non sono stati aggiunti nodi e si desidera aggiungere manualmente i nodi da proteggere.

   Rileva nodi da Active Directory

   Consente di aprire la finestra di dialogo Aggiungi nodi alla Console Arcserve UDP. Selezionare questa opzione se si desidera rilevare e aggiungere nodi da Active Directory.
3. Se è stata selezionata l'opzione **Selezionare i nodi da proteggere in Arcserve UDP**, nella finestra di dialogo Selezionare i nodi da proteggere, procedere come segue:
   a. (Facoltativo) Selezionare un filtro dall'elenco a discesa Gruppi per filtrare i nodi. Immettere parole chiave per applicare ulteriori filtri ai nodi.

      I nodi vengono visualizzati nella colonna Nodi disponibili.

   b. Selezionare i nodi dalla colonna Nodi disponibili, quindi fare clic sulla freccia destra singola (>) o sulla freccia destra doppia (>>) per spostare rispettivamente i nodi selezionati o tutti i nodi nella colonna Nodi selezionati.

      I nodi vengono visualizzati nella colonna Nodi selezionati.

   c. Fare clic su **OK** per chiudere la finestra di dialogo.



4. Per scegliere il Tipo di protezione, selezionare una delle seguenti opzioni:

   Backup di tutti i volumi

   Prepara una snapshot del backup di tutti i volumi.

   Backup dei volumi selezionati

   Prepara una snapshot del backup del volume selezionato.

   L'origine viene specificata.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Selezionare un **Tipo di destinazione** tra quelli elencati di seguito:

   Disco locale o cartella condivisa

   Specifica che la destinazione di backup è una destinazione locale o una cartella condivisa. Se si seleziona questa opzione, è possibile salvare i dati come punti di ripristino o set di ripristino. Le opzioni dei punti di ripristino e dei set di ripristino sono disponibili nella scheda **Pianificazione.**

   Recovery Point Server di Arcserve UDP

   Specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono memorizzati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.

2. Se è stato selezionato il **Recovery Point Server di Arcserve UDP**, immettere i seguenti dettagli:
   a. Selezionare un Recovery Point Server.
   b. Selezionare un archivio dati. L'elenco mostra tutti gli archivi dati creati sul Recovery Point Server specificato.
   c. Fornire una password di sessione.
   d. Confermare la password di sessione.
3. Se è stata selezionata l'opzione **Utilizza il disco locale o la cartella condivisa**, fornire i dettagli seguenti:
   a. Fornire il percorso completo della destinazione locale o di rete. Per la destinazione di rete, specificare le credenziali con l'accesso di scrittura.
   b. Selezionare l'algoritmo di crittografia. Per ulteriori informazioni, consultare la sezione Impostazioni di crittografia.
   c. Facoltativamente, fornire una password di crittografia.
   d. Confermare la password di crittografia.
   e. Selezionare un tipo di compressione. Per ulteriori informazioni, consultare la sezione Tipo di compressione.

Nota: Se si archiviano i dati in un disco locale o in una cartella condivisa, non è possibile replicare i dati in un altro Recovery Point Server. La replica è supportata solo se si archiviano i dati in un Recovery Point Server.

La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

Effettuare le operazioni seguenti:

1. (Facoltativo) Selezionare l'opzione per la gestione dei punti di ripristino. Questa opzione è visibile solamente se sono state selezionate le cartelle Locale o Condivisa come destinazione di backup.

   Conserva per punti di ripristino

   I dati di backup vengono archiviati come punti di ripristino.

   Conserva per set di ripristino

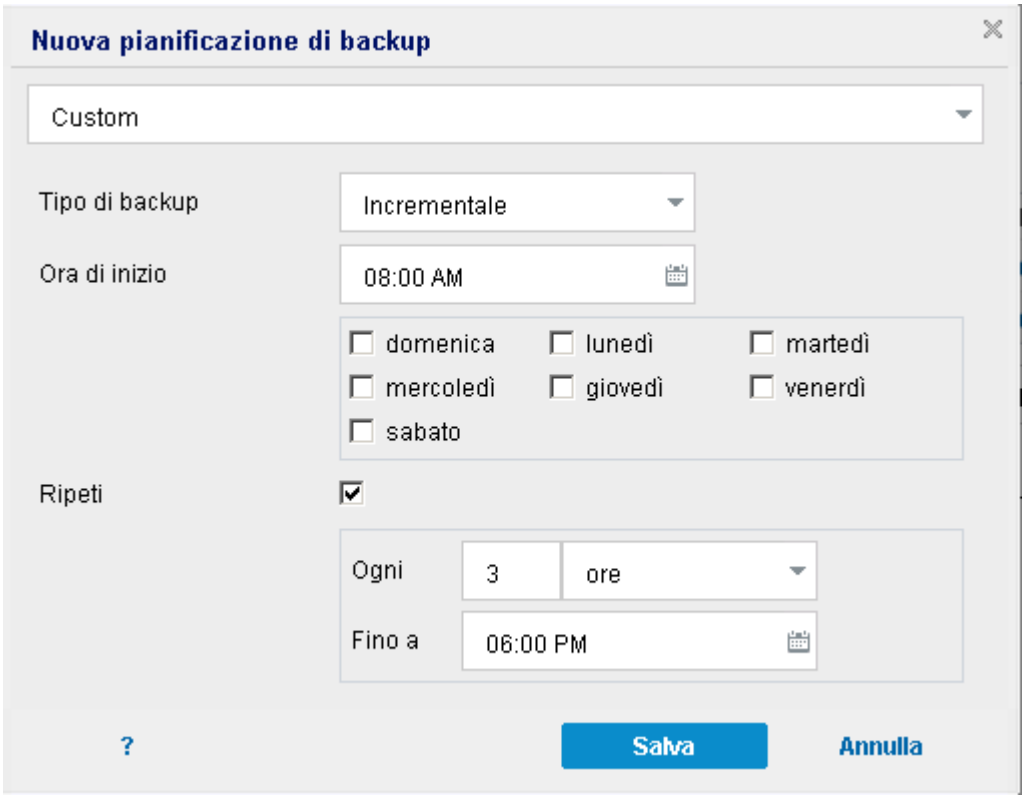
   I dati di backup vengono archiviati come set di ripristino.

2. Aggiungere le pianificazioni di backup, di unione e di definizione del limite di velocità

   Aggiunta di una pianificazione di backup

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base

alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni di backup.

Verifica

Specifica la pianificazione dei backup di verifica.

Arcserve UDP controlla che i dati protetti siano validi e completi eseguendo una verifica di affidabilità dell'immagine di backup archiviata sull'origine di backup. Se necessario esegue la risincronizzazione dell'immagine. Un backup di verifica controlla il backup più recente di ogni blocco e lo confronta con il contenuto e le informazioni di origine. Questo confronto consente di verificare che le informazioni corrispondenti all'origine siano contenute nel blocco di backup più recente. Se l'immagine di backup di un blocco non corrisponde all'origine (probabilmente a causa di modifiche apportate al sistema dall'ultimo backup), Arcserve UDP aggiorna (risincronizza) il backup del blocco non corrispondente. Sebbene si tratti di una procedura poco frequente, il backup di verifica può essere utilizzato per ottenere le stesse garanzie di un backup completo, ma senza occupare lo stesso spazio.

Vantaggi: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.

Svantaggi: il backup di verifica richiede tempi di esecuzione più lunghi, in quanto esegue il confronto di tutti i blocchi originali con i blocchi del backup più recente.

Incrementale

Specifica la pianificazione dei backup incrementali.

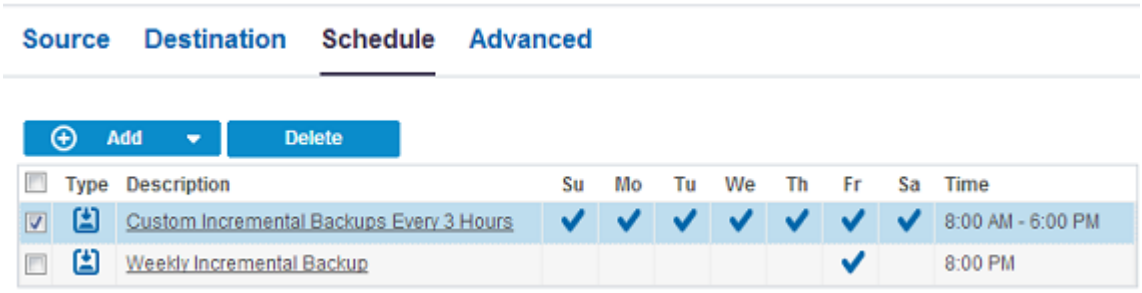
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su Aggiungi e selezionare Aggiungi pianificazione di unione.

   La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

b. Specificare l'ora di inizio per l'avvio del processo di unione.

c. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

d. Fare clic su **Salva**.

   La Pianificazione di unione viene specificata e visualizzata nella pagina **Pianificazione.**

Aggiungi pianificazione del limite delle risorse

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

   Viene visualizzata la finestra di dialogo Aggiungi nuova pianificazione del limite delle risorse.

b. Specificare il limite di velocità effettiva in MB per unità di minuti.

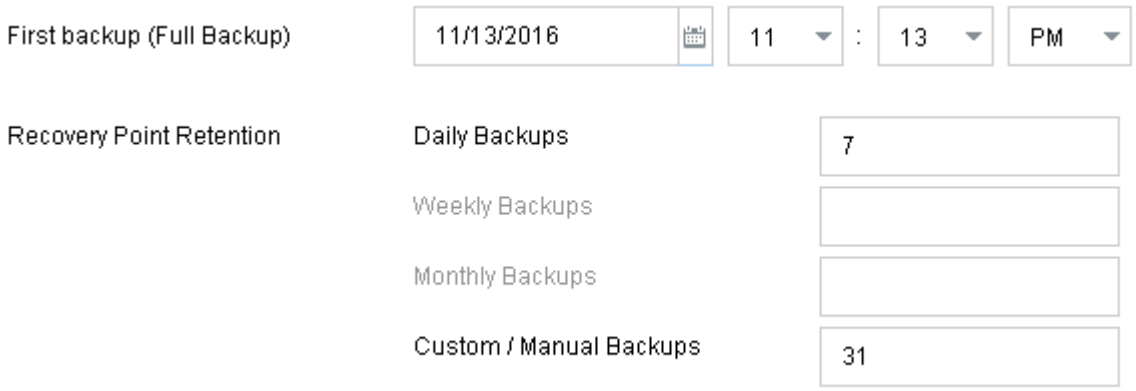
c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

   La pianificazione del limite delle risorse specificata viene visualizzata nella pagina **Pianificazione**.

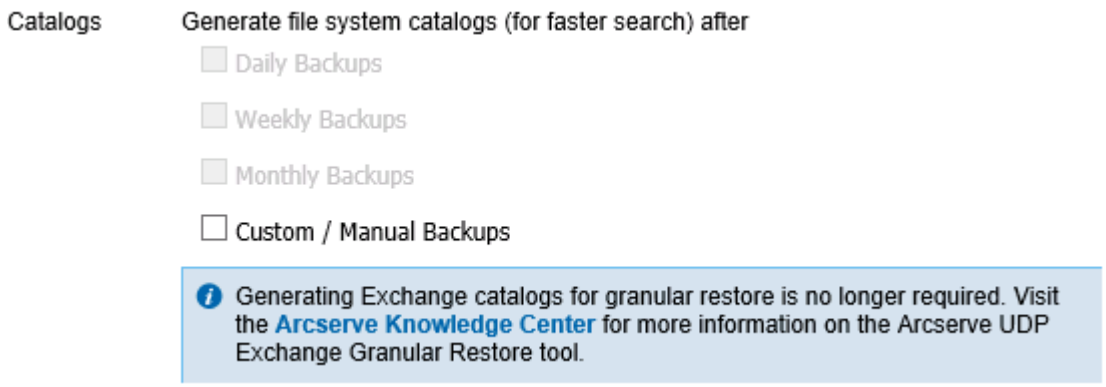
3. Specificare l'ora di inizio per il backup pianificato.



4. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo Pianificazione di backup.

5. Specificare i dettagli relativi al catalogo.



   I cataloghi permettono di generare il catalogo file system. Il catalogo file system è necessario per migliorare e velocizzare la ricerca. Se si selezionano le caselle di controllo del catalogo, i cataloghi verranno abilitati in base al tipo di backup specificato. Deselezionare una casella di controllo per disattivare la generazione del catalogo.

   Viene specificata la pianificazione.

Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione

L'opzione di pianificazione consente di specificare una pianificazione personalizzata o una pianificazione giornaliera/settimanale/mensile o entrambe. Nella pianificazione personalizzata è possibile configurare la pianificazione del backup per ciascun giorno della settimana e aggiungere fino a quattro pianificazioni di backup ogni giorno. È possibile selezionare un giorno specifico di una settimana e creare un intervallo di tempo per definire quando eseguire il backup e la frequenza.

Pianificazione	Processo supportato	Commenti
Backup	Processo di backup	Definire gli intervalli di tempo per eseguire i processi di backup.
Limitazione della velocità di backup	Processo di backup	Definire gli intervalli di tempo per controllare la velocità di backup.
Unione	Processo di unione	Definire quando unire i processi.
Pianificazione quotidiana	Processo di backup	Definire quando eseguire processi di backup quotidiani.
Pianificazione settimanale	Processo di backup	Definire quando eseguire processi di backup settimanali.
Pianificazione mensile	Processo di backup	Definire quando eseguire processi di backup mensili.

È inoltre possibile specificare le impostazioni di memorizzazione per i punti di ripristino.

Nota: All'interno di ogni piano è necessario configurare le impostazioni di conservazione per controllare il modo in cui i nodi assegnati a tale piano vengono memorizzati nell'archivio dati di destinazione.

Le pianificazioni per i backup giornalieri/settimanali/mensili sono indipendenti dalla pianificazione personalizzata e gli uni dagli altri. È possibile configurare di eseguire solo il backup giornaliero, il backup settimanale o il backup mensile senza configurare la pianificazione personalizzata.

Pianificazione del processo di backup

È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del backup. Un intervallo di tempo valido è dalle 00:00 alle 23:59. Non è possibile specificare un intervallo di tempo come ad esempio dalle 18:00 alle 06:00. In tali casi, si devono specificare manualmente due intervalli di tempo diversi.

Per ogni intervallo di tempo l'ora di inizio è inclusa e l'ora di fine è esclusa. Ad esempio, si è configurato il backup incrementale da eseguire ogni ora tra le 06:00 e le 09:00 e il backup inizierà alle 06:00. Ciò significa che il backup verrà eseguito alle 06:00, alle 07:00 e 08:00, ma NON alle 09:00.

Nota: Se si desidera eseguire il processo di backup ripetutamente fino al termine della giornata, impostare la pianificazione fino alle 00:00. Ad esempio, per eseguire un processo di backup ogni 15 minuti per l'intera giornata, impostare la pianificazione dalle 00:00 alle 00:00 ogni 15 minuti.

Pianificazione del limite delle risorse di backup

La pianificazione del limite delle risorse di backup consente di controllare la velocità effettiva di backup, che a sua volta controlla l'utilizzo delle risorse (I/O del disco, CPU, larghezza di banda della rete) del server di cui si esegue il backup. Questo è utile se non si desidera influire sulle prestazioni del server durante i normali orari di ufficio. È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del limite delle risorse di backup. Per ogni intervallo di tempo è possibile specificare un valore, in MB per minuto. Questo valore viene utilizzato per controllare la velocità effettiva di backup. I valori validi sono compresi tra 1 MB/minuto a 99999 MB/minuto.

Se un processo di backup si estende oltre il tempo specificato, il limite della velocità cambia in conformità all'intervallo di tempo specificato. Ad esempio, il limite delle risorse di backup definito è 500 MB/minuto dalle 08:00 alle 20:00 e 2500 MB/minuto dalle 20:00 alle 22:00. Se un processo di backup inizia alle 19:00 e viene eseguito per tre ore, dalle 19:00 alle 20:00 il limite della velocità è pari a 500 MB/minuto e dalle 20:00 alle 22:00 a 2500 MB/minuto.

Se non si definisce alcuna pianificazione del backup e della sua velocità effettiva, il backup viene eseguito il più rapidamente possibile.

Pianificazione di unione

Consente di unire i punti di ripristino in base alla pianificazione fornita.

Considerare i punti seguenti per il processo di unione:

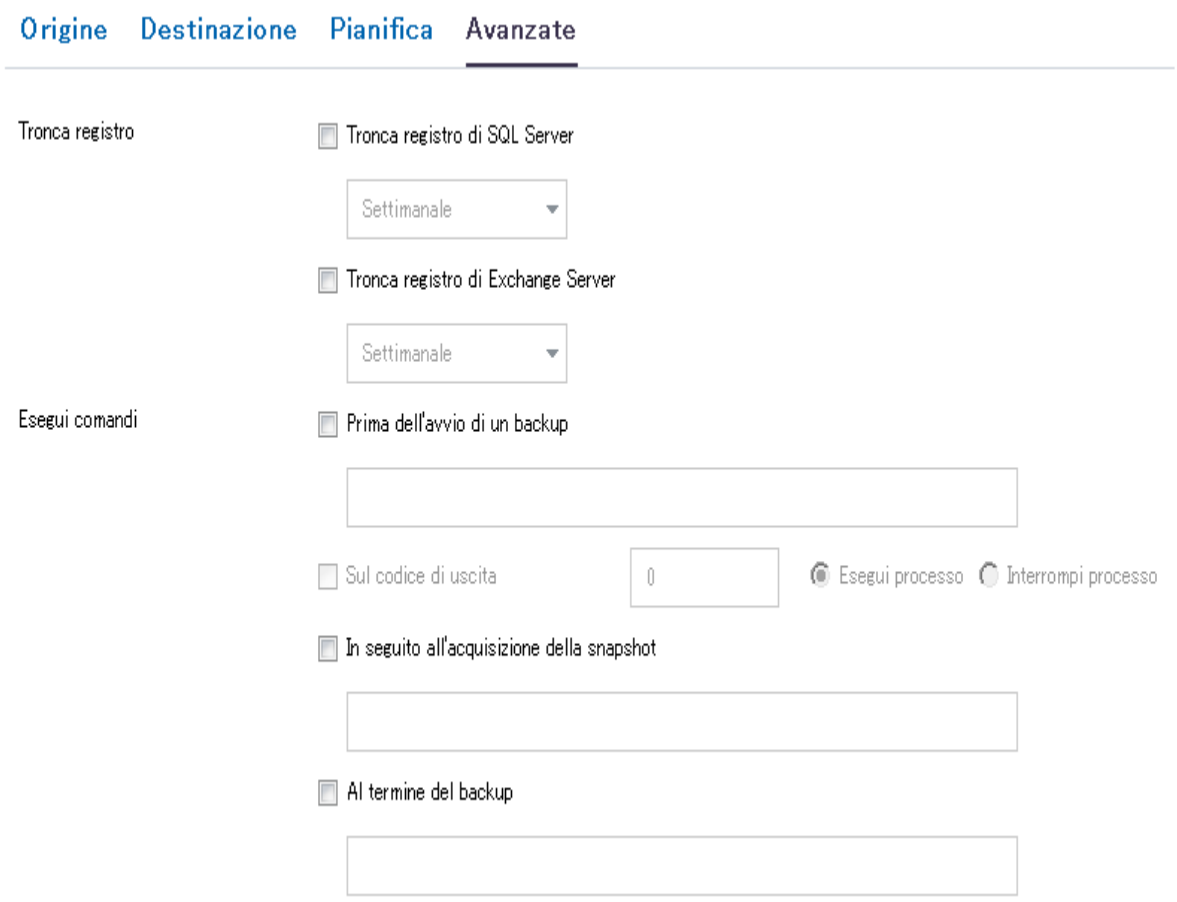
- In qualsiasi momento è possibile eseguire solo un processo di unione per un nodo.
- Se un processo di unione inizia, esso deve essere completato prima di poter avviare il processo di unione successivo. Ciò significa che se uno o più set di punti di ripristino vengono uniti, non è possibile aggiungere nuovi punti di ripristino a questo processo di unione finché il processo di unione dell'insieme corrente dei punti di ripristino non viene completato.

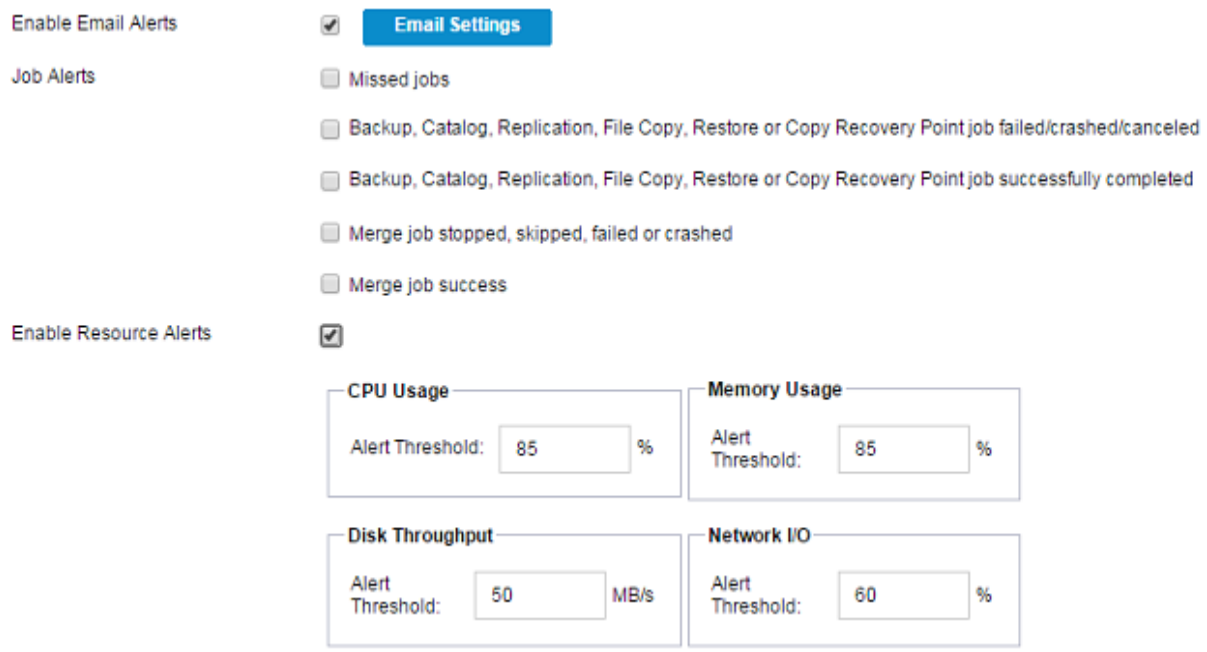
- Se un processo di unione sta elaborando più di un set di punti di ripristino (ad esempio set [1~4], set [5~11] e set [12~14] sono tre set distinti), il Recovery Point Server elabora tali set uno alla volta.
- Se un processo di unione viene ripreso dopo una pausa, il processo individua in quale punto era stato interrotto e riprende l'unione da tale punto.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione delle impostazioni per troncare i registri, l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda Avanzate:





Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

Tronca registro

Consente di specificare la pianificazione per troncare i registri per SQL Server ed Exchange Server. È possibile specificare la pianificazione come **Giornaliero**, **Settimanale** o **Mensile**.

Nome utente

Consente di specificare l'utente autorizzato per l'esecuzione di uno script.

Password

Consente di specificare la password dell'utente autorizzato all'esecuzione dello script.

Esegui un comando prima dell'avvio del backup

Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Esegui processo** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

Esegui un comando dopo l'acquisizione della snapshot

Consente di eseguire uno script dopo l'acquisizione della snapshot del backup. Specificare il percorso di archiviazione dello script.

Esegui un comando al completamento del backup

Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso di archiviazione dello script.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere mediante posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

Abilita avvisi sulle risorse

Consente di specificare una soglia per Utilizzo CPU, Memoria, Velocità del disco, I/O di rete. È possibile fornire il valore in percentuale. Si riceve un messaggio di posta elettronica al superamento del valore Soglia di avviso.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su Salva.

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: Se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo.

Il piano di backup viene creato e distribuito automaticamente al nodo di origine. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

Aggiunta di un'attività di archiviazione file al piano

L'attività di archiviazione file consente di archiviare singoli file nella destinazione specificata. Dopo aver copiato i file nella destinazione specificata e aver fornito più spazio disponibile sull'origine, i file originali vengono eliminati dall'origine. Il processo di archiviazione file non dipende dal processo di catalogo.

Nota: Se è in corso un processo di backup e il piano viene sospeso, il processo di backup verrà interrotto e il processo di archiviazione file non verrà avviato. Quando il piano viene ripreso, il processo di archiviazione file non viene ripreso automaticamente. Per avviare il processo di archiviazione file è necessario eseguire un altro processo di backup manualmente.

Per i file copiati utilizzando l'opzione Archiviazione file, Arcserve UDP genera un file stub con estensione "UDP.txt". Per ulteriori informazioni sull'aggiornamento del file stub, consultare la sezione Aggiornamento dei file stub.

Effettuare le operazioni seguenti:

1. Fare clic su **Aggiungi un'attività** dal riquadro sinistro.

   Viene aggiunta una nuova attività al riquadro sinistro.

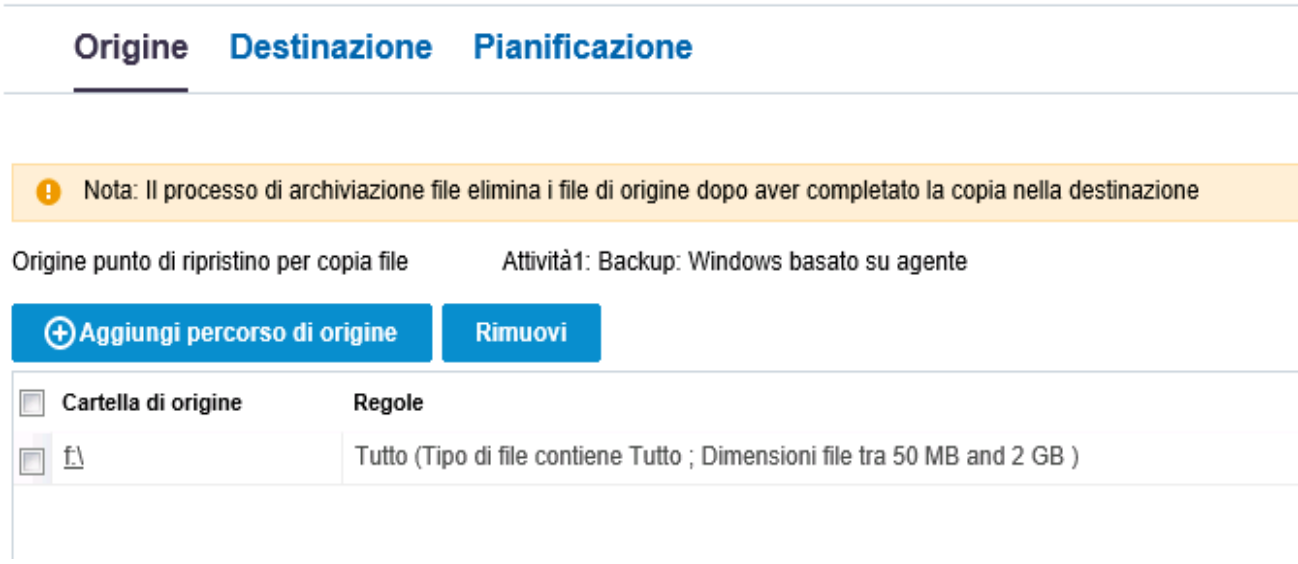
2. Dal menu a discesa **Tipo di attività**, selezionare **Archivio file**.

   L'attività Archivio file viene aggiunta.

3. Fare clic sulla scheda **Origine** e specificare i dettagli.

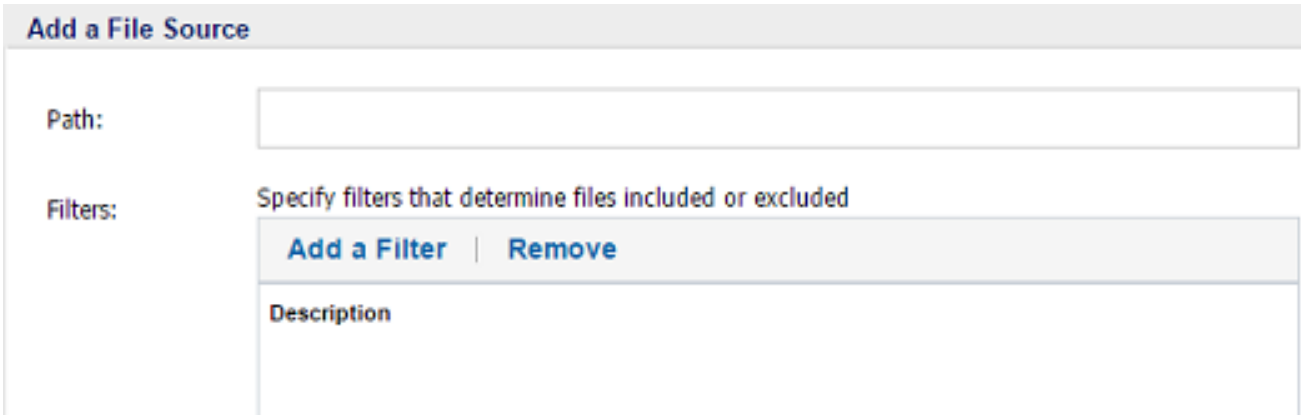
   Posizione dei punti di ripristino

   Specifica la posizione dei punti di ripristino che verranno archiviati. Questo campo è già selezionato.

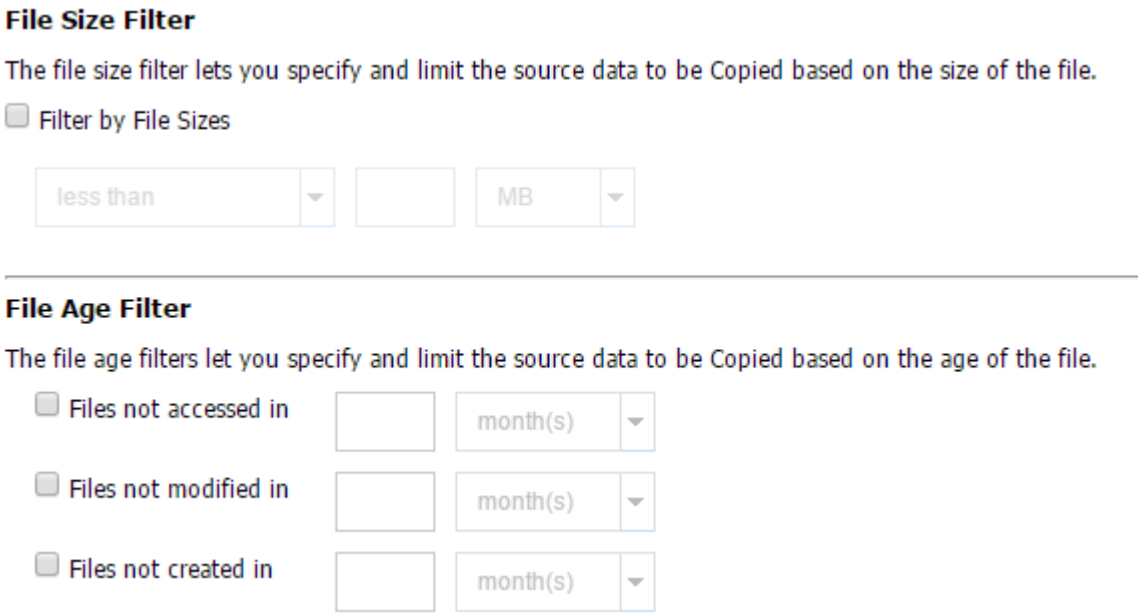


4. Fare clic su **Aggiungi origine**.

   Viene visualizzata la finestra di dialogo **Aggiungi origine file**.

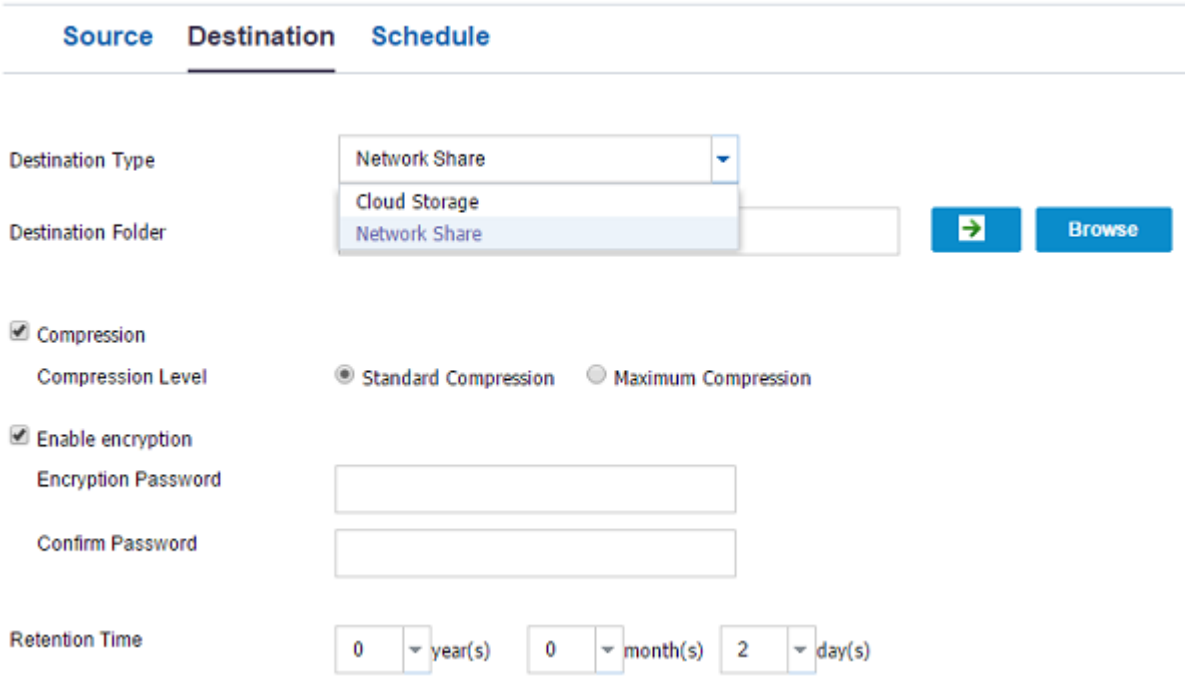


5. Specificare il percorso del file di origine che si desidera copiare.
6. Specificare le opzioni **Filtro dimensioni file** e **Filtro data file**.



7. Fare clic su **Aggiungi filtro**.
8. Selezionare il filtro dall'elenco e fare clic su **Applica**.
9. Fare clic su **OK**.

   La finestra di dialogo **Aggiungi origine file** viene chiusa.
10. Fare clic sulla scheda **Destinazioni** e specificare i dettagli della destinazione.



Tipo di destinazione

Specifica che il tipo di destinazione è una condivisione di rete o un'archiviazione cloud. Per entrambe le opzioni di destinazione, se la connessione alla destinazione specificata viene persa o interrotta, Arcserve UDP esegue più tentativi di completamento del processo di archiviazione file. Nel caso in cui non sia possibile completare il processo, viene eseguito un processo di riparazione a partire dal punto in cui si è verificato l'errore. Inoltre, il registro attività viene aggiornato con il messaggio di errore corrispondente e viene inviata una notifica di posta elettronica (se configurata).

Condivisione di rete

Specifica che la destinazione è una cartella condivisa. Se selezionata, questa opzione consente di specificare il percorso completo della posizione in cui si desidera spostare i file/le cartelle di origine.

Cartella di destinazione

Specifica la destinazione in cui verranno memorizzati i file archiviati. La destinazione può corrispondere a un volume o a una cartella locale oppure a una condivisione file accessibile mediante un percorso conforme al formato UNC (Uniform Naming Convention). Questo campo è disponibile quando si seleziona Condivisione di rete o Volume su un nodo protetto come tipo di destinazione. È anche possibile cercare la cartella di destinazione.

Archiviazione cloud

Specifica che sono i file copiati vengono archiviati in un ambiente cloud. Arcserve UDP attualmente supporta la copia di file su più fornitori cloud, come Amazon S3 (Simple Storage Service), le versioni compatibili con Amazon S3, Windows Azure, le versioni compatibili con Windows Azure, Eucalyptus-Walrus e FUJITSU Hybrid IT Service FJcloud-O. Questi fornitori cloud sono servizi Web disponibili al pubblico che consentono di archiviare e recuperare qualsiasi quantità di dati in qualsiasi momento da ogni punto del Web in un ambiente protetto e sicuro.

Nota: per eliminare eventuali errori di sfasamento orario durante la connessione all'ambiente cloud, verificare sul computer in uso che il fuso orario sia stato impostato correttamente e che l'orologio sia sincronizzato con l'orario globale. Si consiglia di confrontare l'ora del computer con l'ora GMT. Se l'orario del computer in uso non è sincronizzato con l'ora globale corretta (con uno scarto di 5-10 minuti), non sarà possibile utilizzare la connessione cloud. Se necessario, reimpostare l'ora corretta per il computer ed eseguire di nuovo il processo di copia file.

Periferica di archiviazione

Selezionare il tipo di periferica dall'elenco a discesa.

Archiviazione cloud

Selezionare il percorso di archiviazione cloud dall'elenco a discesa. L'elenco a discesa è disponibile se i dettagli di archiviazione cloud sono stati specificati. Se si specifica l'account di archiviazione cloud per la prima volta, fare clic su Aggiungi per aggiungere l'account cloud. Se si seleziona Archiviazione cloud dalla volta successiva, l'account viene visualizzato nell'elenco a discesa Archiviazione cloud.

Nota: Per ulteriori informazioni sull'aggiunta di un account cloud, consultare la sezione Aggiunta account cloud.

Compressione

Specifica il tipo di compressione da utilizzare per i processi di archiviazione file.

La compressione viene utilizzata per ridurre lo spazio di archiviazione nella destinazione di archiviazione file, tuttavia comporta la riduzione della velocità di archiviazione file a causa del maggiore utilizzo della CPU.

Nota: Per i processi di archiviazione file compressi, il registro attività visualizza solo la dimensione non compressa.

Le opzioni disponibili sono:

Compressione standard

Verrà eseguito un certo livello di compressione. L'opzione determina un equilibrio di utilizzo della CPU e dello spazio di archiviazione richiesto. Si tratta dell'impostazione predefinita.

Compressione massima

Verrà eseguita la compressione massima. L'opzione determina un utilizzo massimo della CPU (velocità minima) e un utilizzo minimo dello spazio di archiviazione per la copia file.

Enable Encryption (Abilita crittografia)

Specifica l'utilizzo della crittografia per l'archiviazione file.

La crittografia dei dati corrisponde alla conversione di dati in un modulo incomprensibile senza un meccanismo di decifratura. La protezione dei dati di Arcserve UDP utilizza algoritmi di crittografia AES-256 (Advanced Encryption Standard) per ottenere la massima protezione e riservatezza dei dati. Nel caso in cui venga selezionata l'opzione di crittografia, è necessario specificare e confermare una password di crittografia.

Periodo di memorizzazione

Specifica la durata (anni, mesi, giorni) di memorizzazione dei dati archiviati nel percorso di destinazione. Al termine del periodo di memorizzazione specificato, i dati archiviati verranno eliminati dalla destinazione.

Il calcolo del periodo di memorizzazione si basa sul periodo di un mese di 30 giorni e di un anno di 365 giorni. Ad esempio: Se si specifica un periodo di memorizzazione di 2 anni, 2 mesi e 5 giorni, il tempo di memorizzazione totale per i dati di copia file sarà di 795 giorni (365 + 365 + 30 + 30 + 5).

Importante! Al termine del periodo di memorizzazione specificato i dati vengono eliminati dalla destinazione. Pertanto, non sarà più possibile archiviare o salvare i dati spostati.

Nota: il processo di eliminazione del periodo di memorizzazione viene attivato solamente se l'opzione di pianificazione della copia file viene abilitata.

Versione file precedente a

Questa impostazione si applica solo ai dati copiati e memorizzati (e non ai dati copiati e spostati).

Specifica il numero di copie memorizzate e archiviate nel percorso di destinazione (cloud o disco). Quando questo numero viene raggiunto, la versione meno recente viene eliminata. Il processo di eliminazione della versione archiviata meno recente viene ripetuto con l'aggiunta delle nuove versioni

alla destinazione mantenendo in questo modo il numero di versioni archiviate specificato.

Ad esempio, se il valore delle versioni di file da memorizzare viene impostato su cinque e vengono eseguite cinque copie del file alle ore t1, t2, t3, t4 e t5, tali versioni costituiscono le cinque copie di file memorizzate e disponibili per il recupero. Quando viene eseguita la sesta copia (con il salvataggio della nuova versione), Arcserve UDP rimuove la copia t1 e le cinque versioni disponibili per il ripristino sono t2, t3, t4, t5 e t6.

Per impostazione predefinita, il numero di copie memorizzate nel percorso di destinazione è 15.

11. Fare clic sulla scheda **Pianificazione** e specificare l'ora per l'esecuzione del processo di archiviazione file.



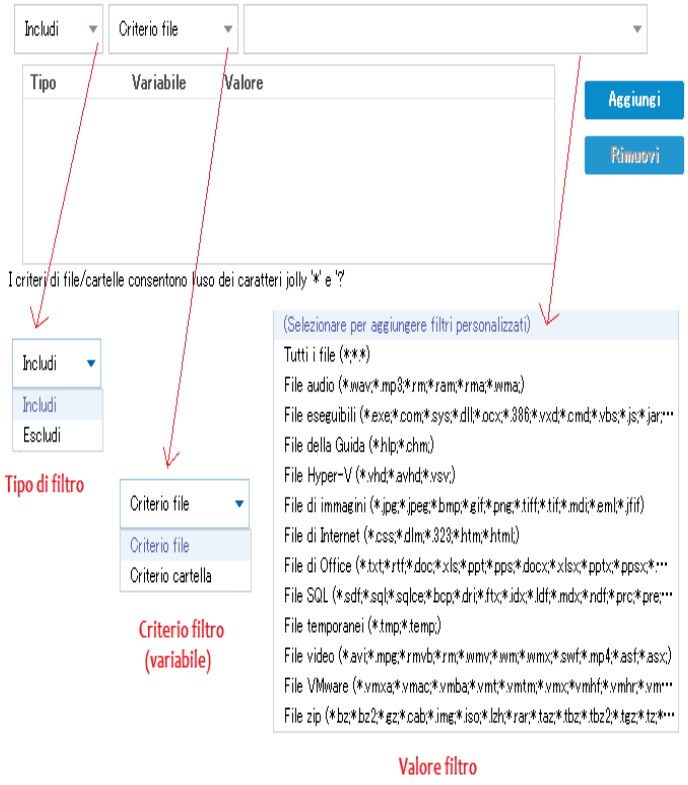
12. Fare clic su **Salva**.

Le modifiche vengono salvate e l'attività di archiviazione file viene distribuita automaticamente al nodo.

Aggiunta di filtri di archiviazione dei file

Aggiungi filtro

Consente di aggiungere un filtro. I filtri consentono di limitare il numero di oggetti di copia file ai tipi e valori specificati.



Tipo di filtro

Esistono due tipi di filtri: Includi ed Escludi.

Il filtro Includi copia solo gli oggetti dell'origine di copia corrispondenti al valore specificato.

Il filtro Escludi copia tutti gli oggetti dell'origine di copia con eccezione degli oggetti corrispondenti al valore specificato.

È possibile specificare più filtri all'interno della stessa copia file separando ciascun valore di filtro con una virgola.

- Se vengono specificati più filtri di inclusione, i dati che corrispondono ad almeno uno dei filtri vengono inclusi nella copia file.
- Se vengono specificati più filtri di esclusione, i dati che corrispondono ad almeno uno dei filtri vengono esclusi dalla copia file.

- È possibile combinare i filtri di inclusione ed esclusione nella stessa richiesta di copia file.

  Nota: Se si verifica un conflitto tra i parametri specificati per i filtri Includi-Escludi, il filtro Escludi viene applicato in quanto è considerato prioritario. Un filtro di inclusione non può eseguire la copia file di un oggetto contrassegnato dal filtro Escludi.

Variabile di filtro (criterio)

Sono disponibili due tipi di filtri per i criteri delle variabili: Criterio file e Criterio cartella.

È possibile utilizzare il filtro Criterio file o Criterio cartella per includere o escludere determinati oggetti dalla copia file.

Valore di filtro

Il valore di filtro consente di limitare le informazioni di copia file selezionando solamente le informazioni di parametro specificate, ad esempio file txt.

Arcserve UDP supporta l'utilizzo dei caratteri jolly per la selezione di più oggetti da includere in un'unica richiesta di copia file. Un carattere jolly è un carattere speciale che può essere utilizzato per rappresentare un carattere singolo o una stringa di testo.

Il campo Valore supporta i caratteri asterisco e punto di domanda. Se non si è a conoscenza del valore completo del criterio file/cartella, è possibile semplificare i risultati del filtro specificando un carattere jolly.

"*": utilizzare l'asterisco per sostituire uno, nessuno o più caratteri del valore.

"?" : utilizzare il punto interrogativo per sostituire un carattere del valore.

Ad esempio, immettere * .txt per escludere tutti i file con estensione .txt, nel caso in cui non si conosca il nome di un file specifico. È possibile specificare il nome parzialmente ed utilizzare i caratteri jolly per completare le parti mancanti.

Nota: Se si seleziona Criterio file come tipo di filtro, viene visualizzato un elenco a discesa contenente filtri predefiniti per i tipi di file più utilizzati (file MS-Office, file Image, file eseguibili, file temporanei ecc.). Dopo aver selezionato uno dei filtri predefiniti, è possibile aggiungere o modificare i valori corrispondenti.

Filtro Dimensione file

I filtri di dimensione file consentono di limitare gli oggetti di origine per la copia file in base alla dimensione del file. Se il filtro di dimensione file è attivato, i parametri specificati costituiscono il filtro che definisce gli oggetti da includere nella copia file. È possibile selezionare l'intervallo (Uguale a o Maggiore di, Uguale a o Minore di oppure Tra) e immettere un valore per la dimensione.

Ad esempio, se viene specificato l'intervallo Uguale a o Maggiore di 10 MB, Arcserve UDP esegue la copia file solo degli oggetti che soddisfano questo criterio. La copia file degli oggetti che non soddisfano i criteri di dimensione dei file non verrà eseguita.

Filtro di data file

I filtri di data file consentono di includere automaticamente gli oggetti di origine per la copia file, in base alle date specificate per il file. È possibile selezionare un parametro (Nessun accesso al file per, File non modificati in, e/o File non creati in) e immettere un valore per il numero di giorni, mesi o anni per il Filtro data file. È possibile selezionare più filtri data file per la copia file automatica.

Ad esempio, se si specifica il parametro File non modificati per 180 giorni, Arcserve UDP esegue automaticamente tutti i file che soddisfano questo criterio, ovvero i file a cui non sono state apportate modifiche durante gli ultimi 180 giorni.

Importante. Se si specificano entrambi i filtri Dimensione file e Data file o più filtri Data file, verrà eseguita la copia dei soli file che soddisfano tutti i parametri di filtro specificati. I file che non soddisfano nessun parametro non verranno inclusi nella copia.

Aggiornamento dei file stub

Per i file copiati utilizzando l'opzione Archiviazione file, Arcserve UDP genera un file stub con estensione "UDP.txt". Il file stub contiene informazioni sulla destinazione in cui sono stati spostati i file e alcune informazioni aggiuntive. Se un file viene ripristinato nella posizione originale e viene spostato nuovamente nella destinazione specificata, il file stub verrà aggiornato con le informazioni di spostamento. Se necessario, è possibile disattivare i file stub di copia dei file o eliminarli senza alcun tipo di conseguenza. (I file stub esistenti non verranno eliminati se la chiave di registro viene modificata per interrompere la creazione dei file stub).

Le seguenti informazioni sono presenti nel file stub per impostazione predefinita:

Please contact your IT department to restore this file (Contattare il reparto IT per ripristinare il file).

È possibile modificare il testo predefinito aggiungendo una voce di configurazione. Aggiungere la seguente voce tag XML nel file FileCopyDebugSetting.xml dalla directory $UDPHome\Engine\Configuration:

<ArchiveStubFileText> qui è possibile aggiungere il nuovo testo da visualizzare nel file stub

</ArchiveStubFileText>

Esempio: Il file FileCopyDebugSetting.xml si presenterà come

```
<?xml version="1.0" encoding="UTF-8"?>
<HKLM>
<AFArchiveDLL>
<ArchiveStubFileText> qui è possibile aggiungere il nuovo testo da visualizzare nel file stub </ArchiveStubFileText>
</AFArchiveDLL>
</HKLM>
```

Se il file FileCopyDebugSetting.xml non è presente nella directory $UDPHome\Engine\Configuration, creare il file XML.

Se si desidera disabilitare la creazione dei file stub, aggiungere la seguente voce tag XML nel file FileCopyDebugSetting.xml dalla directory $UDPHome\Engine\Configuration:

<CreateStubFile>0</CreateStubFile>

Esempio: Il file FileCopyDebugSetting.xml si presenterà come

```
<?xml version="1.0" encoding="UTF-8"?>
<HKLM>

<AFArchiveDLL>
<CreateStubFile>0</CreateStubFile>
</AFArchiveDLL>
</HKLM>
```

Nota: Se si disabilitano o eliminano i file stub della copia file, non è più possibile recuperare lo stato e la posizione dei file spostati.

(Facoltativo) Esecuzione di un'archiviazione file manuale

In genere, l'archiviazione file viene eseguita automaticamente ed è controllata dalle relative impostazioni di pianificazione. In aggiunta all'archiviazione file pianificata, quella manuale permette di eseguire la copia dei file importanti a seconda delle proprie esigenze. Quando si esegue un'archiviazione file manuale, il processo corrispondente archivia tutte le sessioni nell'origine di archiviazione file.

Si può eseguire l'archiviazione file manualmente dalle visualizzazioni Nodi e Piani facendo clic sul menu **Azioni** o sul menu di scelta rapida.

Attenersi alla procedura descritta per eseguire l'archiviazione file manuale dalla visualizzazione Nodi:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   I nodi vengono visualizzati nel riquadro centrale.
3. Selezionare i nodi per il processo di archiviazione file. I nodi devono disporre di un piano di archiviazione file assegnato.
4. Nel riquadro centrale, fare clic su **Azioni**, **Archivia file ora**.

   Viene visualizzata la finestra di dialogo **Run File archive now (Esegui archiviazione file ora)**.
5. Fare clic su **OK**.

   Il processo di archiviazione file viene eseguito.

   L'archiviazione file manuale viene completata correttamente.

Verifica del piano

Per verificare il piano di copia file, confermare di aver creato correttamente il piano. Dopo avere verificato che il piano è stato creato correttamente, verificare se il processo di backup sia in esecuzione in base alla pianificazione. In seguito al completamento del processo di backup, il processo di copia file viene eseguito in base alla pianificazione. È possibile verificare lo stato del processo di backup e del processo Copia file dalla scheda **Jobs** (Processi).

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Seguire questi passaggi per verificare i processi Copia file:

1. Fare clic sulla scheda **Jobs** (Processi).
2. Dal riquadro sinistro, fare clic su **Tutti i processi completati**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare la corretta esecuzione del processo di backup e del processo Copia file.

Creazione di un piano di copia su nastro

Arcserve UDP è integrato con Arcserve Backup per copiare i dati di backup in un supporto di destinazione di tipo nastro. È possibile creare un piano per eseguire il backup dei dati di origine e copiare i dati di backup sul nastro. È possibile creare e gestire il piano dalla console.

Di seguito sono elencati i vantaggi derivati dall'archiviazione dei punti di ripristino su nastro:

- Conformità normativa: consente di conservare documenti, messaggi di posta elettronica e altri dati critici in conformità con i regolamenti interni ed esterni.
- Riduzione dei costi di archiviazione: consente di recuperare la capacità di archiviazione mediante la migrazione dei dati meno recenti o dei dati usati raramente contenuti nei sistemi primari su percorsi di archiviazione più adeguati.
- Gestione di più versioni di file: consente di risalire alle versioni precedenti dei file di cui è stato eseguito il backup (se necessario) oppure di gestire più versioni dello stesso file in destinazioni diverse.

Scenari supportati

- Se la destinazione dell'attività 1 corrisponde al **Recovery Point Server di Arcserve UDP**, installare l'agente client sul nodo RPS.
- Per il piano basato sull'agente che ha come destinazione la **condivisione locale/remota**, installare l'agente client su tutti i nodi dell'agente Arcserve UDP.
- Per il piano senza agente basato su host, installare l'agente client sul nodo proxy Arcserve UDP.

Come procedere?

- Verifica dei prerequisiti
- Creazione di un piano con un'attività di backup
- Aggiunta di un piano di copia su nastro
- Verifica del piano

Verifica delle considerazioni e dei prerequisiti

Verificare se i prerequisiti seguenti sono stati completati:

- Accedere alla console.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.
- Aggiunta del server Arcserve Backup alla console. Per ulteriori informazioni sull'aggiunta del server di backup Arcserve alla console, consultare la sezione Aggiunta di server Arcserve Backup.
- Il Recovery Point Server specificato nell'attività principale di un piano deve avere installato l'agente del server Arcserve Backup.

Creazione di un piano con un'attività di backup

Un piano include diversi tipi di attività da eseguire. In genere, un piano include attività principali seguite da un'attività secondaria. In genere, un'attività principale è un'attività di backup o di replica da un'attività di console remota. Un'attività di backup consiste nella creazione di un backup dei nodi di origine che si desidera proteggere. È possibile eseguire il backup dei dati dai computer virtuali e fisici di Windows e Linux. È quindi possibile salvare i dati di backup in un'altra posizione come precauzione aggiuntiva.

Per ulteriori informazioni su:

- Come eseguire il backup di un nodo Windows, consultare la sezione Creazione di un piano di backup di Windows.
- Come eseguire il backup di computer virtuali, consultare la sezione Creazione di un piano di backup virtuale basato su host.
- Come eseguire il backup di nodi Linux, consultare la sezione Creazione di un piano di backup di Linux.
- Come replicare i dati di backup su una destinazione remota, consultare la sezione Replica dei dati tra archivi di dati gestiti da console UDP diverse.

Aggiunta di un'attività di copia su nastro nel piano

L'attività di copia su nastro consente di copiare i dati su un nastro. Il supporto nastro viene identificato dal server di Arcserve Backup aggiunto.

Effettuare le operazioni seguenti:

1. Fare clic su **Aggiungi un'attività** dal riquadro sinistro.

   Viene aggiunta una nuova attività al riquadro sinistro.

2. Dal menu a discesa **Tipo di attività**, selezionare **Copia su nastro**.

   L'attività Copia su nastro viene aggiunta.

   Nota: i backup personalizzati non attivano i processi di copia su nastro.

   Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

In genere, il file di origine è una destinazione di backup o di replica.

Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli nella scheda **Origine**.

   Origine della copia su nastro

   Specifica la posizione dei punti di ripristino che verranno copiati. Se si dispone solo di un'origine, questo campo è già selezionato. Ad esempio, se il piano ha solamente un'attività di backup e viene aggiunta l'attività Copia su nastro, la destinazione dell'attività di backup diviene l'origine della copia su nastro. Se si dispone di più origini per la copia su nastro, è possibile aggiungere una copia su nastro per ciascuna di queste origini. Ad esempio, se la prima attività è un'attività di backup, la seconda e la terza attività sono attività di replica. Sarà quindi possibile aggiungere tre attività di Copia su nastro al piano.

   Tipi di punti di ripristino

   Specifica i tipi di punti di ripristino. Le opzioni disponibili sono Backup giornalieri, Backup settimanali e Backup mensili.

2. Fare clic sulla scheda **Destinazione**.

   Viene visualizzata la pagina **Destinazione**.

   I dettagli di origine sono stati specificati correttamente.

Definizione della destinazione

La destinazione è un gruppo di supporti nastro nel server di Arcserve Backup. Prima di creare questa attività, è necessario aggiungere il server di Arcserve Backup alla console.

Effettuare le operazioni seguenti:

1. Specificare i dettagli seguenti per la destinazione di backup.

   Server Arcserve Backup

   Selezionare il server Arcserve Backup dall'elenco a discesa.

   Gruppo di supporti

   Selezionare il gruppo di supporti dall'elenco a discesa. Il gruppo di supporti varia a seconda del server di Arcserve Backup. Per impostazione predefinita, la periferica basata su disco <ASBU> e il gruppo Tape RAID non vengono elencati nel gruppo di supporti.

   Per effettuare la migrazione dei punti di ripristino di Arcserve UDP su una periferica basata su disco di Arcserve Backup, è necessario convertire i punti di ripristino incrementale in punti di ripristino completo. Il metodo consigliato per eseguire la migrazione del punto di ripristino di Arcserve UDP su una periferica basata su disco consiste nell'eseguire una replica dall'archivio dati di Arcserve UDP su un altro archivio dati.

   Come destinazione per il processo di copia su nastro è possibile configurare soltanto i gruppi di nastri. È possibile modificare una chiave di impostazione nel file ConsoleConfiguration.xml disponibile nel percorso di UDP Management Configuration per visualizzare il gruppo ASBU FSD come destinazione della copia su nastro:

   C:\Programmi\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml

   <displayASBUFSDGroup>0</displayASBUFSDGroup>

   Se il valore è 0, il gruppo ASBU FSD non viene visualizzato.

   <displayASBUFSDGroup>1</displayASBUFSDGroup>

   Se il valore è 1, il gruppo ASBU FSD viene visualizzato.

   Dopo aver modificato le impostazioni, riavviare il servizio di gestione Arcserve UDP per renderle effettive.

   L'elenco del gruppo di supporti viene interrogato dal server di Arcserve Backup. Corrisponde all'elenco del gruppo di periferiche nel server di Arcserve Backup.

Multiplexing

Selezionare la casella di controllo per attivare il multiplexing. Specificare il numero massimo degli stream che possono scrivere contemporaneamente su un nastro. Il numero di stream predefinito corrisponde a 4 e l'intervallo supportato è compreso tra 2 e 32.

Crittografia

Specifica l'utilizzo della crittografia per la copia su nastro.

L'attivazione della crittografia assicura che i dati vengano crittografati sul nastro. Nel caso in cui venga selezionata l'opzione di crittografia, è necessario specificare e confermare una password di crittografia.

Compressione

L'attivazione della compressione assicura che i dati vengano compressi sul nastro.

2. Verificare i dettagli del gruppo di supporti per il server di Arcserve Backup e il gruppo di supporti selezionati.
3. Fare clic sulla scheda **Pianificazione**.

   Viene visualizzata la pagina Pianificazione.

   La destinazione è stata specificata.

Definizione della pianificazione

È possibile specificare la pianificazione per avviare il processo di copia su nastro. È inoltre possibile scegliere il criterio di conservazione dei supporti e la modalità di utilizzo del nastro.

Effettuare le operazioni seguenti:

1. Fare clic su **Aggiungi**, **Aggiungi pianificazione di copia su nastro**.

   Viene visualizzata la finestra di dialogo **Aggiungi nuova pianificazione di copia su nastro**.

2. Specificare una pianificazione per il nastro.

   Una pianificazione consente di definire l'intervallo di tempo per l'avvio di un processo di copia su nastro. Se si aggiunge una pianificazione, il processo di copia su nastro viene eseguito solo durante la pianificazione definita. Se non si specifica una pianificazione, il processo di copia su nastro viene eseguito entro i 30 minuti successivi dal momento in cui un punto di ripristino qualificato su un archivio dati è pronto.

3. Fare clic su **Salva**.

   Viene visualizzata la finestra di dialogo **Aggiungi nuova pianificazione di copia su nastro**.

4. Selezionare l'opzione **Nome pool di supporti** dall'elenco a discesa.

   Viene selezionato un nome di pool di supporti predefinito in base al nome del piano.

   È inoltre possibile selezionare il nome di un pool di supporti esistente dall'elenco a discesa. In tal caso, il criterio di conservazione del supporto e la modalità di utilizzo del nastro con tale pool di supporti verranno copiati nell'attività. È possibile condividere i nastri tra più piani Arcserve UDP specificando lo stesso pool di supporti in tutti i piani Arcserve UDP.

   È inoltre possibile specificare un nome di pool diverso. Per un nome di pool di supporti è consentito un massimo di 13 caratteri.

5. Specificare un criterio **Conservazione punto di ripristino**.

   Un criterio di conservazione del punto di ripristino consente di conservare i punti di ripristino su base giornaliera, settimana o mensile. È possibile specificare un periodo di conservazione differente per i diversi tipi di punti di ripristino. Ad esempio, se si seleziona **Backup giornalieri** e **Backup settimanali** dalla scheda **Origine**, sarà possibile specificare un periodo di conservazione del punto di ripristino diverso per entrambi i tipi di backup.

6. Selezionare una delle opzioni **Utilizzo nastri**.

Aggiungi a nastri esistenti

Indica che tutti i punti di ripristino generati entro il periodo di conservazione specificato vengono copiati sullo stesso nastro. Ad esempio, se si è scelto 7 come periodo di conservazione per i backup giornalieri, tutti i punti di ripristino dal giorno 1 al giorno 7 vengono copiati sullo stesso nastro. Di conseguenza, tutti i punti di ripristino a partire dal giorno 7 (dal giorno 8 al giorno 14) vengono copiati su un nastro diverso, e così via.

I punti di ripristino della prima settimana (dal giorno 1 al giorno 7) vengono conservati per i 7 giorni successivi (dal giorno 8 al giorno 14). A partire dal giorno 15, i punti di ripristino vengono copiati nuovamente sul nastro 1 in quanto il criterio di conservazione per i punti di ripristino della prima settimana è scaduto.

Il seguente elenco mostra il periodo di conservazione predefinito per l'opzione Aggiungi a nastri esistenti:

- Giornaliero: 7 giorni
- Settimanale: 5 settimane
- Mensile: 12 mesi

Vengono copiati sullo stesso nastro: sette punti di ripristino giornalieri, cinque punti di ripristino settimanali e 12 punti di ripristino mensili.

Copia su nastri distinti

Indica che i punti di ripristino di ogni giorno vengono copiati su un nastro distinto. Ad esempio, se è stato specificato 7 come periodo di conservazione per i backup giornalieri, i punti di ripristino a partire dal giorno 1 vengono copiati sul nastro 1, quelli a partire dal giorno 2 vengono copiati sul nastro 2, quelli a partire dal giorno 3 vengono copiati sul nastro 3, e così via.

I punti di ripristino a partire dal giorno 1 vengono conservati per 7 giorni. Il giorno 8 i punti di ripristino vengono copiati sul nastro 1 poiché il criterio di conservazione è scaduto per i punti di ripristino del giorno 1.

Il seguente elenco mostra il periodo di conservazione predefinito per l'opzione Copia su nastri distinti:

- Giornaliero: 7 giorni
- Settimanale: 5 settimane
- Mensile: 12 mesi

Ciascuno dei sette punti di ripristino giornalieri viene copiato in un nastro distinto, così come ciascuno dei cinque punti di ripristino settimanali e ciascuno dei 12 punti di ripristino mensili.

7. Fare clic sulla scheda **Avanzate**.

   Viene visualizzata la pagina **Impostazioni avanzate**.

   La pianificazione è stata specificata.

Definizione delle impostazioni avanzate

Le impostazioni avanzate consentono di configurare alcune impostazioni aggiuntive per le attività di copia su nastro.

1. Specificare i seguenti dettagli:

   Media Eject (Rimozione supporto)

   Indica che il supporto viene rimosso dall'unità al termine del processo, impedendo la sovrascrittura del supporto con i dati di un altro processo.

   Backup Verification (Verifica backup)

   Specifica che Arcserve Backup consente di verificare l'affidabilità del backup controllando la leggibilità dell'intestazione di ogni file. Questa opzione non viene applicata ai backup in multiplexing.

   Run a command before a copy to tape job is started (Esegui un comando prima dell'avvio di una copia su nastro)

   Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script. Fare clic su Sul codice di uscita e specificare il codice di uscita per Esegui processo o Interrompi processo. Esegui processo indica che il processo di backup continua quando lo script restituisce il codice di uscita. Interrompi processo indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

   Run a command after a copy to tape job is over (Esegui un comando al completamento un processo di copia su nastro)

   Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso di archiviazione dello script.

   Nome utente comandi

   Consente di specificare il nome utente per eseguire lo script.

   Password comandi

   Consente di specificare la password per eseguire i comandi.

   Abilitazione degli avvisi di posta elettronica

   Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere mediante posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

   Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

2. Fare clic su **Salva**.

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

L'attività di copia su nastro viene creata ed eseguita in base alla pianificazione.

Nota: Quando si esegue il processo **Copia su nastro**, i valori di monitoraggio del processo nella Console di Arcserve UDP sono differenti da quelli di Arcserve Backup.

Importante. Dopo aver copiato i punti di ripristino su un nastro, è possibile ripristinare i dati nel nastro dalla console di Arcserve UDP. È necessario ripristinare i dati dalla funzionalità di gestione backup di Arcserve. Per ulteriori informazioni sul ripristino di dati su nastro, consultare la sezione Backup e recupero di dati D2D/UDP nella Guida per l'amministratore di Arcserve Backup.

Creazione e gestione di un computer virtuale istantaneo su Microsoft Azure

Il computer virtuale istantaneo supporta la creazione istantanea di un computer virtuale su Microsoft Azure. Il computer virtuale istantaneo su Microsoft Azure apporta i seguenti vantaggi:

- Consente l'accesso immediato ai dati e alle applicazioni presenti nelle sessioni di backup di Arcserve UDP.
- Elimina i tempi di inattività associati a un ripristino tradizionale o alla conversione della sessione di backup in un computer virtuale.
- Fornisce una posizione alternativa per la creazione di un computer virtuale su cloud, anziché in locale.

È possibile creare un computer virtuale istantaneo dalle sessioni di backup seguenti:

- Backup di Linux basato su agente
- Backup senza agente basato su host per il computer virtuale Linux

Nota: per seguire le procedure consigliate per un computer istantaneo su Microsoft Azure, consultare la sezione Procedure consigliate.

Come procedere?

- Verifica dei prerequisiti
- Creazione di un piano del computer virtuale su Microsoft Azure
- Gestione di un piano del computer virtuale su Microsoft Azure

Verifica dei prerequisiti di un computer virtuale istantaneo su Microsoft Azure

Completare i prerequisiti seguenti prima di creare un computer virtuale istantaneo:

- Dalla Matrice di compatibilità, verificare che il computer virtuale sia supportato da Microsoft Azure e da UDP.
- Aggiunta di un account cloud Microsoft Azure
- Verificare di disporre di almeno un Recovery Point Server sul computer locale come destinazione di backup.
- Verificare di disporre di almeno un Recovery Point Server su Microsoft Azure come destinazione di replica.
- Verificare di disporre di almeno un server di backup Linux in locale per il processo di backup.
- Verificare di disporre almeno un server di backup Linux su Microsoft Azure per il processo del computer virtuale istantaneo.
- Verificare che l'account Microsoft Azure sia stato aggiunto.

Limitazioni

- L'avvio dei computer Linux con EUFI NON è supportato.
- I computer Linux con file system Btrfs su più dischi NON sono supportati.

Creazione di un computer virtuale su Microsoft Azure

Per creare un computer virtuale istantaneo su un piano Microsoft Azure, si consiglia di eseguire una delle seguenti opzioni:

- Eseguire il backup locale del nodo protetto sull'archivio dati locale del Recovery Point Server, quindi eseguirne la replica sul Recovery Point Server in Microsoft Azure. Per informazioni sull'aggiunta di un nodo, consultare la sezione Aggiunta di nodi alla Console.
- Eseguire il backup locale del nodo protetto sul percorso condiviso locale CIFS (/NFS), quindi eseguirne la copia sul percorso condiviso in Microsoft Azure. Per informazioni sull'esecuzione del backup dei nodi protetti, consultare la sezione Creazione di un piano di backup di Linux.

La creazione di un computer virtuale istantaneo richiede i cinque passaggi seguenti:

1. Apertura della procedura guidata del computer virtuale istantaneo
2. Selezione del punto di ripristino
3. Selezione della posizione del computer virtuale
4. Selezione del server di ripristino
5. Definizione dei dettagli del computer virtuale istantaneo
6. Invio del processo del computer virtuale istantaneo

Apertura della procedura guidata del computer virtuale istantaneo

È possibile configurare e creare un computer virtuale istantaneo mediante la procedura guidata del computer virtuale istantaneo. Esistono tre metodi per aprire la procedura guidata del computer virtuale istantaneo:

- Da Gestione nodo
- Da Gestione destinazione: Recovery Point Server
- Da Gestione destinazione: Cartella condivisa

Aprire la procedura guidata dalla visualizzazione Gestione nodi

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.
3. Tutti i nodi vengono visualizzati nel riquadro centrale.
4. Fare clic con il tasto destro del mouse e selezionare **Crea un computer virtuale istantaneo**.

   Viene visualizzata la procedura guidata del computer virtuale.

   Nota: se un nodo non è associato a nessun piano, tale nodo non dispone dell'opzione **Crea un computer virtuale istantaneo**.

Aprire la procedura guidata dalla visualizzazione della Gestione destinazione

Da Destinazioni: Recovery Point Server

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Se sono stati aggiunti degli archivi dati, essi vengono visualizzati nel riquadro centrale.
3. Fare clic sull'archivio dati.

   Se è già stato eseguito il backup dei dati sul server RPS, tutti i nodi di origine vengono elencati nel riquadro.
4. Fare clic con il tasto destro del mouse e selezionare **Crea un computer virtuale istantaneo**.

   Viene visualizzata la procedura guidata del computer virtuale.

Da Destinazioni: Cartella condivisa

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni** e fare clic su **Cartelle condivise**.
3. Se sono stati aggiunte cartelle condivise, esse vengono visualizzate nel riquadro centrale.
4. Fare clic su una cartella condivisa e selezionare **Browser punto di ripristino**.

   Se è già stato eseguito il backup dei dati sulla cartella condivisa, tutti i nodi di origine vengono elencati nel riquadro.
5. Fare clic con il tasto destro del mouse su un nodo e scegliere **Crea un computer virtuale istantaneo**.

   Viene visualizzata la procedura guidata del computer virtuale.

Selezione di un punto di ripristino

La pagina Seleziona punto di ripristino consente di visualizzare la posizione del punto di ripristino e di selezionarlo. Il punto di ripristino può trovarsi in una posizione condivisa o in un archivio dati nel server RPS.

La console riconosce automaticamente la posizione del punto di ripristino e preseleziona i campi **Tipo di posizione**, **Recovery Point Server** e **Archivio dati** o **Cartella di condivisione di rete**.

Nota: selezionare la sessione Recovery Point Server (cartella condivisa) come destinazione di replica per risparmiare tempo e larghezza di banda della rete.

Espandere l'elenco Data, selezionare il punto di ripristino richiesto dall'elenco e fare clic su **Avanti**.

Viene visualizzata la pagina **Posizione computer virtuale**.

Nota: se si crea un computer virtuale istantaneo dalla visualizzazione Gestione nodi, vengono elencati solo i Recovery Point Server che si trovano nello stesso sito del nodo di origine. Se si desidera creare un computer virtuale istantaneo dal Recovery Point Server gestito da un sito diverso, accedere a tale sito e aprire la procedura guidata dalla vista Gestione della destinazione.

Selezione della posizione per il computer virtuale

Specificare la posizione del computer virtuale in cui creare il computer virtuale istantaneo.

Effettuare le operazioni seguenti:

1. Selezionare Microsoft Azure.
2. Selezionare il nome dell'account.

   Nota: selezionare l'account corrispondente, se non è già stato aggiunto. Fare riferimento alla sezione Aggiunta di un account cloud Microsoft Azure.
3. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Server di ripristino**.

Selezione di un server di ripristino

Il server di ripristino ospita il modulo di base del computer virtuale istantaneo. Il server di ripristino predefinito è il server RPS. È inoltre possibile assegnare un nodo come server di ripristino.

Per le sessioni di backup di Linux, il server di ripristino è un server di backup di Linux.

Effettuare le operazioni seguenti:

1. Selezionare il server di backup Linux dall'elenco dei nodi.

   Note: selezionare la sessione Recovery Point Server (cartella condivisa) come destinazione di replica per salvare la larghezza di banda e l'ora.

2. Fare clic su **Avanti**.

   Viene visualizzata la pagina dei dettagli del computer virtuale istantaneo.

   Nota: assicurarsi aver selezionato il Recovery Point Server contenuto in Microsoft Azure.

Definizione dei dettagli relativi al computer di virtuale istantaneo

Specificare i dettagli del computer virtuale istantaneo.

Effettuare le operazioni seguenti:

1. Specificare il nome e la descrizione del computer virtuale istantaneo.

Nome computer virtuale

Specifica il nome del computer virtuale istantaneo. Il prefisso del nome del nodo di origine con "UDPIVM_" diventa il nome predefinito del computer virtuale istantaneo. È possibile modificare il nome. Alcuni caratteri speciali, come '@', \ e così via non sono consentiti nel nome.

Descrizione

(Facoltativo) Specifica la descrizione per il computer virtuale istantaneo.

Posizione

Specifica il percorso dell'account Microsoft Azure.

Tipo di disco

Specifica il tipo di disco.

Dimensioni del computer virtuale Azure

Specifica le dimensioni del computer virtuale supportate.

Rete

Specifica la rete esistente sull'account Microsoft Azure.

Subnet

Specifica la subnet esistente sull'account Microsoft Azure.

IP pubblico con assegnazione automatica

Specifica l'indirizzo IP pubblico assegnato al computer virtuale.

IP principale

Specificare l'IP principale del computer virtuale. Specifica l'opzione automaticamente, nel caso in cui non venga specificata.

Selezione di un gruppo di protezione

Specifica il gruppo di protezione. È possibile selezionare più gruppi. Se non viene selezionata alcuna opzione, crea automaticamente un nuovo gruppo di protezione.

Avanzate: Modifica nome host

Specifica il nome host del nuovo computer di destinazione.

Avanzate: Ripristino automatico dei dati in seguito all'avvio del computer virtuale istantaneo

Specifica se il ripristino dei dati viene eseguito automaticamente dopo aver creato il computer virtuale istantaneo.

2. Fare clic su **Fine**.

A questo punto è possibile inoltrare il processo.

Invio del processo del computer virtuale istantaneo

Per creare il computer virtuale istantaneo, inviare il processo del computer virtuale istantaneo. Una volta completato il processo, è possibile visualizzare il computer virtuale istantaneo in **Risorse**, **Infrastruttura Computer virtuale istantaneo**.

Effettuare le operazioni seguenti:

1. Fare clic su **Crea computer virtuale**.

   Viene visualizzata la finestra di dialogo **Crea computer virtuale**.

2. Selezionare una delle seguenti opzioni:

   Avvia ora

   Invia un processo per creare il computer virtuale istantaneo. Al termine del processo di creazione del computer virtuale, avvia automaticamente il computer virtuale.

   Avvia più tardi

   Crea un computer virtuale istantaneo. È necessario avviare manualmente il computer virtuale. È possibile avviare il computer virtuale una volta completato il processo del computer virtuale istantaneo.

   Annulla

   Chiude la finestra di dialogo Crea computer virtuale senza creare alcun computer virtuale. Viene visualizzata di nuovo la pagina Crea computer virtuale.

Il processo computer virtuale istantaneo è stato creato correttamente.

Gestione di un computer virtuale istantaneo

È possibile gestire il computer virtuale istantaneo dalla console. È possibile attivare o spegnere un computer virtuale istantaneo dalla console. Inoltre, è possibile eliminare qualsiasi computer virtuale istantaneo.

Nota: nella console vengono visualizzati soltanto i computer virtuali istantanei creati a partire dai punti di ripristino gestiti dal sito selezionato.

- Avvio o arresto di un computer virtuale istantaneo
- Eliminazione di un computer virtuale istantaneo

Avvio o arresto di un computer virtuale istantaneo

È possibile avviare o interrompere un computer virtuale istantaneo dopo la creazione. Il pulsante Avvia o Interrompi viene visualizzato a seconda dello stato del computer virtuale.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic su **Risorse**.
2. Accedere a **Infrastrutture** e fare clic su **Computer virtuale istantaneo**.
3. Selezionare il computer virtuale dal riquadro centrale e fare clic su **Azioni**.
4. Selezionare **Attiva** o **Disattiva** a seconda dello stato del computer virtuale.

   Il computer virtuale si avvia o si arresta correttamente.

Eliminazione di un computer virtuale istantaneo

È possibile eliminare qualsiasi computer virtuale istantaneo che non è più necessario.

Effettuare le operazioni seguenti:

1. Dalla console, fare clic su **Risorse**.
2. Accedere a **Infrastrutture** e fare clic su **Computer virtuale istantaneo**.
3. Selezionare il computer virtuale dal riquadro centrale e fare clic su **Azioni**.
4. Fare clic su **Elimina**.

   Viene visualizzata una finestra di dialogo di conferma.
5. Fare clic su **OK**.

   Il computer virtuale viene eliminato correttamente.

Creazione e gestione di un computer virtuale istantaneo sui server Hyper-V e VMware ESX

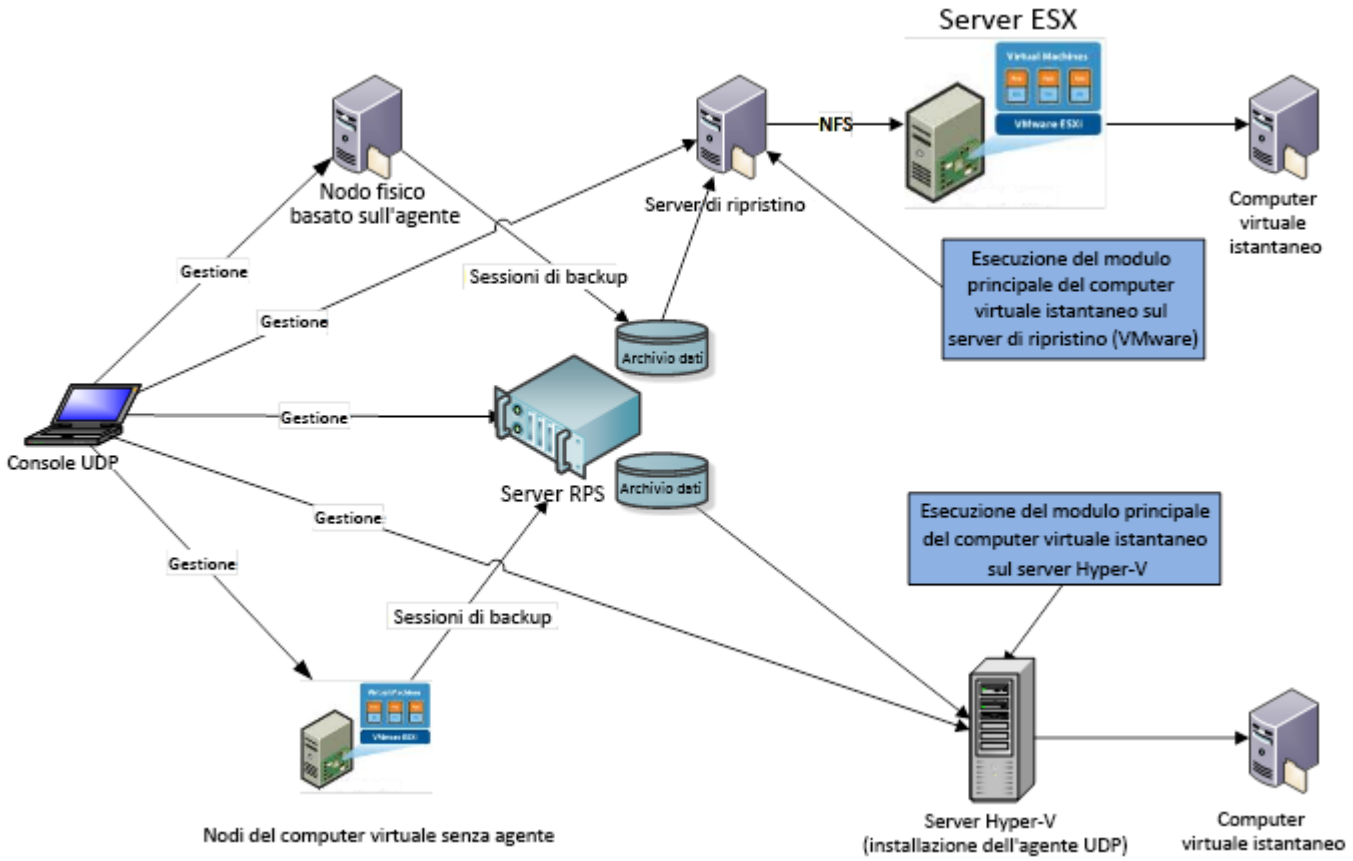
Il computer virtuale istantaneo crea un computer virtuale nell'hypervisor ed esegue la sessione di backup all'interno del computer virtuale senza alcuna conversione precedente. Il vantaggio di un computer virtuale istantaneo consiste nel fornire un accesso immediato ai dati e alle applicazioni presenti nelle sessioni di backup di Arcserve UDP. Un computer virtuale istantaneo elimina i tempi di inattività associati a un ripristino tradizionale o alla conversione della sessione di backup in un computer fisico o virtuale.

È possibile creare un computer virtuale istantaneo dalle sessioni di backup seguenti:

- Backup di Windows basato su agente
- Backup di Linux basato su agente
- Backup senza agente basato su host

È possibile scegliere come hypervisor il server VMware vCenter/ESX(i) o il server Windows Hyper-V.

Il diagramma seguente illustra l'architettura di un computer virtuale istantaneo:



Come procedere?

- Verifica dei prerequisiti per un computer virtuale istantaneo
- Creazione di un computer virtuale istantaneo
- Gestione di un computer virtuale istantaneo

Verifica dei prerequisiti per un computer virtuale istantaneo

Completare i prerequisiti seguenti prima di creare un computer virtuale istantaneo:

- Verificare di disporre di almeno un backup Arcserve UDP.
- Verificare che gli agenti Arcserve UDP siano già installati sul server di ripristino.
- Verificare che la funzionalità NFS sia installata sul server di ripristino, se l'hypervisor di destinazione è un server VMware vCenter/ESX(i).
- Verificare che il sistema operativo del server di ripristino sia Windows Server 2008 R2 a 64 bit o versioni successive.
- Verificare che il server di ripristino abbia spazio sufficiente per il computer virtuale istantaneo.
- Verificare di disporre delle autorizzazioni minime per eseguire le attività obbligatorie di computer virtuale istantaneo. Per ulteriori informazioni, consultare la sezione Autorizzazioni minime di VMware richieste per le attività IVM.

Nota: È possibile avviare il computer. Le schede NIC vengono configurate in base all'input utente nell'interfaccia.

Considerazioni

- La funzionalità di migrazione del computer virtuale istantaneo tra i nodi non è supportata quando un computer virtuale istantaneo viene avviato in un cluster Hyper-V.
- Quando si crea un computer virtuale istantaneo da un backup agente di Linux, non è possibile modificare le impostazioni di un computer virtuale create da un computer virtuale istantaneo mediante un client vSphere. Per modificare le impostazioni del computer virtuale, è necessario utilizzare il client Web vSphere.
- Se il numero di archivi dati NFS raggiunge il numero massimo di montaggi NFS su un host ESXi/ESX e si crea un computer virtuale istantaneo, Arcserve UDP non è in grado di creare l'archivio dati NFS. Per aumentare il numero massimo di montaggi NFS sull'host ESX/ESXi, consultare l'articolo della Knowledge Base di VMware.
- Se si tratta di un punto di ripristino da backup senza agente e l'hypervisor di destinazione è vSphere ESX/VC, il server NFS deve trovarsi sul computer del server di backup Linux.

- Se l'hypervisor di destinazione è MS Hyper-V, il comando net deve trovarsi sul server di backup Linux. Questo comando può essere installato da pacchetti client Samba.
- Il computer virtuale non funziona nelle situazioni seguenti:
  - Riavvio del server di ripristino.
  - Arresto anomalo del server di ripristino.
  - Disconnessione della rete tra server di ripristino e destinazione di backup (archivio dati o cartella condivisa).

Autorizzazioni VMware minime necessarie per le attività del Computer virtuale istantaneo

La tabella visualizza l'elenco delle autorizzazioni VMware minime necessarie per eseguire tutte le attività del Computer virtuale istantaneo .

Nota: Le autorizzazioni globali sono impostate a livello di vCenter.

Attività	**Autorizzazione**
Archivio dati	Allocare spazio
Globale	Disattivare metodi
	Attivare metodi
	Licenze
Host > Configurazione	Configurazione della partizione di archiviazione
Rete	Assegnare una rete
Resource	Assegnare un computer virtuale al pool di risorse
Computer virtuale > Configurazione	Aggiunta di un disco esistente
	Avanzato
Computer virtuale > Interazione	Disattiva
	Attiva
	Reimposta
	Interazione di console
Computer virtuale > Inventario	Creazione nuovo
	Rimuovi
Computer virtuale > Provisioning	Consentire l'accesso al disco
	Consentire l'accesso di sola lettura al disco
	Consentire il download nel computer virtuale
Computer virtuale > Gestione di snapshot	Crea snapshot
	Rimuovi snapshot
	Ripristina snapshot
Computer virtuale > Operazioni guest	Query dell'operazione guest

Creazione di un computer virtuale istantaneo

La creazione di un computer virtuale istantaneo richiede i cinque passaggi seguenti:

1. Apertura della procedura guidata del computer virtuale istantaneo
2. Selezione di un punto di ripristino
3. Definizione della posizione del computer virtuale
4. Definizione del server di ripristino
5. Definizione dei dettagli del computer virtuale istantaneo
6. Invio del processo del computer virtuale istantaneo

   Un volta completato correttamente il processo, viene creato un computer virtuale istantaneo.

Apertura della procedura guidata del computer virtuale istantaneo

È possibile configurare e creare un computer virtuale istantaneo mediante la procedura guidata del computer virtuale istantaneo. Esistono tre metodi per aprire la procedura guidata del computer virtuale istantaneo:

- Dalla gestione del nodo
- Da Gestione della destinazione: Recovery Point Server
- Da Gestione della destinazione: Cartella condivisa

Aprire la procedura guidata dalla visualizzazione Gestione nodi

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.
3. Tutti i nodi vengono visualizzati nel riquadro centrale.
4. Fare clic con il tasto destro del mouse e selezionare **Crea un computer virtuale istantaneo**.

   Viene visualizzata la procedura guidata del computer virtuale.

   Nota: Se un nodo non è associato ad alcun piano, tale nodo non dispone dell'opzione **Crea computer virtuale istantaneo**.

Aprire la procedura guidata dalla visualizzazione della Gestione destinazione

Da Destinazioni: Recovery Point Server

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Se sono stati aggiunti degli archivi dati, essi vengono visualizzati nel riquadro centrale.
3. Fare clic sull'archivio dati.

   Se è già stato eseguito il backup dei dati sul server RPS, tutti i nodi di origine vengono elencati nel riquadro.
4. Fare clic con il tasto destro del mouse e selezionare **Crea un computer virtuale istantaneo**.

   Viene visualizzata la procedura guidata del computer virtuale.

Da Destinazioni: Cartella condivisa

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni** e fare clic su **Cartelle condivise**.
3. Se sono stati aggiunte cartelle condivise, esse vengono visualizzate nel riquadro centrale.
4. Fare clic su una cartella condivisa e selezionare **Browser punto di ripristino**.

   Se è già stato eseguito il backup dei dati sulla cartella condivisa, tutti i nodi di origine vengono elencati nel riquadro.
5. Fare clic con il tasto destro del mouse su un nodo e scegliere **Crea un computer virtuale istantaneo**.

   Viene visualizzata la procedura guidata del computer virtuale.

Seleziona punto di ripristino

La pagina Seleziona punto di ripristino consente di visualizzare la posizione del punto di ripristino e di selezionarlo. Il punto di ripristino può trovarsi in una posizione condivisa o in un archivio dati nel server RPS.

La console riconosce automaticamente la posizione del punto di ripristino e preseleziona i campi **Tipo di posizione**, **Recovery Point Server** e **Archivio dati** o **Cartella di condivisione di rete**.

Espandere l'elenco Data, selezionare il punto di ripristino richiesto dall'elenco e fare clic su **Avanti**.

Viene visualizzata la pagina **Posizione computer virtuale**.

Nota: Se si crea un computer virtuale istantaneo dalla vista Gestione nodi, vengono elencati solo i Recovery Point Server che si trovano nello stesso sito del nodo di origine. Se si desidera creare un computer virtuale istantaneo dal Recovery Point Server gestito da un sito diverso, accedere a tale sito e aprire la procedura guidata dalla vista Gestione della destinazione.

Selezione della posizione per il computer virtuale

Specificare la posizione del computer virtuale in cui si desidera creare il computer virtuale istantaneo. È possibile specificare un computer virtuale VMware o Microsoft Hyper-V.

Effettuare le operazioni seguenti:

1. Selezionare un tipo di hypervisor.

   VMware vSphere

   a. Selezionare **VMware vSphere**.

   b. Se è stato già aggiunto un nodo VMware al sito selezionato nella Console, selezionare tale nodo dall'elenco a discesa **Host**.

   c. Se non è stato aggiunto alcun nodo VMware, dall'elenco a discesa Host, fare clic su **+Aggiungi nuovo hypervisor**.

      Viene visualizzata la finestra di dialogo Aggiungi hypervisor.

   d. Specificare i dettagli del server VMware vCenter o ESX(i), quindi fare clic su **OK**.

      La finestra di dialogo Aggiungi hypervisor viene chiusa e viene nuovamente visualizzata la pagina **Posizione computer virtuale**. Tutti gli ESX(i) o i pool di risorse vengono visualizzati nel riquadro centrale.

   e. Selezionare l'ESX(i), il cluster, il pool di risorse o l'app virtuale come posizione.

   Il computer VMware vSphere è stato specificato.

   Microsoft Hyper-V

   a. Selezionare **Microsoft Hyper-V**.

   b. Se è stato già aggiunto un nodo Hyper-V al sito selezionato nella Console, selezionare tale nodo dall'elenco a discesa **Server/Cluster Hyper-V**.

   c. Se non è stato aggiunto nessun nodo Hyper-V, fare clic su **Aggiungi**.

      Viene visualizzata la finestra di dialogo **Specifica destinazione del computer virtuale**.

      Nota: Quando ci si connette al computer virtuale istantaneo Hyper-V mediante un account di amministratore locale non integrato, occorre disabilitare il controllo dell'account utente remoto. Per ulteriori informazioni sulla disattivazione del controllo dell'account utente remoto per

l'amministratore non integrato, consultare la sezione Disattivazione del controllo dell'account utente remoto per un amministratore non integrato.

d. Specificare i dettagli del server Hyper-V, quindi fare clic su **OK**.

   Il computer virtuale Hyper-V è stato specificato.

   Nota: il supporto del computer virtuale istantaneo non è in grado di installare il servizio di integrazione nei computer virtuali istantanei con Microsoft Hyper-V 2016 se il nodo di origine è Windows 2008 (o versioni precedenti).

2. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Server di ripristino**.

Disattivazione di un account utente remoto per un amministratore non integrato

L'account amministrativo aggiuntivo fa riferimento agli account che non utilizzano amministratori predefiniti. Tali account vengono detti anche account amministrativi non integrati. Per importare un computer virtuale da un host Hyper-V, è possibile utilizzare l'account di amministratore integrato dell'host Hyper-V, un account di dominio compreso nel gruppo degli amministratori locali dell'host Hyper-V oppure un account utente amministrativo non integrato.

L'utente con un account amministrativo aggiuntivo può attenersi alle procedure per disabilitare l'accesso UAC remoto.

Note:

- Questa procedura non è analoga alla disabilitazione del controllo accesso utente. Permette di disabilitare soltanto alcune funzionalità UAC.
- Poiché viene utilizzata la tecnologia WMI remota per l'importazione, verificare che non sia bloccata dal firewall.

Effettuare le operazioni seguenti:

1. Fare clic su Start, digitare *regedit* nel campo Cerca programmi e file e premere Invio.

   Viene visualizzato l'editor del Registro di sistema di Windows.

   Nota: Potrebbe essere necessario fornire le credenziali di amministratore per accedere all'editor del Registro di sistema di Windows.

2. Individuare e fare clic sulla chiave di registro seguente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. Dal menu Modifica, fare clic su Nuovo e selezionare il valore DWORD (32 bit).
4. Specificare *LocalAccountTokenFilterPolicy* come nome della nuova voce e premere Invio.
5. Fare clic con il tasto destro del mouse su *LocalAccountTokenFilterPolicy*, quindi selezionare Modifica.
6. Specificare 1 nel campo Dati valore e fare clic su OK.
7. Uscire dall'editor del Registro di sistema.

   Per ulteriori informazioni sul comportamento di Windows, consultare la documentazione di Microsoft.

Selezione di un server di ripristino

Il server di ripristino ospita il modulo di base del computer virtuale istantaneo. Il server di ripristino predefinito è il server RPS. È inoltre possibile assegnare un nodo come server di ripristino.

Per le sessioni di backup di Linux, il server di ripristino è un server di backup di Linux.

Effettuare le operazioni seguenti:

1. Selezionare una delle opzioni seguenti per la selezione del server di ripristino:

   Use Recovery Point Server (Usa Recovery Point Server)

   Specifica che il server RPS viene utilizzato come server di ripristino.

   Select a Windows node from the node list (Seleziona un nodo Windows dall'elenco dei nodi)

   Specifica che il server di ripristino è un nodo Windows. È possibile selezionare il nodo dall'elenco. Vengono visualizzati solo i nodi gestiti dal sito selezionato.

   Note:

   - È necessario selezionare un server di ripristino solo quando l'hypervisor è VMware vSphere.
   - Quando l'hypervisor è VMware vSphere, il ruolo Network File System (NFS) di Windows deve essere installato sul Recovery Point Server. Tale ruolo potrebbe venire installato automaticamente dal processo del computer virtuale istantaneo. Per installare manualmente il servizio NFS, consultare la sezione Installazione manuale di NFS su un server Windows.
   - Se Arcserve Backup è installato sul server di ripristino, l'avvio del servizio NFS di Windows potrebbe non riuscire. Ciò si verifica perché il numero di porta predefinito del servizio NFS di Windows (111) è utilizzato dal servizio **Server chiamata di procedura remota** di Arcserve Backup. Per modificare il numero di porta predefinito del servizio **Server di chiamata a procedura remota** di Arcserve Backup, consultare le sezioni Modifica del file di configurazione delle porte e Porte di comunicazione tra server primario e server membro nella documentazione di Arcserve Backup.

2. Fare clic su **Avanti**.

   Viene visualizzata la pagina dei dettagli del computer virtuale istantaneo.

Installazione manuale del file system di rete su un server Windows

È possibile installare manualmente Network File System (NFS) su un server Windows mediante la Gestione server.

Effettuare le operazioni seguenti:

1. Aprire Gestione server e fare clic su Gestisci, quindi sulla procedura guidata Aggiungi ruoli e funzionalità.

   Viene visualizzata la procedura guidata Aggiungi ruoli e funzionalità.

2. Fare clic su Ruoli server, quindi selezionare *Servizi file e archiviazione*.
3. Espandere *File e servizi iSCSI*.
4. Selezionare *File server* e *Server per NFS*.
5. Fare clic su Aggiungi funzionalità per includere le funzionalità NFS selezionate.
6. Fare clic su Installa per installare sul server i componenti NFS necessari.

   Il file system di rete è stato installato manualmente sul server Windows.

Definizione dei dettagli relativi al computer virtuale istantaneo

Specificare i dettagli del computer virtuale istantaneo. Le opzioni possono variare a seconda dell'hypervisor.

Effettuare le operazioni seguenti:

1. Specificare il nome e la descrizione del computer virtuale istantaneo.

   Nome computer virtuale

   Specifica il nome del computer virtuale istantaneo. Il nome del nodo di origine con prefisso diventa il nome predefinito del computer virtuale istantaneo. Per il nome non sono ammessi alcuni caratteri speciali, quali @, \ e così via.

   Descrizione

   (Facoltativo) Specifica la descrizione per il computer virtuale istantaneo.

2. Specificare il percorso della cartella del computer virtuale istantaneo sul server di ripristino.

   È possibile esplorare le informazioni sul volume del server di ripristino.

   Nota: Se si seleziona **VMware vSphere** come posizione del computer virtuale, la cartella selezionata monta l'archivio dati NFS su VMware. Nella cartella del computer locale verrà visualizzata un'icona condivisa. Per impostazione predefinita, l'archivio dati NFS è montato nella stessa posizione della cartella ed è possibile smontarlo solo manualmente dal server VMware ESX(i).

3. Specificare le impostazioni del computer virtuale istantaneo.

   Numero CPU

   Specifica il numero di CPU necessarie nel computer virtuale istantaneo.

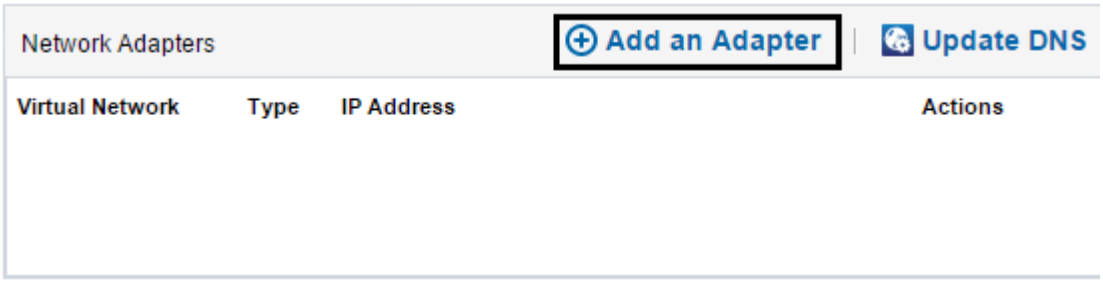
   Dimensioni memoria

   Specifica le dimensioni della memoria necessarie nel computer virtuale istantaneo.

4. Aggiungere le schede di rete.

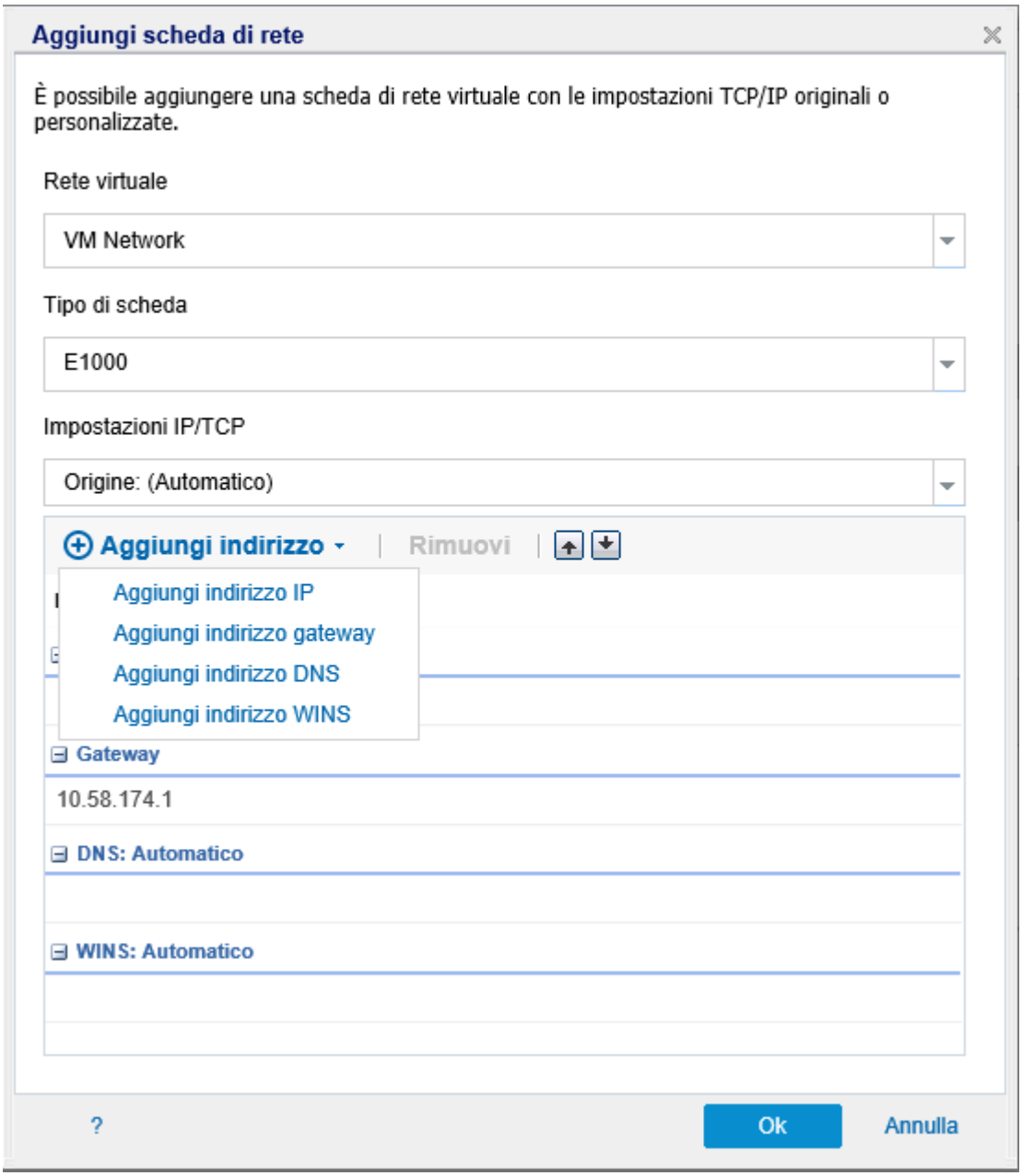
   Nota: Per un computer virtuale istantaneo di Linux, è possibile utilizzare almeno una scheda NIC virtuale per la connessione al server di backup Linux.

   a. Fare clic sul pulsante **Aggiungi una scheda** per aggiungere una scheda e specificare i dettagli della rete.



Si possono aggiungere più schede di rete. Una volta aggiunta la scheda di rete, è possibile modificarla ed eliminarla dalla colonna **Azioni**.

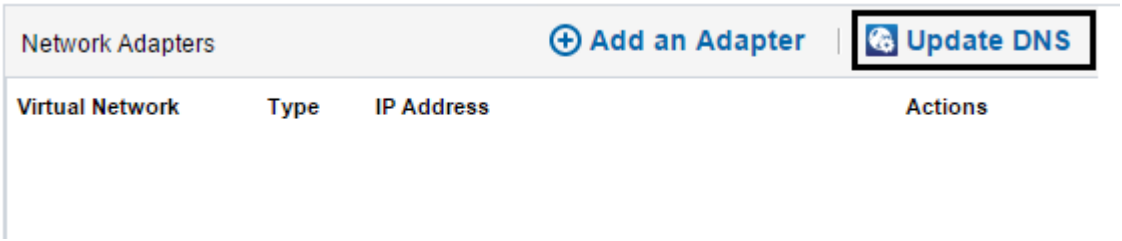
b. Specificare la **rete virtuale**, il **tipo di scheda** e le **impostazioni TCP/IP**. Per specificare l'indirizzo IP del computer virtuale istantaneo, fare clic sull'opzione **Aggiungi indirizzo**, quindi selezionare l'indirizzo da configurare.



5. Aggiornare il DNS.

   Nota: Questa funzione è disponibile solo per i computer virtuali istantanei di Windows.

   a. Fare clic sul pulsante **Aggiorna DNS** per specificare i dettagli del DNS.



Nota: Se sono stati indicati gli indirizzi IP e DNS in Scheda di rete e il computer di origine è compreso in un dominio, è possibile specificare le informazioni dettagliate per Aggiorna DNS.

b. Fare clic sull'opzione **Aggiungi indirizzo DNS** per aggiungere un record di aggiornamento DNS. Fare clic sul pulsante **Rimuovi** per rimuovere il record di aggiornamento DNS. Fare clic sui pulsanti Su e Giù per modificare l'ordine dei record.



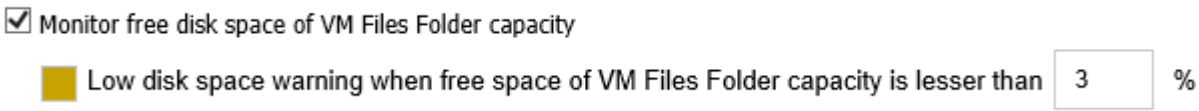
c. Selezionare un indirizzo DNS e un indirizzo IP dall'elenco a discesa, quindi fare clic su **OK**.

d. Specificare la **durata** (TTL).

e. Specificare l'autenticazione DNS.

Per i server DNS di Microsoft, immettere nome utente e password. Per i server Bind, è necessario specificare il percorso completo, compreso il nome del file di chiave sul server di ripristino.

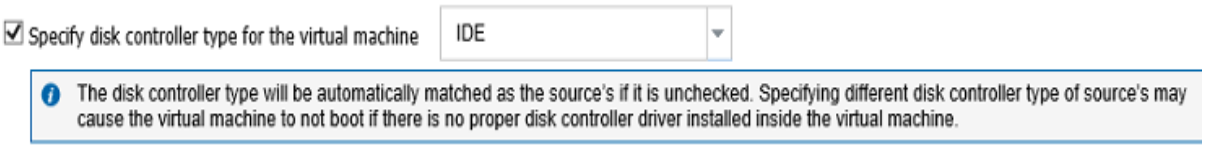
6. Verificare lo spazio libero su disco della capacità della cartella del file del computer virtuale.



Nota: La casella di controllo **Monitora spazio libero su disco per la capacità della cartella di file del computer virtuale** è selezionata per impostazione predefinita. La barra di capacità viene visualizzata in giallo nella pagina Computer virtuale istantaneo se lo spazio libero della capacità della cartella del file del computer virtuale è minore del valore di soglia. Il valore di soglia predefinito è 3%. È possibile modificare il valore, se necessario.

7. Selezionare la casella di controllo **Specificare il tipo di controller disco per il computer virtuale** e selezionare il tipo di controller del disco per il computer virtuale

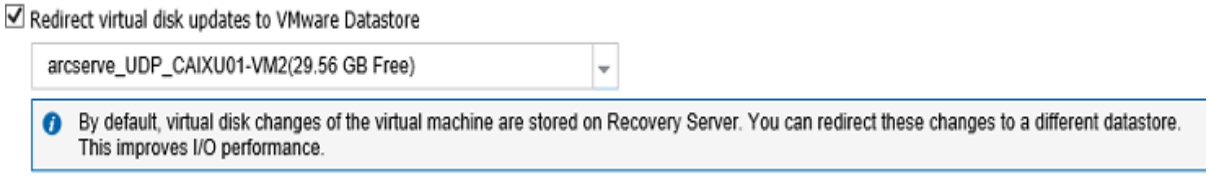
dall'elenco a discesa.



Nota: La casella di controllo **Specificare il tipo di controller disco per il computer virtuale** è disponibile se è stato selezionato **VMware vSphere** come posizione del computer virtuale.

Il computer virtuale istantaneo viene creato mediante l'applicazione del controller del disco specificato in VMware.

8. Per reindirizzare gli aggiornamenti del disco virtuale all'archivio dati di VMware, procedere come segue:
   a. Selezionare la casella di controllo **Reindirizza aggiornamenti del disco virtuale all'archivio dati VMware**.

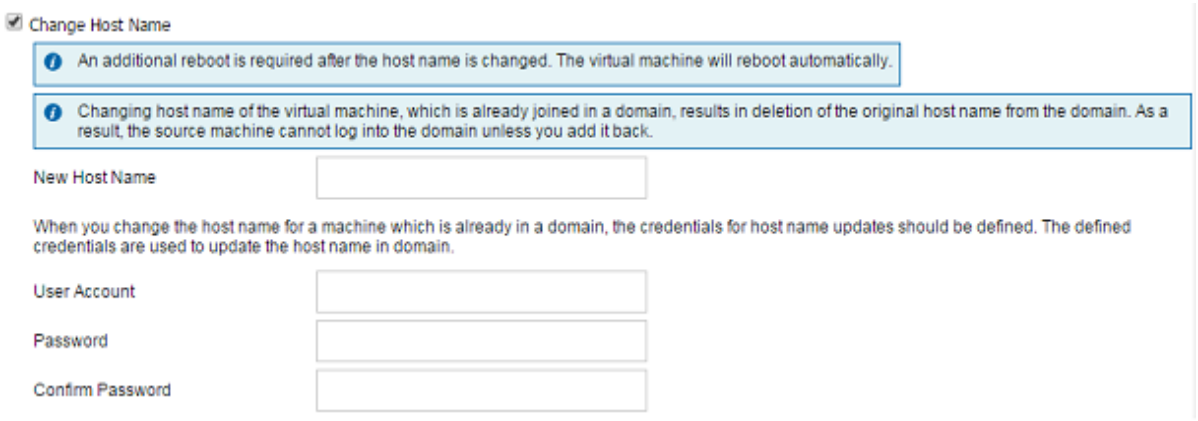


   Nota: La casella di controllo **Reindirizza aggiornamenti del disco virtuale all'archivio dati VMware** è disponibile se è stato selezionato **VMware vSphere** come posizione del computer virtuale.

   b. Selezionare l'archivio dati VMware necessario dall'elenco a discesa.

   Gli aggiornamenti del disco virtuale vengano reindirizzati all'archivio dati VMware selezionato.

9. Per modificare il nome host del computer virtuale istantaneo, procedere come segue:
   a. Selezionare la casella di controllo **Modifica nome host** per aggiornare il nome host del computer virtuale istantaneo.



b. Specificare un nuovo nome host per il computer virtuale istantaneo. Se il computer di origine è compreso in un dominio, immettere l'account utente e la password associata.

Nota: Se il computer di origine è compreso in un dominio, l'account deve disporre dell'autorizzazione per modificare il nome host nel dominio.

10. (Facoltativo) Per il **computer virtuale istantaneo di Linux**, selezionare l'opzione **Ripristina i dati automaticamente dopo l'avvio del computer virtuale istantaneo** per abilitare il ripristino automatico dei dati con l'avvio del computer virtuale istantaneo di destinazione.

    Il comportamento predefinito del **computer virtuale istantaneo di Linux** deve innanzitutto eseguire il ripristino dei dati necessari e avviare il computer virtuale. Se l'opzione non è selezionata, quando il computer virtuale viene avviato, i dati restanti non vengono ripristinati, anche nel caso in cui vengano utilizzati come computer virtuale normale. Se l'opzione è attivata, i dati rimanenti vengono ripristinati sul backend durante l'utilizzo del computer virtuale. È inoltre possibile salvare la destinazione del computer virtuale istantaneo in modo permanente una volta completato il ripristino dei dati.

    Nota: quando lo stato del computer virtuale istantaneo di Linux di destinazione non è attivato, il processo del computer virtuale non riesce. Se tale punto di ripristino viene unito, il computer virtuale istantaneo di Linux non viene attivato.

    A questo punto è possibile inoltrare il processo.

Invio del processo del computer virtuale istantaneo

Per creare il computer virtuale istantaneo, inviare il processo del computer virtuale istantaneo. Una volta completato il processo, è possibile visualizzare il computer virtuale istantaneo in **Risorse**, **Infrastruttura Computer virtuale istantaneo**.

Effettuare le operazioni seguenti:

1. Fare clic su **Fine**.

   Viene visualizzata la finestra di dialogo **Avvia computer virtuale**.

2. Selezionare una delle seguenti opzioni:

   Avvia ora

   Invia un processo per creare il computer virtuale istantaneo. Al termine del processo di creazione del computer virtuale, avvia automaticamente il computer virtuale.

   Avvia più tardi

   Crea un computer virtuale istantaneo. È necessario avviare manualmente il computer virtuale. È possibile avviare il computer virtuale una volta completato il processo del computer virtuale istantaneo.

   Annulla

   Chiude la finestra di dialogo Crea computer virtuale senza creare alcun computer virtuale. Viene visualizzata di nuovo la pagina Crea computer virtuale.

Il processo computer virtuale istantaneo è stato creato correttamente.

Gestione di un computer virtuale istantaneo

È possibile gestire il computer virtuale istantaneo dalla console. È possibile attivare o spegnere un computer virtuale istantaneo dalla console. Inoltre, è possibile eliminare qualsiasi computer virtuale istantaneo.

Nota: La console visualizza soltanto i computer virtuali istantanei creati dai punti di ripristino gestiti dal sito selezionato.

- Avvio o arresto di un computer virtuale istantaneo
- Riavvio di un computer virtuale istantaneo
- Eliminazione di un computer virtuale istantaneo
- Conversione del computer virtuale istantaneo Linux in un computer virtuale indipendente
- Migrazione del computer virtuale istantaneo Linux in un computer fisico

Avvio o arresto di un computer virtuale istantaneo

È possibile avviare o interrompere un computer virtuale istantaneo dopo la creazione. Il pulsante Avvia o Interrompi viene visualizzato a seconda dello stato del computer virtuale.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Accedere a **Infrastrutture** e fare clic su **Computer virtuale istantaneo**.
3. Selezionare il computer virtuale dal riquadro centrale e fare clic su **Azioni**.
4. Selezionare **Attiva** o **Disattiva** a seconda dello stato del computer virtuale.

   Il computer virtuale si avvia o si arresta correttamente.

Riavvio di un computer virtuale istantaneo

È possibile riavviare un computer virtuale istantaneo dopo la creazione.

Nota: È possibile riavviare un computer virtuale istantaneo solo se è in stato **Non riuscito/Arresto anomalo del processo**

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Accedere a **Infrastrutture**, quindi fare clic su **Computer virtuale istantaneo**.
3. Selezionare il computer virtuale con stato **Non riuscito/Arresto anomalo del processo** dal riquadro centrale, quindi fare clic su **Azioni**.
4. Fare clic su **Riavvia**.

   Il computer virtuale viene riavviato.

Eliminazione di un computer virtuale istantaneo

È possibile eliminare qualsiasi computer virtuale istantaneo che non è più necessario.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Accedere a **Infrastrutture** e fare clic su **Computer virtuale istantaneo**.
3. Selezionare il computer virtuale dal riquadro centrale e fare clic su **Azioni**.
4. Fare clic su **Elimina**.

   Viene visualizzata una finestra di dialogo di conferma.
5. Fare clic su **OK**.

   Il computer virtuale viene eliminato correttamente.

Conversione del computer virtuale istantaneo Linux in un computer virtuale indipendente

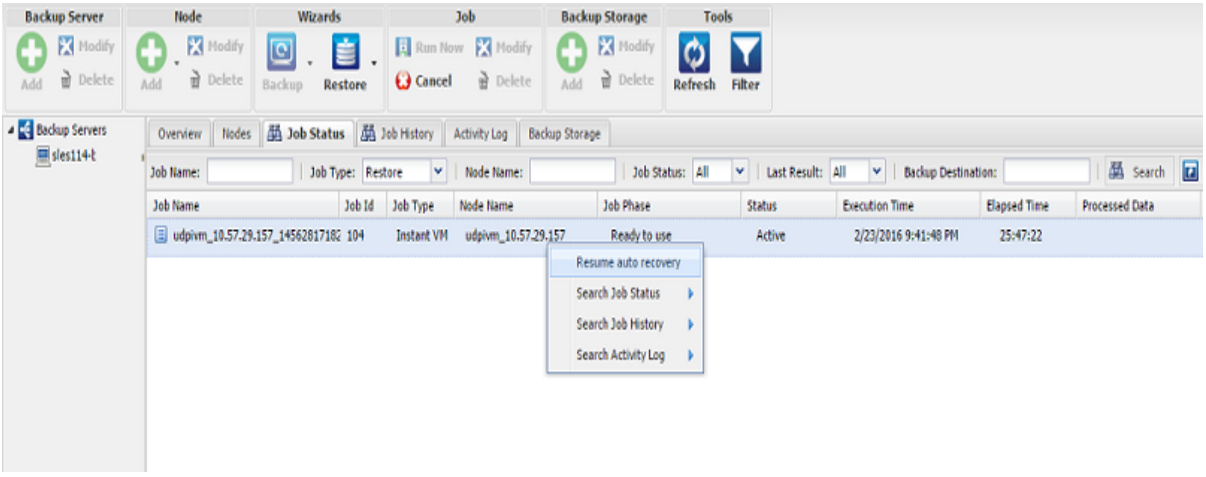
È possibile modificare un computer virtuale istantaneo Linux (IVM) su un computer virtuale indipendente (VM).

Note:

- Per procedere, è necessaria una voce del menu disponibile solo in seguito all'esecuzione da parte del computer virtuale indipendente della fase di processo Pronto per l'uso.
- La voce del menu non è disponibile se il punto di ripristino è un backup senza agente e l'hypervisor di destinazione è vSphere ESX/VC. È necessario utilizzare VMware Storage vMotion per convertire il computer virtuale istantaneo in un computer virtuale indipendente.

Effettuare le operazioni seguenti:

1. Aprire l'interfaccia utente del server di backup Linux.



2. Dalla scheda Stato processo, selezionare il processo del computer virtuale istantaneo, quindi fare clic con il pulsante destro del mouse sul menu di scelta rapida.
3. Selezionare Riprendi ripristino automatico.

   Il processo del computer virtuale istantaneo viene spostato in Cronologia processo in seguito al completamento del processo.

Migrazione del computer virtuale istantaneo Linux in un computer fisico

Per eseguire la migrazione del computer virtuale istantaneo di Linux su un computer fisico, consultare la sezione **Esecuzione di un ripristino bare metal di migrazione per computer Linux** nella *Guida per l'utente dell'agente per Linux*.

Modalità di creazione e gestione di un computer virtuale istantaneo su Amazon EC2

Il computer virtuale istantaneo supporta la creazione istantanea di un computer virtuale su Amazon EC2. Il computer virtuale istantaneo su Amazon EC2 apporta i seguenti vantaggi:

- Consente l'accesso immediato ai dati e alle applicazioni presenti nelle sessioni di backup di Arcserve UDP.
- Elimina i tempi di inattività associati a un ripristino tradizionale o alla conversione della sessione di backup in un computer virtuale.
- Fornisce una posizione alternativa per la creazione di un computer virtuale su cloud, anziché in locale.

È possibile creare un computer virtuale istantaneo dalle sessioni di backup seguenti:

- Backup di Linux basato su agente
- Backup senza agente basato su host

Come procedere?

- Verifica dei prerequisiti
- Creazione di un piano del computer virtuale istantaneo su Amazon EC2
- Gestione di un piano del computer virtuale istantaneo su Amazon EC2

È possibile creare un computer virtuale istantaneo dalle seguenti sessioni di backup: al completamento del processo, verrà creato un computer virtuale istantaneo su Amazon EC2.

Verifica dei prerequisiti per un computer virtuale istantaneo su Amazon EC2

Completare i prerequisiti seguenti prima di creare un computer virtuale istantaneo:

- Dalla matrice di compatibilità, verificare se il computer virtuale è supportato da Amazon EC2 e UDP.
- Verificare che sia presente almeno un Recovery Point Server sul computer locale come destinazione di backup.
- Verificare che sia presente almeno un Recovery Point Server su Amazon EC2 come destinazione di replica.
- Verificare che sia presente almeno un server locale di backup Linux per il processo di backup.
- Verificare che sia presente almeno un server di backup Linux per Amazon EC2 per il processo del computer virtuale istantaneo.
- Verificare che l'account Amazon EC2 disponga di quote dell'istanza in esecuzione per il computer virtuale istantaneo.

Limitazioni

I backup del computer virtuale Windows di tipo basato sull'agente e senza agente basato sull'host NON sono supportati.

Creazione di un computer virtuale istantaneo su Amazon EC2

La creazione di un computer virtuale istantaneo richiede i cinque passaggi seguenti:

1. Apertura della procedura guidata del computer virtuale istantaneo
2. Selezione del punto di ripristino
3. Selezione della posizione del computer virtuale
4. Selezione del server di ripristino
5. Definizione dei dettagli del computer virtuale istantaneo
6. Invio del processo del computer virtuale istantaneo

Apertura della procedura guidata del computer virtuale istantaneo

È possibile configurare e creare un computer virtuale istantaneo mediante la procedura guidata del computer virtuale istantaneo. Esistono tre metodi per aprire la procedura guidata del computer virtuale istantaneo:

- Dalla gestione del nodo
- Dalla vista Gestione della destinazione: Recovery Point Server
- Dalla vista Gestione della destinazione: Cartella condivisa

Aprire la procedura guidata dalla visualizzazione Gestione nodi

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.
3. Tutti i nodi vengono visualizzati nel riquadro centrale.
4. Fare clic con il tasto destro del mouse e selezionare **Crea un computer virtuale istantaneo**.

   Viene visualizzata la procedura guidata del computer virtuale.

   Nota: Se un nodo non è associato ad alcun piano, tale nodo non dispone dell'opzione **Crea computer virtuale istantaneo**.

Aprire la procedura guidata dalla visualizzazione della Gestione destinazione

Da Destinazioni: Recovery Point Server

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Se sono stati aggiunti degli archivi dati, essi vengono visualizzati nel riquadro centrale.
3. Fare clic sull'archivio dati.

   Se è già stato eseguito il backup dei dati sul server RPS, tutti i nodi di origine vengono elencati nel riquadro.
4. Fare clic con il tasto destro del mouse e selezionare **Crea un computer virtuale istantaneo**.

   Viene visualizzata la procedura guidata del computer virtuale.

Da Destinazioni: Cartella condivisa

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni** e fare clic su **Cartelle condivise**.
3. Se sono stati aggiunte cartelle condivise, esse vengono visualizzate nel riquadro centrale.
4. Fare clic su una cartella condivisa e selezionare **Browser punto di ripristino**.

   Se è già stato eseguito il backup dei dati sulla cartella condivisa, tutti i nodi di origine vengono elencati nel riquadro.
5. Fare clic con il tasto destro del mouse su un nodo e scegliere **Crea un computer virtuale istantaneo**.

   Viene visualizzata la procedura guidata del computer virtuale.

Seleziona punto di ripristino

La pagina Seleziona punto di ripristino consente di visualizzare la posizione del punto di ripristino e di selezionarlo. Il punto di ripristino può trovarsi in una posizione condivisa o in un archivio dati nel server RPS.

La console riconosce automaticamente la posizione del punto di ripristino e preseleziona i campi **Tipo di posizione**, **Recovery Point Server** e **Archivio dati** o **Cartella di condivisione di rete**.

Nota: Selezionare la sessione Recovery Point Server (cartella condivisa) come destinazione di replica per risparmiare tempo e larghezza di banda della rete.

Espandere l'elenco Data, selezionare il punto di ripristino richiesto dall'elenco e fare clic su **Avanti**.

Viene visualizzata la pagina **Posizione computer virtuale**.

Nota: Se si crea un computer virtuale istantaneo dalla vista Gestione nodi, vengono elencati solo i Recovery Point Server che si trovano nello stesso sito del nodo di origine. Se si desidera creare un computer virtuale istantaneo dal Recovery Point Server gestito da un sito diverso, accedere a tale sito e aprire la procedura guidata dalla vista Gestione della destinazione.

Selezione della posizione per il computer virtuale

Specificare la posizione del computer virtuale in cui creare il computer virtuale istantaneo. È possibile specificare Amazon EC2 oppure Amazon EC2 (China) in base al tipo di account.

Effettuare le operazioni seguenti:

1. Selezionare Amazon EC2 o Amazon EC2 (China).
2. Selezionare il nome dell'account.

   Nota: Selezionare l'account corrispondente, se non è stato aggiunto, e consultare la sezione Aggiunta di un account cloud.
3. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Server di ripristino**.

Selezione di un server di ripristino

Il server di ripristino ospita il modulo di base del computer virtuale istantaneo. Il server di ripristino predefinito è il server RPS. È inoltre possibile assegnare un nodo come server di ripristino.

Per le sessioni di backup di Linux, il server di ripristino è un server di backup di Linux.

Effettuare le operazioni seguenti:

1. Selezionare il server di backup Linux dall'elenco dei nodi.

   Note: Selezionare la sessione Recovery Point Server (cartella condivisa) come destinazione di replica per risparmiare tempo e larghezza di banda della rete.

2. Fare clic su **Avanti**.

   Viene visualizzata la pagina dei dettagli del computer virtuale istantaneo.

Definizione dei dettagli relativi al computer di virtuale istantaneo

Specificare i dettagli del computer virtuale istantaneo.

Effettuare le operazioni seguenti:

1. Specificare il nome e la descrizione del computer virtuale istantaneo.

   Nome computer virtuale

   Specifica il nome del computer virtuale istantaneo. Il prefisso del nome del nodo di origine con "UDPIVM_" diventa il nome predefinito del computer virtuale istantaneo. È possibile modificare il nome. Alcuni caratteri speciali, come '@', \ e così via non sono consentiti nel nome.

   Descrizione

   (Facoltativo) Specifica la descrizione per il computer virtuale istantaneo.

   Area

   Specifica l'area geografica del proprio account Amazon EC2.

   Tipo di istanza

   Specifica il tipo di istanza supportato.

   Tipo di volume

   Specifica il tipo di volume.

   Rete

   Specifica la rete esistente sull'account Amazon EC2.

   Subnet

   Specifica la subnet esistente sull'account Amazon EC2.

   IP pubblico con assegnazione automatica

   Specifica l'indirizzo IP pubblico assegnato al computer virtuale .

   IP principale

   Specificare l'IP principale del computer virtuale. Specifica l'opzione automaticamente, nel caso in cui non venga specificata.

   Selezione di un gruppo di protezione

   Specifica il gruppo di protezione. È possibile selezionare più gruppi. Se non viene selezionata alcuna opzione, crea automaticamente un nuovo gruppo di protezione.

Avanzate: Modifica nome host

Specifica il nome host del nuovo computer di destinazione.

Avanzate: Ripristina dati automaticamente dopo l'avvio del computer virtuale istantaneo

Specifica se il ripristino dei dati viene eseguito automaticamente dopo aver creato il computer virtuale istantaneo.

2. Fare clic su **Fine**.

A questo punto è possibile inoltrare il processo.

Invio del processo del computer virtuale istantaneo

Per creare il computer virtuale istantaneo, inviare il processo del computer virtuale istantaneo. Una volta completato il processo, è possibile visualizzare il computer virtuale istantaneo in **Risorse**, **Infrastruttura Computer virtuale istantaneo**.

Effettuare le operazioni seguenti:

1. Fare clic su **Crea computer virtuale**.

   Viene visualizzata la finestra di dialogo **Crea computer virtuale**.

2. Selezionare una delle seguenti opzioni:

   Avvia ora

   Invia un processo per creare il computer virtuale istantaneo. Al termine del processo di creazione del computer virtuale, avvia automaticamente il computer virtuale.

   Avvia più tardi

   Crea un computer virtuale istantaneo. È necessario avviare manualmente il computer virtuale. È possibile avviare il computer virtuale una volta completato il processo del computer virtuale istantaneo.

   Annulla

   Chiude la finestra di dialogo Crea computer virtuale senza creare alcun computer virtuale. Viene visualizzata di nuovo la pagina Crea computer virtuale.

Il processo computer virtuale istantaneo è stato creato correttamente.

Gestione di un computer virtuale istantaneo

È possibile gestire il computer virtuale istantaneo dalla console. È possibile attivare o spegnere un computer virtuale istantaneo dalla console. Inoltre, è possibile eliminare qualsiasi computer virtuale istantaneo.

Nota: nella console vengono visualizzati soltanto i computer virtuali istantanei creati a partire dai punti di ripristino gestiti dal sito selezionato.

- Avvio o arresto di un computer virtuale istantaneo
- Riavvio di un computer virtuale istantaneo
- Eliminazione di un computer virtuale istantaneo
- Conversione del computer virtuale istantaneo Linux in un computer virtuale indipendente
- Migrazione del computer virtuale istantaneo Linux in un computer fisico

Avvio o arresto di un computer virtuale istantaneo

È possibile avviare o interrompere un computer virtuale istantaneo dopo la creazione. Il pulsante Avvia o Interrompi viene visualizzato a seconda dello stato del computer virtuale.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Accedere a **Infrastrutture** e fare clic su **Computer virtuale istantaneo**.
3. Selezionare il computer virtuale dal riquadro centrale e fare clic su **Azioni**.
4. Selezionare **Attiva** o **Disattiva** a seconda dello stato del computer virtuale.

   Il computer virtuale si avvia o si arresta correttamente.

Riavvio di un computer virtuale istantaneo

È possibile riavviare un computer virtuale istantaneo dopo la creazione.

Nota: È possibile riavviare un computer virtuale istantaneo solo se è in stato **Non riuscito/Arresto anomalo del processo**

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Accedere a **Infrastrutture**, quindi fare clic su **Computer virtuale istantaneo**.
3. Selezionare il computer virtuale in stato **Non riuscito/Arresto anomalo** dal riquadro centrale, quindi fare clic su **Azioni**.
4. Fare clic su **Riavvia**.

   Il computer virtuale viene riavviato.

Eliminazione di un computer virtuale istantaneo

È possibile eliminare qualsiasi computer virtuale istantaneo che non è più necessario.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Accedere a **Infrastrutture** e fare clic su **Computer virtuale istantaneo**.
3. Selezionare il computer virtuale dal riquadro centrale e fare clic su **Azioni**.
4. Fare clic su **Elimina**.

   Viene visualizzata una finestra di dialogo di conferma.
5. Fare clic su **OK**.

   Il computer virtuale viene eliminato correttamente.

Conversione del computer virtuale istantaneo Linux in un computer virtuale indipendente

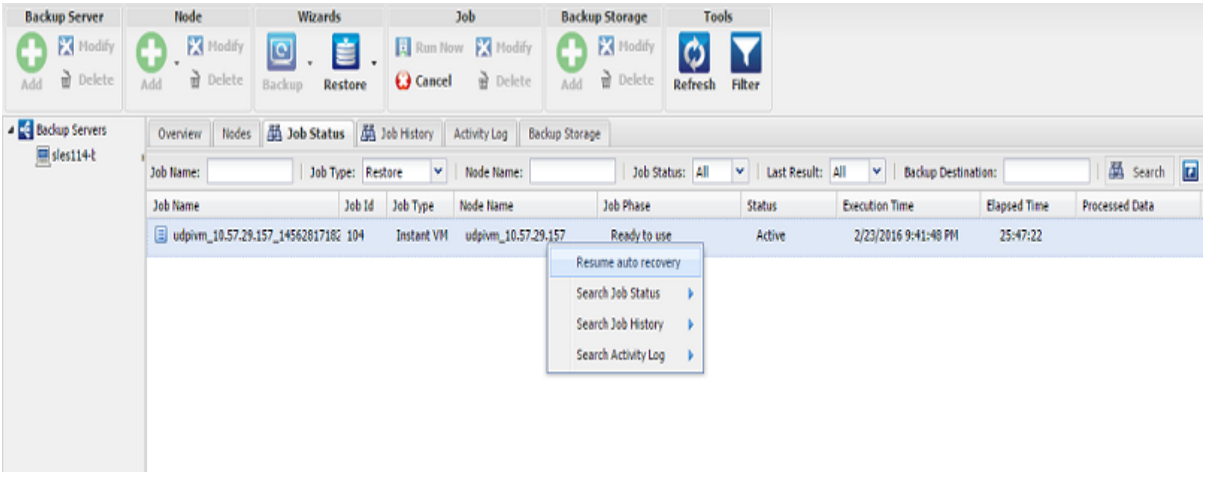
È possibile modificare un computer virtuale istantaneo Linux (IVM) su un computer virtuale indipendente (VM).

Note:

- Per procedere, è necessaria una voce del menu disponibile solo in seguito all'esecuzione da parte del computer virtuale indipendente della fase di processo Pronto per l'uso.
- La voce del menu non è disponibile se il punto di ripristino è un backup senza agente e l'hypervisor di destinazione è vSphere ESX/VC. È necessario utilizzare VMware Storage vMotion per convertire il computer virtuale istantaneo in un computer virtuale indipendente.

Effettuare le operazioni seguenti:

1. Aprire l'interfaccia utente del server di backup Linux.



2. Dalla scheda Stato processo, selezionare il processo del computer virtuale istantaneo, quindi fare clic con il pulsante destro del mouse sul menu di scelta rapida.
3. Selezionare Riprendi ripristino automatico.

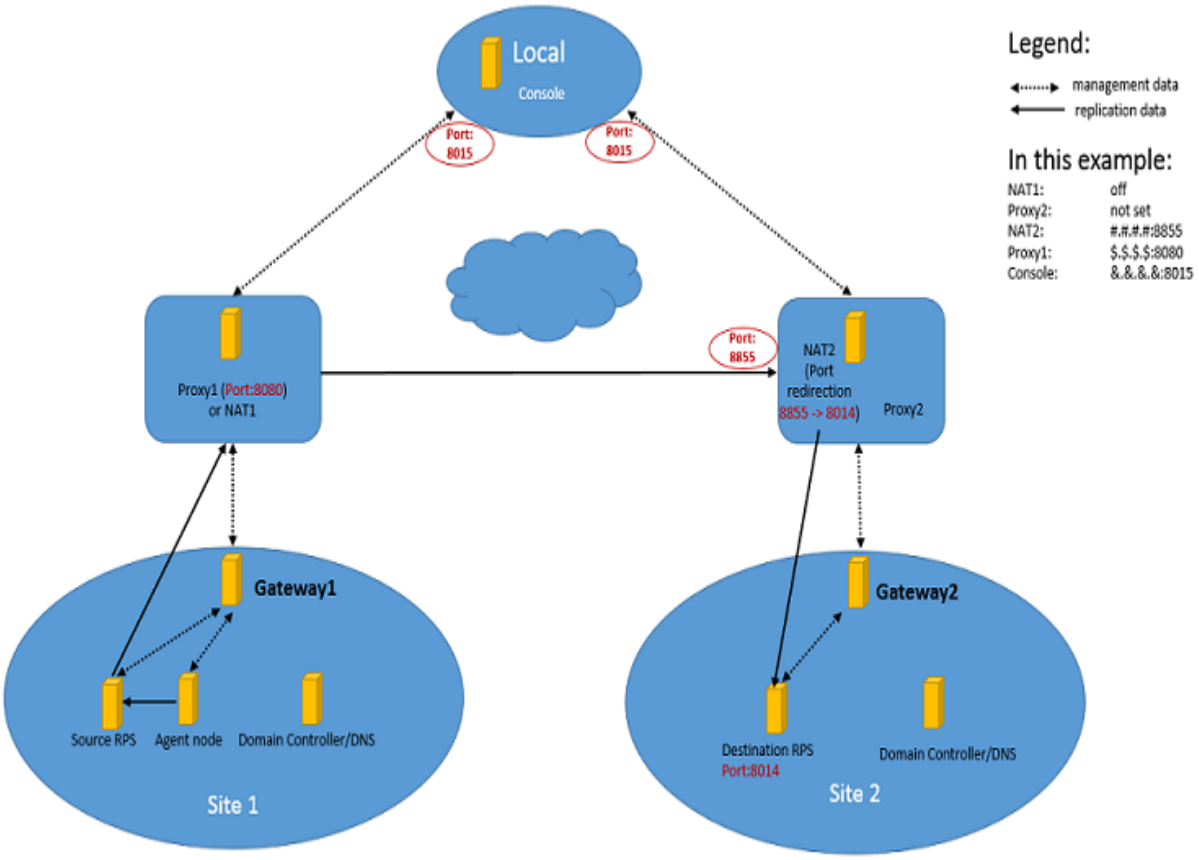
   Il processo del computer virtuale istantaneo viene spostato in Cronologia processo in seguito al completamento del processo.

Migrazione del computer virtuale istantaneo Linux da Amazon EC2 in un computer fisico

Per eseguire la migrazione del computer virtuale istantaneo di Linux su un computer fisico, consultare la sezione **Esecuzione di un ripristino bare metal di migrazione per computer Linux da Amazon EC2 in locale** nella *Guida per l'utente dell'agente per Linux*.

Creazione di un piano per la replica intersito

La funzionalità di replica intersito permette di utilizzare la stessa console per la replica dei dati tra siti diversi. Il diagramma seguente illustra la connessione tra console, Sito 1 e Sito 2:



La console (rete pubblica), il Sito 1 (rete privata) e il Sito 2 (altra rete privata) possono trovarsi in segmenti di rete diversi. Il Sito 1 e il Sito 2 sono gestiti dalla console tramite il gateway.

Il diagramma offre un esempio per illustrare questa funzionalità di UDP valido a titolo di riferimento dal momento che l'ambiente in uso potrebbe essere diverso da quello descritto. L'esempio mira a replicare i dati dal server RPS di origine del Sito 1 al server RPS di destinazione del Sito 2. Il gateway del Sito 1 e del Sito 2 stabilisce la connessione alla console via proxy o NAT. Eseguire la configurazione proxy e NAT correttamente.

Descrizione del diagramma:

- Proxy1 o NAT1 dispongono di un'interfaccia pubblica e di una privata. Ad esempio, IP-1, ossia l'indirizzo IP pubblico, si trova nello stesso segmento della

console, mentre IP-2, ossia l'indirizzo IP privato, è nello stesso segmento del Sito 1. Nell'impostazione di rete del computer Gateway1, il gateway predefinito è impostato sull'indirizzo IP privato di Proxy1 o NAT1.

- Anche Proxy2 e NAT2 presentano la stessa impostazione di Proxy1/NAT1, eccetto che NAT2 necessita di un'ulteriore configurazione della regola di reindirizzamento porte in modo che sia possibile accedere dalla rete pubblica al servizio privato mediante questo mapping. Nell'esempio descritto, il server RPS di origine attraverso il quale avviene il reindirizzamento della porta NAT2 può stabilire la connessione al server RPS di destinazione.
- In un sistema operativo Windows Server 2012R2, sia l'interfaccia utente che i comandi di Windows consentono di impostare l'indirizzamento delle porte per NAT. Il seguente comando di esempio indica di inserire l'indirizzo dal browser Web del server RPS di origine https o http://<NAT2 IP-1>:<port number=8855> affinché avvenga il reindirizzamento al server RPS di destinazione https o http://<destination RPS IP=192.168.30.102>:8014. In questo modo è possibile eseguire la replica intersito.

netsh interface portproxy add v4tov4 listenport=8855 connectaddress="192.168.30.102" connectport=8014 protocol=tcp

Creazione di un piano per la replica intersito

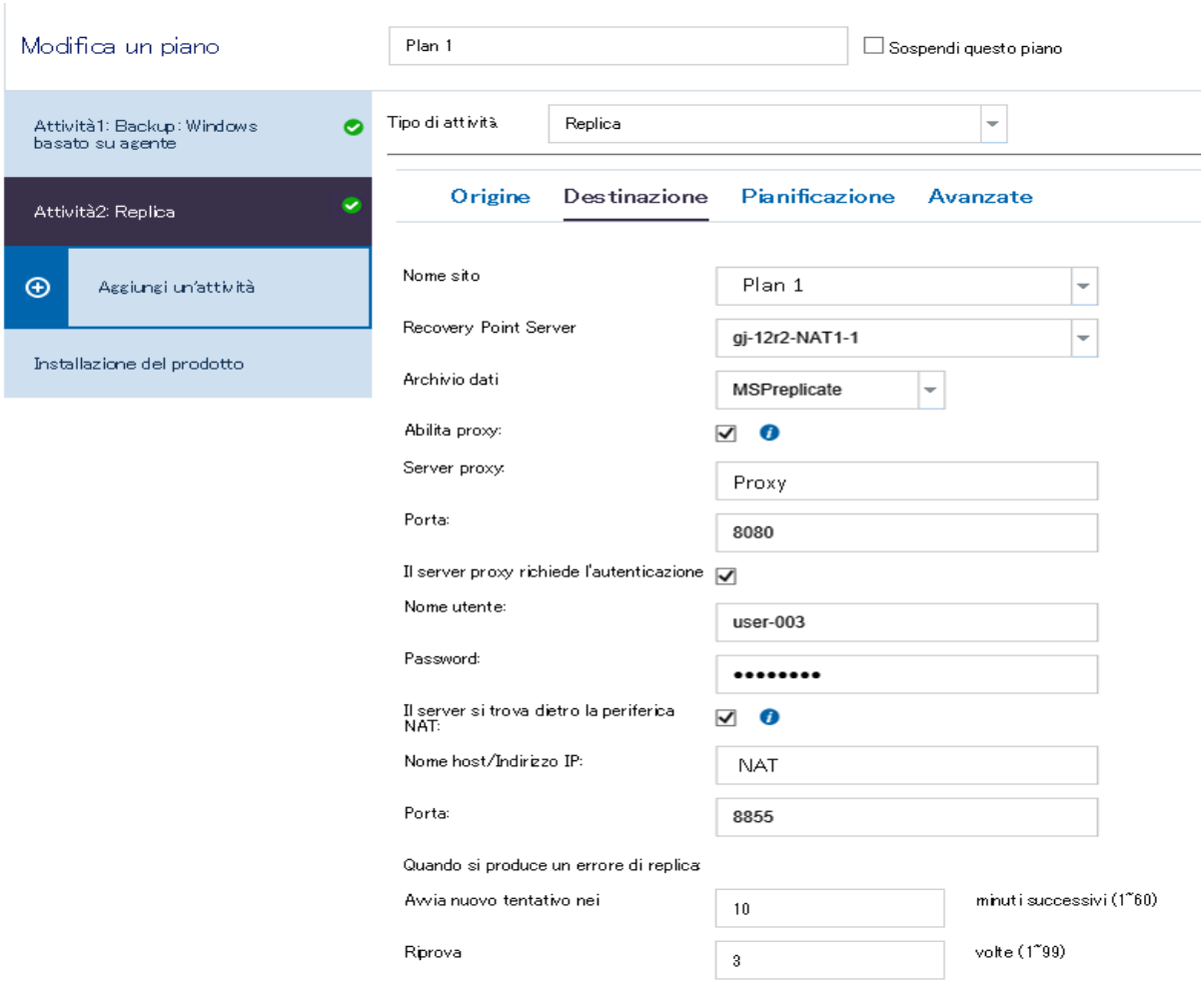
È possibile creare un piano per la replica intersito.

Effettuare le operazioni seguenti:

1. Nel Sito 1, che rappresenta il server RPS di origine, creare l'attività di backup Attività1.
2. Aggiungere allo stesso piano l'attività di **replica**.
3. Nella scheda **Destinazione**, selezionare l'altro sito (il Sito 2 nell'esempio) in cui si trova l'archivio dati o il server RPS di destinazione.
4. (Facoltativo) Abilitare i dettagli del proxy (server, porta e autenticazione).

   Nota: Prima di abilitare i dettagli del proxy, è necessario configurare il server proxy tra il Sito 1 e la console.
5. (Facoltativo) Abilitare i dettagli NAT.

   Nota: Prima di abilitare i dettagli NAT, è necessario configurare il server NAT e il reindirizzamento delle porte tra la console e il Sito 2.



6. Configurare le altre schede, quali **Pianificazione** e **Avanzate**, quindi salvare il piano.
7. Durante l'esecuzione del processo, verificare lo stato del computer di monitoraggio e del registro per il backup, la replica in uscita e la replica in entrata.

Protezione dei dati di Microsoft Office 365

La presente sezione descrive i seguenti argomenti:

Autenticazione moderna

In questa sezione vengono fornite informazioni su come configurare i prerequisiti per i backup di Office 365 utilizzando l'autenticazione moderna. Per effettuare la configurazione, attenersi alla procedura seguente:

1. Preparazione del computer proxy
2. Configurazione di un'applicazione nel portale Azure
3. Assegnazione delle autorizzazioni di amministratore globale all'applicazione Azure
4. Download del certificato da UDP e caricamento in Azure
5. Assegnazione del ruolo di rappresentazione dell'applicazione all'account utente specificato per il backup

Preparazione del computer proxy

Questa sezione fornisce informazioni su come preparare il computer proxy.

Effettuare le operazioni seguenti:

1. Installare PowerShell versione 5.1 o versioni successive (appartenente a Windows Management Framework (WMF)).

   Nota: per verificare la versione di PowerShell, eseguire il seguente comando:

   Get-Host | Select-Object Version

2. Per installare i componenti di sistema richiesti, eseguire una delle seguenti operazioni:
   - Per installare automaticamente i componenti di sistema richiesti, procedere come segue:
     a. Scaricare lo script PowerShell. Per eseguire il download, fare clic su *Script2InstallPrerequisites.ps1_*.
     b. Rinominare *Script2InstallPrerequisites.ps1_* in *Script2InstallPrerequisites.ps1*.
     c. Aprire la finestra di PowerShell utilizzando l'opzione *Esegui come amministratore*, quindi eseguire *Script2InstallPrerequisites.ps1*.

- Per installare manualmente i componenti di sistema richiesti, eseguire i seguenti comandi PowerShell:
  - *Install-Module -Name AzureAD -Force*
  - *Install-Module -Name ExchangeOnlineManagement -Force*
  - *Install-Module -Name PackageManagement -Force*
  - *Install-Module -Name PowerShellGet -Force*

  Nota: quando si installano i moduli PowerShell utilizzando i comandi precedenti, è possibile che venga installata una versione più recente dei moduli in base alla versione GA del componente disponibile nel repository Microsoft.

Configurazione di un'applicazione nel portale Azure

In questa sezione vengono fornite informazioni su come configurare un'applicazione nel portale Azure.

Effettuare le operazioni seguenti:

1. Accedere al portale Azure.
2. Per accedere alla pagina di registrazione dell'applicazione, eseguire una delle seguenti operazioni:
   - Dal riquadro sinistro, selezionare **Azure Active Directory** e nel riquadro destro fare clic su **Registrazioni app**.
   - Cercare Registrazioni app nella barra di ricerca, quindi selezionare **Registrazioni app**.
3. Nella pagina Registrazioni app, fare clic su **Nuova registrazione**.
4. Nella pagina Registrazione di un'applicazione, effettuare le operazioni descritte di seguito, quindi fare clic su **Registra**.
   - Nome: immettere un nome per l'applicazione. Ad esempio, *UDP365*.
   - Tipi di account supportati: selezionare l'opzione **Accounts in this organizational directory only ("your-domain" only – Single tenant)**.
5. Copiare e salvare l'**ID applicazione (client)** per un utilizzo futuro.

Assegnazione delle autorizzazioni di amministratore globale all'applicazione Azure

In questa sezione vengono fornite informazioni su come assegnare le autorizzazioni di amministratore globale all'applicazione Azure.

Per assegnare il ruolo di amministratore globale all'app AzureAD, eseguire una delle seguenti operazioni:

- Per assegnare automaticamente il ruolo, procedere come segue:
  1. Scaricare lo script PowerShell. Per eseguire il download, fare clic su *AssignGlobalAdminRoleToADApplication.ps1*.
  2. Aprire la finestra di PowerShell utilizzando l'opzione *Esegui come amministratore*, accedere al percorso dello script scaricato, quindi eseguire il seguente comando:

     .\AssignGlobalAdminRoleToADApplication.ps1 <Application(client) id generated from the Azure portal>

     Ad esempio:

     .\AssignGlobalAdminRoleToADApplication.ps1 60f92079-d1bf-40f7-9ab5-59caab8e7534
- Per assegnare il ruolo manualmente utilizzando i cmdlet PowerShell, procedere come segue:
  1. Per installare il modulo MSOnline, eseguire il seguente comando dalla finestra di PowerShell utilizzando l'opzione Esegui come amministratore:

     Install-Module MSOnline
  2. Per avviare una connessione con Azure Active Directory (AzureAD), eseguire il comando seguente:

     Connect-MSolService
  3. Ottenere l'ID dell'app utilizzando il seguente comando:

     $sp = Get-MsolServicePrincipal -AppPrincipalID <APP ID GUID>

     Nota: la parte APP ID GUID corrisponde all'ID dell'applicazione UDP.
  4. Ottenere il ruolo di amministratore globale/aziendale utilizzando il comando seguente:

     $role = Get-MsolRole -RoleName "Company Administrator"
  5. Per aggiungere il ruolo di amministratore globale/aziendale all'app AzureAD, utilizzare il comando seguente:

     Add-MsolRoleMember -RoleObjectId $role.ObjectId -RoleMemberType ServicePrincipal -RoleMemberObjectId $Sp.ObjectId

Download del certificato da UDP e caricamento in Azure

In questa sezione vengono fornite informazioni su come scaricare il certificato da UDP e caricarlo sul portale Azure.

Nella console UDP, durante la creazione di un piano di Office 365 nuovo o esistente per Exchange Online, SharePoint oppure OneDrive, dopo aver selezionato l'opzione di autenticazione moderna, eseguire una delle operazioni seguenti:

Metodo 1: per generare e scaricare un nuovo certificato autofirmato per l'autenticazione, procedere come segue:

1. Per generare un nuovo certificato autofirmato, selezionare **Genera e scarica nuovo certificato autofirmato**.
2. Immettere ed immettere nuovamente la password del certificato, se necessario.
3. Per scaricare il certificato, fare clic su una delle opzioni seguenti:
   - **Certificato pubblico**: scaricare il certificato per caricarlo sul portale Azure.
   - **Certificato privato**: scaricare il certificato per salvarlo sul computer per un utilizzo futuro.

     Nota: dopo aver scaricato il certificato pubblico, viene attivata l'opzione di download per il certificato privato.
4. Accedere al portale Azure.
5. Cercare Registrazioni app nella barra di ricerca, quindi selezionare **Registrazioni app**.
6. Dall'elenco delle app registrate, fare clic sull'applicazione creata precedentemente nella sezione *Configurazione di un'applicazione nel portale Azure*.
7. Accedere a Certificati e segreti, fare clic su **Carica certificato**, ricercare il certificato esistente [file .cer], quindi fare clic su **Aggiungi**.
8. Nel riquadro sinistro, selezionare le autorizzazioni API, quindi fare clic su **Concedi il consenso dell'amministratore per <nome tenant>**.

   Verrà visualizzato un messaggio di conferma.
9. Fare clic su **Sì**.
10. Nella console UDP, fare clic su **Avanti** per procedere con la registrazione del nodo.

Metodo 2: Per eseguire l'autenticazione utilizzando un certificato esistente, procedere come segue:

Note:

- Quando è selezionata l'opzione *Usa certificato esistente*, l'utente deve disporre dei file del certificato (file .cer) e del certificato con chiave privata (file .PFX con password). Tali certificati possono essere autofirmati o firmati da un'autorità di certificazione (CA).
- Se lo stesso certificato viene utilizzato per la creazione di più piani, è sufficiente caricarlo una sola volta nel portale Azure.
- Se si utilizza Internet Explorer (IE 11), la procedura viene bloccata quando si seleziona l'opzione *Utilizza certificato esistente*. Per risolvere il problema, consultare la sezione Configurazione delle impostazioni di protezione di Internet Explorer (IE 11).

1. Accedere al portale Azure.
2. Cercare Registrazioni app nella barra di ricerca, quindi selezionare **Registrazioni app**.
3. Dall'elenco delle app registrate, fare clic sull'applicazione creata precedentemente nella sezione *Configurazione di un'applicazione nel portale Azure*.
4. Accedere a Certificati e segreti, fare clic su **Carica certificato**, ricercare il certificato esistente [file .cer], quindi fare clic su **Aggiungi**.
5. Nel riquadro sinistro, selezionare le autorizzazioni API, quindi fare clic su **Concedi il consenso dell'amministratore per <nome tenant>**.

   Verrà visualizzato un messaggio di conferma.
6. Fare clic su **Sì**.
7. Seguire questi passaggi dalla console UDP:
   a. Cercare il certificato con chiave privata [file .PFX] e immettere la password.
   b. Fare clic su **Avanti** per procedere con la registrazione del nodo.

Assegnazione del ruolo di rappresentazione dell'applicazione all'account utente specificato per il backup

In questa sezione vengono fornite informazioni su come aggiungere l'account di backup al gruppo di ruoli Discovery Management e assegnare l'autorizzazione di rappresentazione dell'applicazione.

Per aggiungere il ruolo e il gruppo richiesti, eseguire una delle seguenti operazioni:

Metodo 1: utilizzo del portale Office 365

Effettuare le operazioni seguenti:

1. Accedere al Portale di Office 365 con i privilegi di amministratore o con un account in possesso delle autorizzazioni di amministrazione globale.

   Viene visualizzata la pagina dell'interfaccia di amministrazione di Exchange.

2. Accedere alle **autorizzazioni** e dall'elenco a discesa **Aggiungi**, fare doppio clic su **Discovery Management**.

   Viene visualizzata la finestra di dialogo Discovery Management.

   Nota: i membri del gruppo del ruolo Discovery Management possono eseguire le ricerche nelle caselle di posta della struttura di Exchange per i dati che soddisfano determinati criteri.

3. In **Ruoli**, fare clic sul segno **+** per aggiungere il ruolo *ApplicationImpersonation*.

   Viene visualizzata la finestra di dialogo Selezionare un ruolo.

4. Dall'elenco a discesa **Nome visualizzato**, selezionare **ApplicationImpersonation**.

   Nota: il ruolo *ApplicationImpersonation* consente alle applicazioni di rappresentare gli utenti in un'organizzazione allo scopo di eseguire le attività per conto dell'utente.

5. Fare clic su **Aggiungi** per aggiungere il ruolo ApplicationImpersonation, quindi fare clic su **OK**.

6. Nella finestra di dialogo Discovery Management, in **Membri**, fare clic sul segno **+** per aggiungere l'account di backup come membro.

   Viene visualizzata la finestra di dialogo Selezionare membri.

7. Dall'elenco a discesa Nome, selezionare l'account di backup, fare clic su **Aggiungi** per aggiungere il membro, quindi fare clic su **OK**.

L'account di backup selezionato viene visualizzato in **Membri** della finestra di dialogo **Discovery Management**.

8. Fare clic su **Salva**.

Metodo 2: utilizzo di PowerShell remoto

Effettuare le operazioni seguenti:

1. Connettersi al tenant di Exchange Online utilizzando PowerShell remoto. Per ulteriori informazioni, consultare la sezione Connessione a Exchange Online PowerShell.
2. Una volta stabilita la connessione, per aggiungere l'account di backup come membro del gruppo di ruoli Discovery Management, utilizzare il seguente comando:

   `"Add-RoleGroupMember" cmdlet`

   Ad esempio: *Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.*
3. Per assegnare il ruolo di rappresentazione dell'applicazione all'account di backup, utilizzare il seguente comando:

   `"New-ManagementRoleAssignment" cmdlet`

   Ad esempio: *New-ManagementRoleAssignment -Name: impersonationAssignmentName -Role:ApplicationImpersonation - User: "username@domain.onmicrosoft.com"*

Il ruolo *ApplicationImpersonation* e il gruppo Membri vengono aggiunti all'account di backup di Exchange Online.

Creazione di un piano di backup di Exchange Online

Exchange Online è un'applicazione di posta elettronica ospitata su cloud di Microsoft. Per proteggere gli elementi di posta di Exchange Online (messaggi di posta elettronica, gli elementi calendario, contatti e così via) dal cloud Microsoft, è necessario creare un piano. Il piano di backup per Exchange Online consiste in un'attività di backup. Questa attività di backup consente di specificare i nodi Exchange Online che si desidera proteggere, la destinazione di backup e la pianificazione dei backup.

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di un piano di backup di Exchange Online
3. (Facoltativo) Esecuzione di un backup manuale
4. Configurazione per l'autenticazione a più fattori

Verifica delle considerazioni e dei prerequisiti

Rivedere i prerequisiti e le considerazioni seguenti prima di creare un piano di backup di Exchange Online.

Creazione di un piano di backup di Exchange Online:

Prerequisiti:

Per l'account di backup:

- Utilizzare un account del servizio di backup con autorizzazioni di amministratore globale.
- Aggiungere le autorizzazioni di rappresentazione per l'utente di backup all'account di backup di Exchange Online per la connessione dell'organizzazione Exchange Online e l'esecuzione del backup e del ripristino.

  Nota: se non si aggiunge l'account di backup al gruppo del ruolo Discovery Management e non vengono assegnate le autorizzazioni di rappresentazione dell'applicazione, il backup non riesce.

- Associare l'account utente di backup con una casella di posta di Exchange Online.

Per il proxy di backup:

- Accedere alla Console.
- Installare l'agente Arcserve UDP sul computer proxy in cui si desidera eseguire il backup o il ripristino.

Considerazioni:

- Durante il backup di un ampio set di utenti, è possibile utilizzare i gruppi di Exchange per migliorare il backup e l'ottimizzazione.
- L'impostazione predefinita per il backup in linea di Exchange utilizza 4 thread di backup (un thread per utente) alla volta. È inoltre possibile modificare i thread nel file di configurazione di *Engine\BIN\Office365\Arcserve.Office365.Exchange.config* nel modo seguente:

  ```
  <!--#region for multi thread--> <!Valore predefinito --MultiThreadEnable: 0. Se attivato, impostare su 1.--> <add key-y="MultiThreadEnable" value ="1"/> <!--impostare quanti thread verranno utilizzati per i backup della casella di posta. default value is 4--> <add key-
  ```

```
="MaxDegreeOfParallelismForMailbox" value="4"/> <!--#endregion-
->
```

Si consiglia di impostare il valore da 1 a 5. Il valore massimo possibile è 10. Tuttavia, si consiglia di non impostare il valore da 6 a 10.

Nota: UDP 8.0 supporta quanto segue:

- Casella di posta dell'utente
- Casella di posta condivisa
- Cartelle pubbliche abilitate per la posta
- Caselle di posta della stanza
- Caselle di posta dell'apparecchiatura
- Caselle di posta di gruppo

Nota: per ulteriori informazioni sulle procedure consigliate per Exchange Online, consultare la sezione Problemi correlati a Exchange Online.

Creazione di un piano di backup di Exchange Online mediante l'autenticazione di base (BA):

Rivedere i seguenti prerequisiti:

- Installare PowerShell versione 5.1 o versioni successive (appartenente a Windows Management Framework (WMF)) sul server proxy (computer a 64 bit).
- Installare i seguenti moduli PowerShell sul server proxy utilizzando la finestra PowerShell:
  - Per installare il modulo Azure , eseguire il comando seguente:

    Install-Module -Name AzureAD -Force
  - Per installare il modulo ExchangeOnlineManagement, eseguire il comando seguente:

    Install-Module -Name ExchangeOnlineManagement -Force

Nota: quando si installano i moduli PowerShell utilizzando i comandi precedenti, è possibile che venga installata una versione più recente dei moduli in base alla versione GA del componente disponibile nel repository Microsoft.

Creazione di un piano di backup di Exchange Online mediante l'autenticazione moderna (MA):

Verificare i prerequisiti prima di creare un piano utilizzando l'autenticazione moderna.

Assegnazione del ruolo di rappresentazione dell'applicazione all'account utente specificato per il backup

In questa sezione vengono fornite informazioni su come aggiungere l'account di backup al gruppo di ruoli Discovery Management e assegnare l'autorizzazione di rappresentazione dell'applicazione.

Per aggiungere il ruolo e il gruppo richiesti, eseguire una delle seguenti operazioni:

Metodo 1: utilizzo del portale Office 365

Effettuare le operazioni seguenti:

1. Accedere al Portale di Office 365 con i privilegi di amministratore o con un account in possesso delle autorizzazioni di amministrazione globale.

   Viene visualizzata la pagina dell'interfaccia di amministrazione di Exchange.

2. Accedere alle **autorizzazioni** e dall'elenco a discesa **Aggiungi**, fare doppio clic su **Discovery Management**.

   Viene visualizzata la finestra di dialogo Discovery Management.

   Nota: i membri del gruppo del ruolo Discovery Management possono eseguire le ricerche nelle caselle di posta della struttura di Exchange per i dati che soddisfano determinati criteri.

3. In **Ruoli**, fare clic sul segno **+** per aggiungere il ruolo *ApplicationImpersonation*.

   Viene visualizzata la finestra di dialogo Selezionare un ruolo.

4. Dall'elenco a discesa **Nome visualizzato**, selezionare **ApplicationImpersonation**.

   Nota: il ruolo *ApplicationImpersonation* consente alle applicazioni di rappresentare gli utenti in un'organizzazione allo scopo di eseguire le attività per conto dell'utente.

5. Fare clic su **Aggiungi** per aggiungere il ruolo ApplicationImpersonation, quindi fare clic su **OK**.

6. Nella finestra di dialogo Discovery Management, in **Membri**, fare clic sul segno **+** per aggiungere l'account di backup come membro.

   Viene visualizzata la finestra di dialogo Selezionare membri.

7. Dall'elenco a discesa Nome, selezionare l'account di backup, fare clic su **Aggiungi** per aggiungere il membro, quindi fare clic su **OK**.

L'account di backup selezionato viene visualizzato in **Membri** della finestra di dialogo **Discovery Management**.

8. Fare clic su **Salva**.

Metodo 2: utilizzo di PowerShell remoto

Effettuare le operazioni seguenti:

1. Connettersi al tenant di Exchange Online utilizzando PowerShell remoto. Per ulteriori informazioni, consultare la sezione Connessione a Exchange Online PowerShell.
2. Una volta stabilita la connessione, per aggiungere l'account di backup come membro del gruppo di ruoli Discovery Management, utilizzare il seguente comando:

   `"Add-RoleGroupMember" cmdlet`

   Ad esempio: *Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.*
3. Per assegnare il ruolo di rappresentazione dell'applicazione all'account di backup, utilizzare il seguente comando:

   `"New-ManagementRoleAssignment" cmdlet`

   Ad esempio: *New-ManagementRoleAssignment -Name: impersonationAssignmentName -Role:ApplicationImpersonation - User: "username@domain.onmicrosoft.com"*

Il ruolo *ApplicationImpersonation* e il gruppo Membri vengono aggiunti all'account di backup di Exchange Online.

Creazione di un piano di backup di Exchange Online

Un piano di backup include un'attività di backup che esegue un backup degli elementi di posta elettronica di Exchange Online (messaggi di posta elettronica, calendari, contatti e così via) e archivia i dati in un archivio dati di deduplicazione o non di deduplicazione. Inoltre, questo piano di backup consente a UDP di rilevare e specificare i gruppi di Exchange Online per i quali viene eseguita un'attività di backup. Ciascuna attività consiste di parametri che definiscono l'origine, la destinazione, la pianificazione, e altri dettagli di backup.

Effettuare le operazioni seguenti:

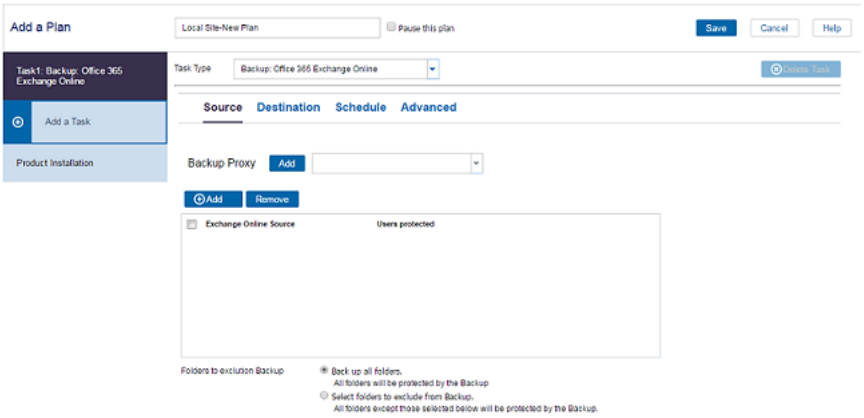
1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa Tipo di attività, selezionare **Backup: Exchange Online Office 365**.



Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

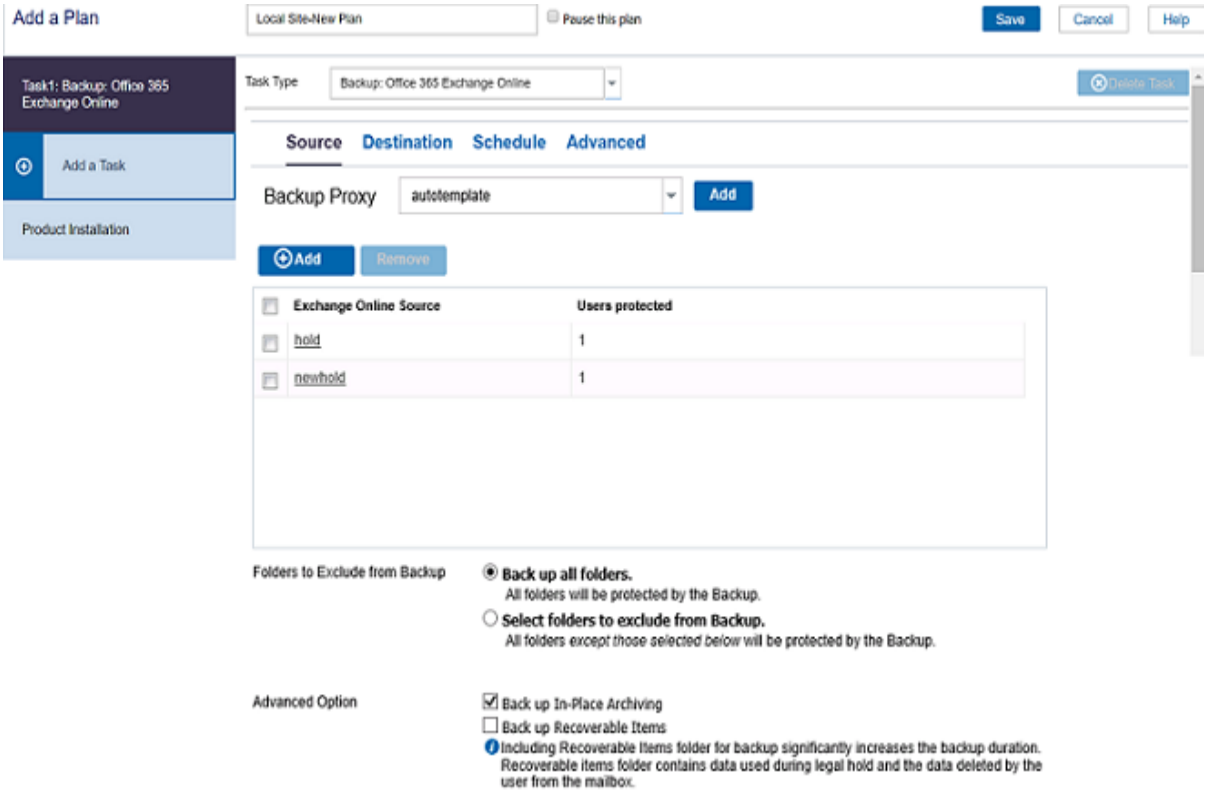
La pagina Origine consente di specificare i nodi di origine di Exchange Online che si desidera proteggere. È possibile selezionare più di un nodo di origine di Exchange Online per un piano. Se non sono stati aggiunti nodi di origine alla Console, è possibile aggiungerli dalla pagina Origine.

Nota: È possibile salvare un piano senza aggiungere nodi di origine. Il piano non verrà comunque distribuito a meno che vengano aggiunti altri nodi.

È inoltre possibile gestire i nodi Exchange Online utilizzando il supporto della casella di posta della cartella pubblica per la protezione Exchange Online.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Origine**.



2. Per il proxy di backup, eseguire una delle seguenti operazioni:
   - Dall'elenco a discesa, selezionare un proxy di backup esistente.
   - Per aggiungere un nuovo proxy di backup, fare clic su **Aggiungi** accanto all'elenco a discesa.
3. Aggiungere il nodo Exchange Online utilizzando una delle seguenti opzioni:

   Metodo 1

a. Fare clic su **Aggiungi**, quindi su **Seleziona origine da proteggere in Arcserve UDP**.

   Viene visualizzata la finestra di dialogo Aggiungi nodi al piano.

b. Selezionare un nodo e fare clic su **Connetti**.

   Nota: È inoltre possibile ricercare i nodi Exchange Online che si desidera proteggere nel campo di **ricerca**.

c. Selezionare la casella di controllo di **protezione completa delle origini di Office 365 Exchange** per proteggere tutti gli account di Exchange Online in tutte le pagine.

   Nota: Per aggiungere tutti gli account di Exchange Online all'elenco protetto, è possibile fare clic sulla freccia verso destra (>).

   Gli account di Exchange Online selezionati vengono aggiunti.

Metodo 2

- Fare clic su **Aggiungi**, quindi selezionare **Aggiungi origine Exchange Online**.

  Viene visualizzata la finestra di dialogo Aggiungi nodi a un piano.

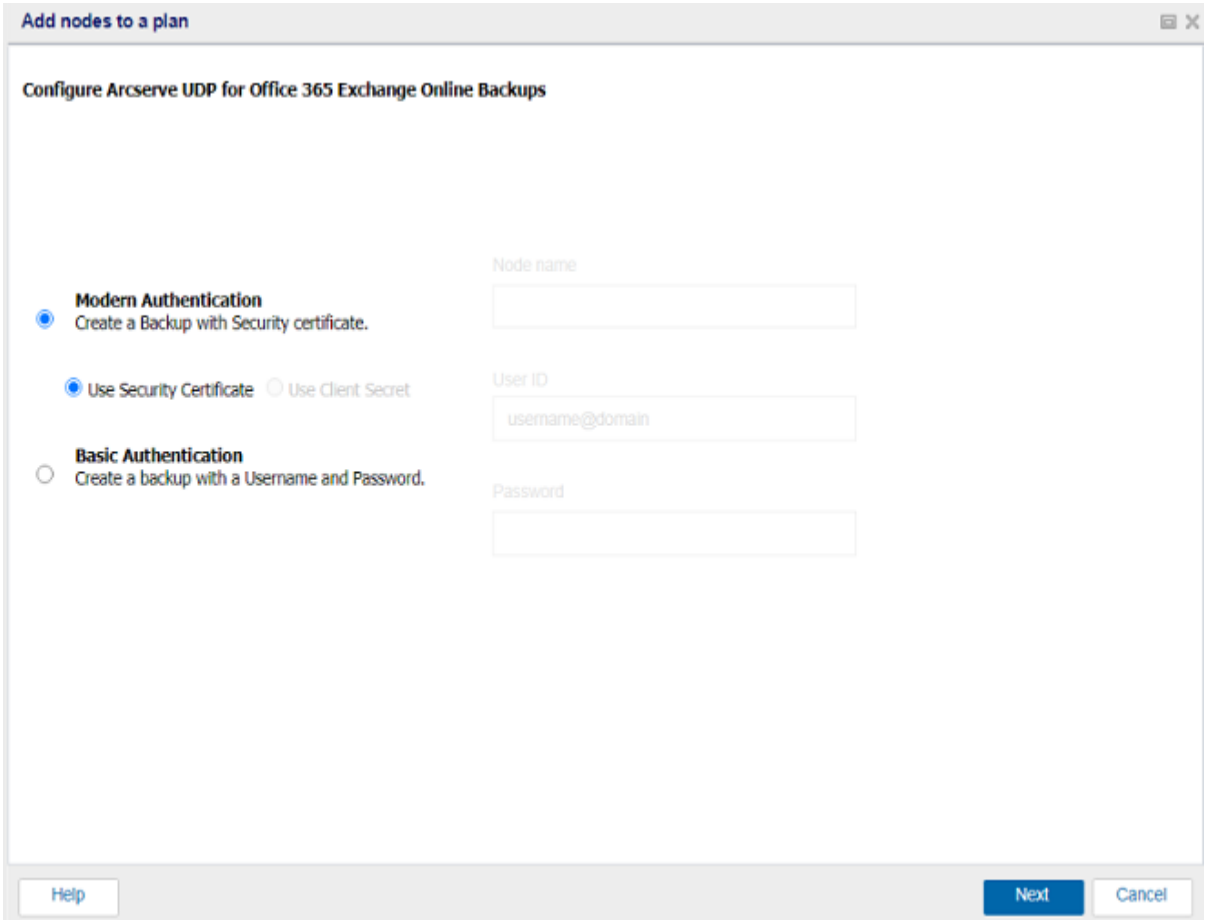
  Nota: A differenza di altri nodi, non è possibile aggiungere il nodo Exchange Online dalla pagina **Tutti i nodi**. È possibile aggiungere un nodo Exchange Online soltanto in un piano o con la modifica di un piano.

  Più nodi Exchange Online possono utilizzare lo stesso account utente (account servizio) di Exchange Online.

4. Per applicare l'autenticazione, eseguire una delle seguenti operazioni:

   Autenticazione moderna

   Per l'autenticazione moderna, è possibile eseguire un backup utilizzando il certificato di sicurezza.



Usa certificato di sicurezza

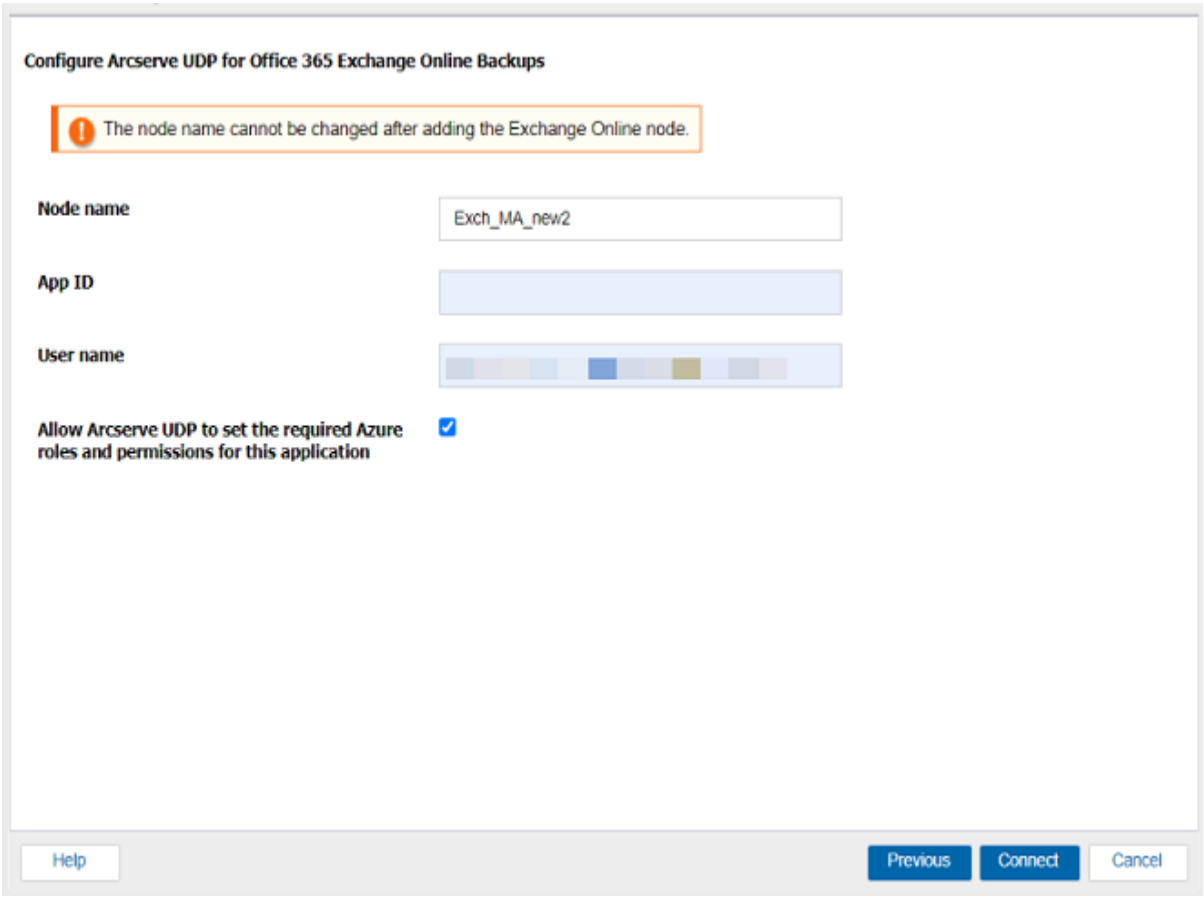
Nota: per impostazione predefinita, il piano di backup seleziona l'opzione **Usa certificato di sicurezza** per l'autenticazione moderna.

Effettuare le operazioni seguenti:

a. Per eseguire l'autenticazione dell'applicazione UDP con i certificati di protezione, consultare la sezione Download del certificato da UDP e caricamento in Azure.

b. Immettere le seguenti informazioni:

- Nome nodo
- ID app
- Nome utente



c. Per applicare automaticamente le autorizzazioni API, selezionare la casella di controllo **Consenti ad Arcserve UDP di impostare le autorizzazioni API richieste per questa applicazione**.

   Nota: per applicare manualmente le autorizzazioni senza utilizzare il ruolo di amministratore globale/aziendale, consultare la sezione Configurazione manuale delle autorizzazioni API senza utilizzare il ruolo di amministratore globale/aziendale.

d. Fare clic su **Connetti**.

Note:

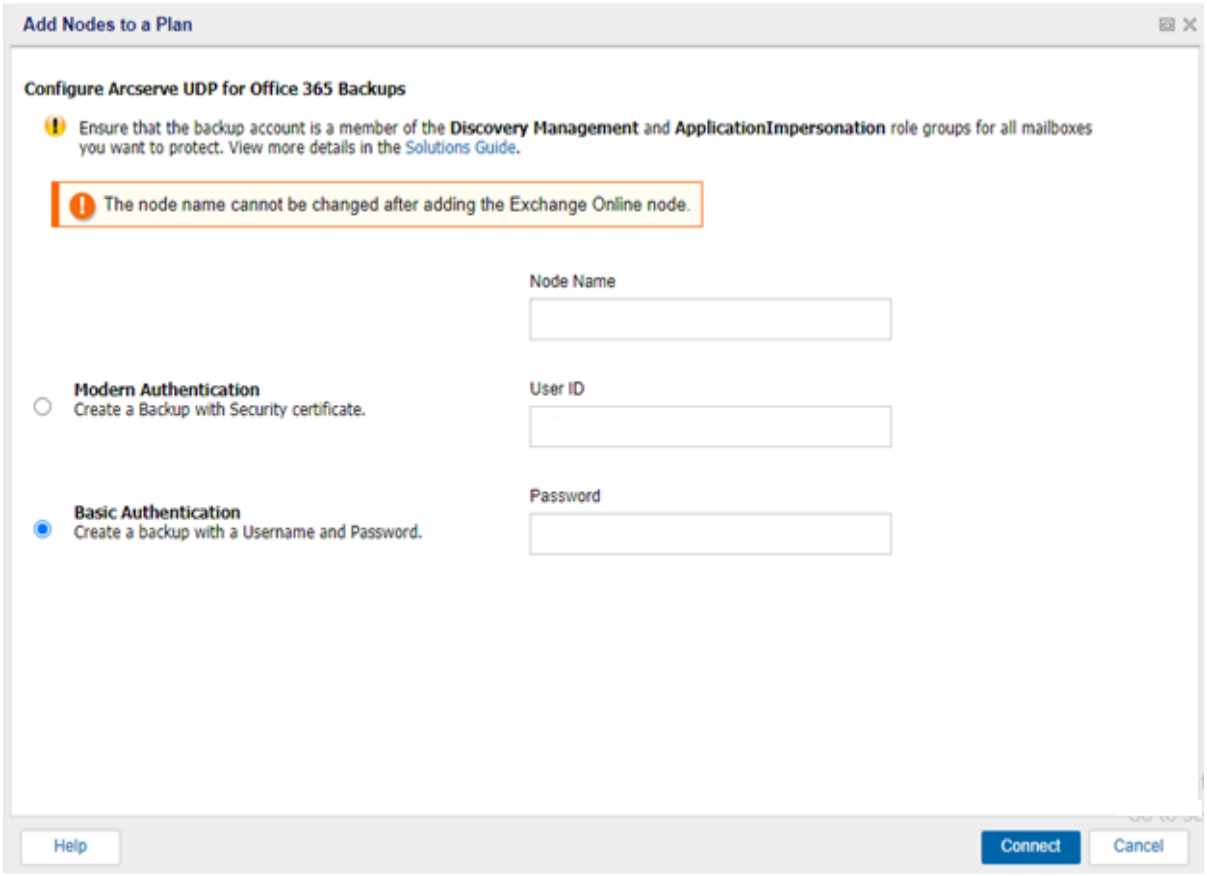
- Il nome del nodo di Exchange Online non può essere modificato dopo aver aggiunto il nodo.
- Immettere il nome utente dell'account di backup di Exchange Online in grado di soddisfare i prerequisiti nel campo **Nome utente amministratore**.
- L'autenticazione moderna non si applica nei seguenti casi:

- I clienti che utilizzano Microsoft 365 (Office 365) per le istanze Arcserve Cloud Hybrid o Arcserve Cloud Backup for Office 365, create prima del 18 ottobre 2020, non consentono l'autenticazione moderna.
- Clienti che continuano a utilizzare l'autenticazione di base

Autenticazione di base

Per l'autenticazione di base, fornire le seguenti informazioni per procedere con il backup, quindi fare clic su **Connetti**:

- Nome nodo
- ID utente
- Password



Nota: aggiornando o modificando l'account utente, il numero di caselle di posta protette potrebbe risultare modificato. Verificare che l'account del servizio nuovo/aggiornato disponga dei diritti di impersonificazione per la protezione delle caselle di posta elettronica.

5. Per proteggere le caselle di posta di Exchange Online, eseguire una delle operazioni seguenti:

   - Per proteggere tutte le caselle di posta e i gruppi di Exchange Online, selezionare la casella di controllo **Proteggere tutte le origini di Office 365 Exchange**.

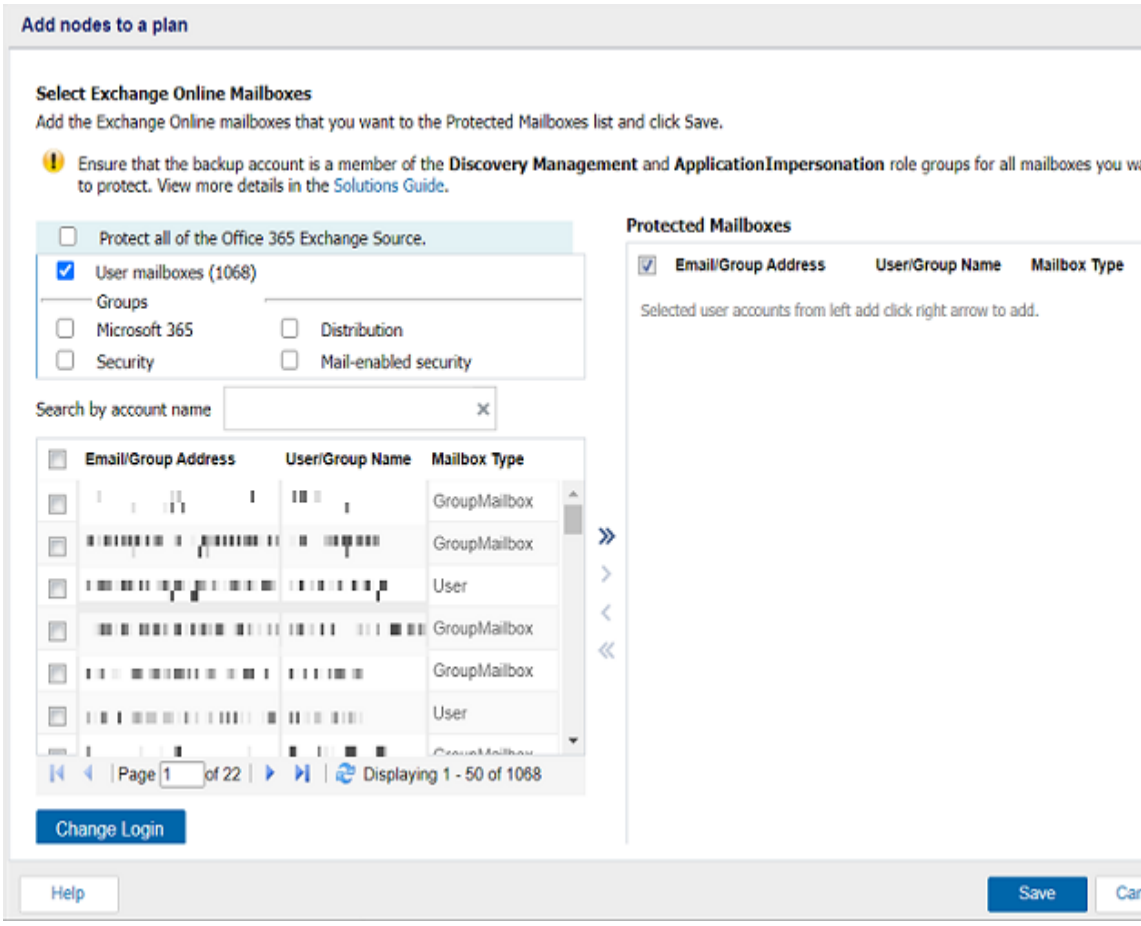
     Nota: questa opzione è selezionata automaticamente per impostazione predefinita quando viene visualizzata la schermata Seleziona caselle di posta Exchange Online.

   - Per le caselle di posta degli utenti, procedere come segue:

     a. Selezionare la casella di controllo **Caselle di posta dell'utente**.

        Viene visualizzato l'elenco delle caselle di posta dell'utente.

     b. (Facoltativo) Per cercare un account dall'elenco, nel campo Cerca per nome account, immettere il nome dell'account.



     c. Dall'elenco delle caselle di posta dell'utente, selezionare le caselle di posta che si desidera proteggere.

d. Fare clic sulla freccia destra (>) per spostare le caselle di posta selezionate nell'elenco Caselle di posta protette.

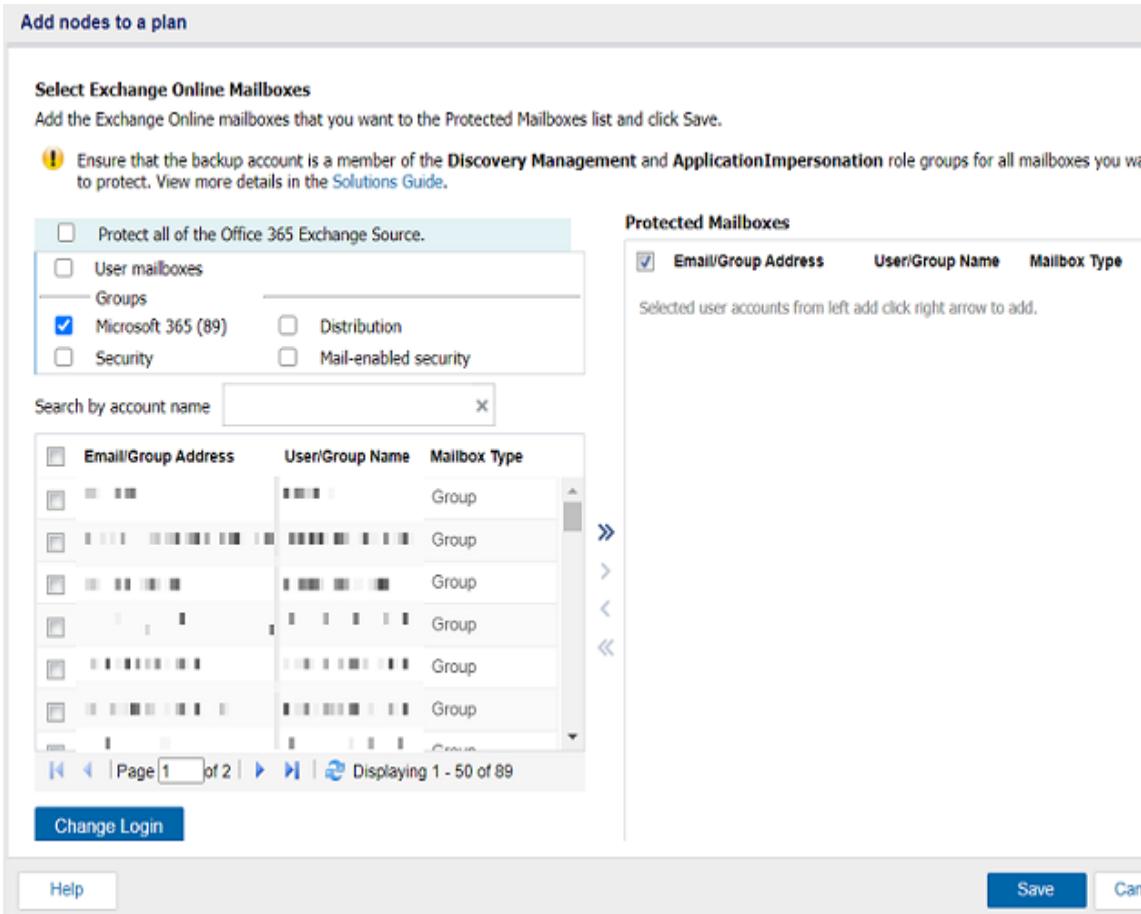
- Per i gruppi, procedere come segue:

a. Selezionare la casella di controllo **Microsoft 365**.

Viene visualizzato l'elenco dei gruppi.

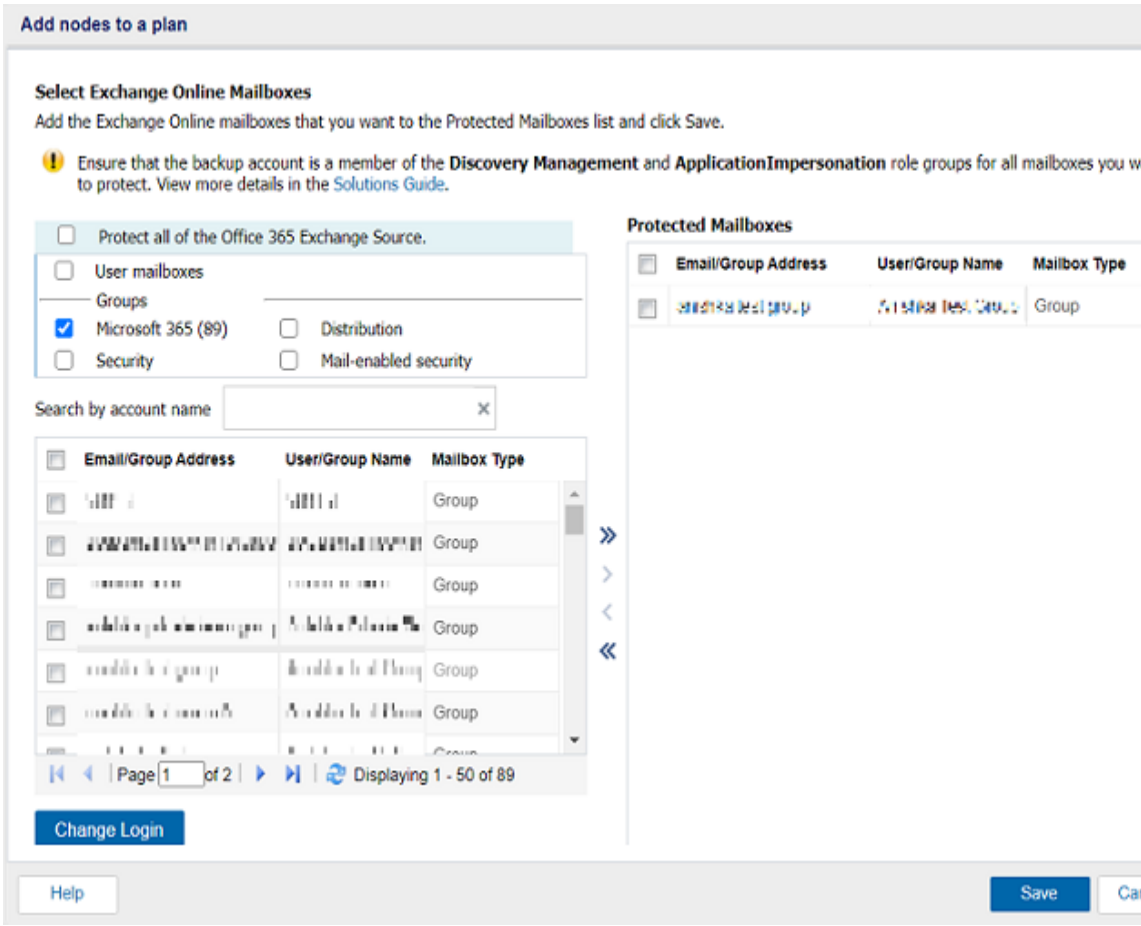
Nota: se si desidera selezionare i gruppi insieme ai gruppi secondari quali **Distribuzione**, **Protezione** o **Protezione abilitata per la posta elettronica**, selezionare la casella di controllo **Microsoft 365**, quindi la casella di controllo corrispondente al gruppo secondario.

b. (Facoltativo) Per cercare un account dall'elenco, nel campo Cerca per nome account, immettere il nome dell'account.



c. Dall'elenco dei gruppi, selezionare i gruppi che si desidera proteggere.

d. Fare clic sulla freccia destra (>) per spostare i gruppi selezionati nell'elenco Caselle di posta protette.



6. Fare clic su **Salva**.
7. Nella scheda Origini, accedere a **Cartelle da escludere dal backup**, quindi selezionare la casella di controllo desiderata.
8. Da Opzione avanzata, selezionare la casella di controllo desiderata.
   - Per consentire alla protezione di Exchange Online di supportare la casella di posta di archiviazione, selezionare la casella di controllo **Archiviazione sul posto di backup**.

     Nota: Per ulteriori informazioni sulla casella di posta di archiviazione, consultare il seguente collegamento.
   - Selezionare la casella di controllo **Backup degli elementi recuperabili** per consentire la protezione della casella di posta che attiva la funzionalità Blocco sul posto o Blocco per controversia legale.

Nota: Per l'archiviazione Blocco sul posto e Blocco per controversia legale per Exchange Online, consultare il seguente collegamento.

Nota: Per attivare entrambe le funzionalità contemporaneamente nella casella di posta per eseguire il backup degli elementi recuperabili nella casella di posta di archiviazione, selezionare entrambe le opzioni **Archiviazione sul posto di backup** e **Backup degli elementi recuperabili**.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Destinazione**.
2. Selezionare l'opzione **Arcserve UDP Recovery Point Server. Arcserve UDP Recovery Point Server** specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono archiviati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.
3. Fornire i dettagli seguenti:
    a. Selezionare un Recovery Point Server.
    b. Selezionare un archivio dati di deduplicazione o di non deduplicazione. L'elenco mostra tutti gli archivi dati creati per il Recovery Point Server specificato.
    c. Fornire una password di sessione. Quando la destinazione del backup è un archivio dati RPS non crittografato, la password di sessione è facoltativa.
    d. Confermare la password di sessione.

La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

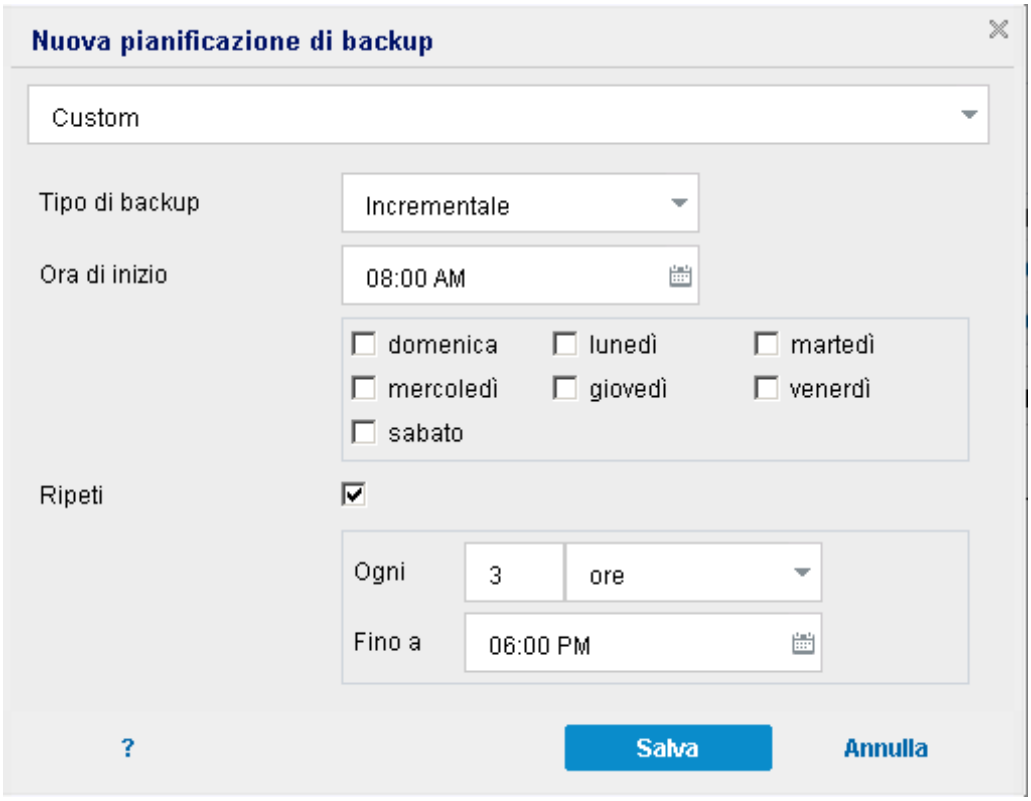
Effettuare le operazioni seguenti:

1. Aggiungere le pianificazioni di backup, di unione e di definizione del limite di velocità

   Aggiunta di una pianificazione di backup

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni di backup.

Incrementale

Specifica la pianificazione dei backup incrementali.

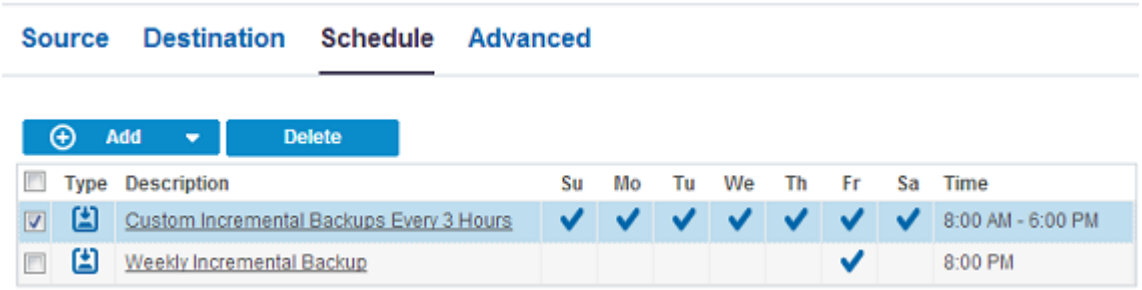
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di unione**.

La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

b. Specificare l'ora di inizio per l'avvio del processo di unione.

c. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

d. Fare clic su **Salva**.

La pianificazione di unione specificata viene visualizzata nella pagina **Pianificazione**.

Aggiungi pianificazione del limite delle risorse

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

Viene visualizzata la finestra di dialogo **Aggiungi nuova pianificazione del limite delle risorse**.

b. Specificare il limite di velocità effettiva in MB per unità di minuti.

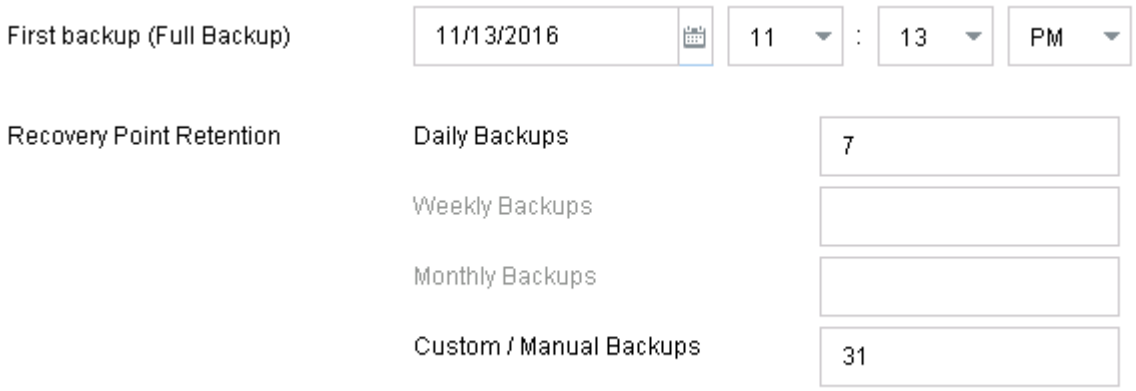
c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

La pianificazione del limite delle risorse specificata viene visualizzata nella pagina **Pianificazione**.

2. Specificare l'ora di inizio per il backup pianificato.



3. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo **Pianificazione di backup**.

   Viene specificata la pianificazione.

Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione

L'opzione di pianificazione consente di specificare una pianificazione personalizzata o una pianificazione giornaliera/settimanale/mensile o entrambe. Nella pianificazione personalizzata è possibile configurare la pianificazione del backup per ciascun giorno della settimana e aggiungere fino a quattro pianificazioni di backup ogni giorno. È possibile selezionare un giorno specifico di una settimana e creare un intervallo di tempo per definire quando eseguire il backup e la frequenza.

Pianificazione	Processo supportato	Commenti
Backup	Processo di backup	Definire gli intervalli di tempo per eseguire i processi di backup.
Limitazione della velocità di backup	Processo di backup	Definire gli intervalli di tempo per controllare la velocità di backup.
Unione	Processo di unione	Definire quando unire i processi.
Pianificazione quotidiana	Processo di backup	Definire quando eseguire processi di backup quotidiani.
Pianificazione settimanale	Processo di backup	Definire quando eseguire processi di backup settimanali.
Pianificazione mensile	Processo di backup	Definire quando eseguire processi di backup mensili.

È inoltre possibile specificare le impostazioni di memorizzazione per i punti di ripristino.

Nota: All'interno di ogni piano è necessario configurare le impostazioni di conservazione per controllare il modo in cui i nodi assegnati a tale piano vengono memorizzati nell'archivio dati di destinazione.

Le pianificazioni per i backup giornalieri/settimanali/mensili sono indipendenti dalla pianificazione personalizzata e gli uni dagli altri. È possibile configurare di eseguire solo il backup giornaliero, il backup settimanale o il backup mensile senza configurare la pianificazione personalizzata.

Pianificazione del processo di backup

È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del backup. Un intervallo di tempo valido è dalle 00:00 alle 23:59. Non è possibile specificare un intervallo di tempo come ad esempio dalle 18:00 alle 06:00. In tali casi, si devono specificare manualmente due intervalli di tempo diversi.

Per ogni intervallo di tempo l'ora di inizio è inclusa e l'ora di fine è esclusa. Ad esempio, si è configurato il backup incrementale da eseguire ogni ora tra le 06:00 e le 09:00 e il backup inizierà alle 06:00. Ciò significa che il backup verrà eseguito alle 06:00, alle 07:00 e 08:00, ma NON alle 09:00.

Nota: Se si desidera eseguire il processo di backup ripetutamente fino al termine della giornata, impostare la pianificazione fino alle 00:00. Ad esempio, per eseguire un processo di backup ogni 15 minuti per l'intera giornata, impostare la pianificazione dalle 00:00 alle 00:00 ogni 15 minuti.

Pianificazione del limite delle risorse di backup

La pianificazione del limite delle risorse di backup consente di controllare la velocità effettiva di backup, che a sua volta controlla l'utilizzo delle risorse (I/O del disco, CPU, larghezza di banda della rete) del server di cui si esegue il backup. Questo è utile se non si desidera influire sulle prestazioni del server durante i normali orari di ufficio. È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del limite delle risorse di backup. Per ogni intervallo di tempo è possibile specificare un valore, in MB per minuto. Questo valore viene utilizzato per controllare la velocità effettiva di backup. I valori validi sono compresi tra 1 MB/minuto a 99999 MB/minuto.

Se un processo di backup si estende oltre il tempo specificato, il limite della velocità cambia in conformità all'intervallo di tempo specificato. Ad esempio, il limite delle risorse di backup definito è 500 MB/minuto dalle 08:00 alle 20:00 e 2500 MB/minuto dalle 20:00 alle 22:00. Se un processo di backup inizia alle 19:00 e viene eseguito per tre ore, dalle 19:00 alle 20:00 il limite della velocità è pari a 500 MB/minuto e dalle 20:00 alle 22:00 a 2500 MB/minuto.

Se non si definisce alcuna pianificazione del backup e della sua velocità effettiva, il backup viene eseguito il più rapidamente possibile.

Pianificazione di unione

Consente di unire i punti di ripristino in base alla pianificazione fornita.

Considerare i punti seguenti per il processo di unione:

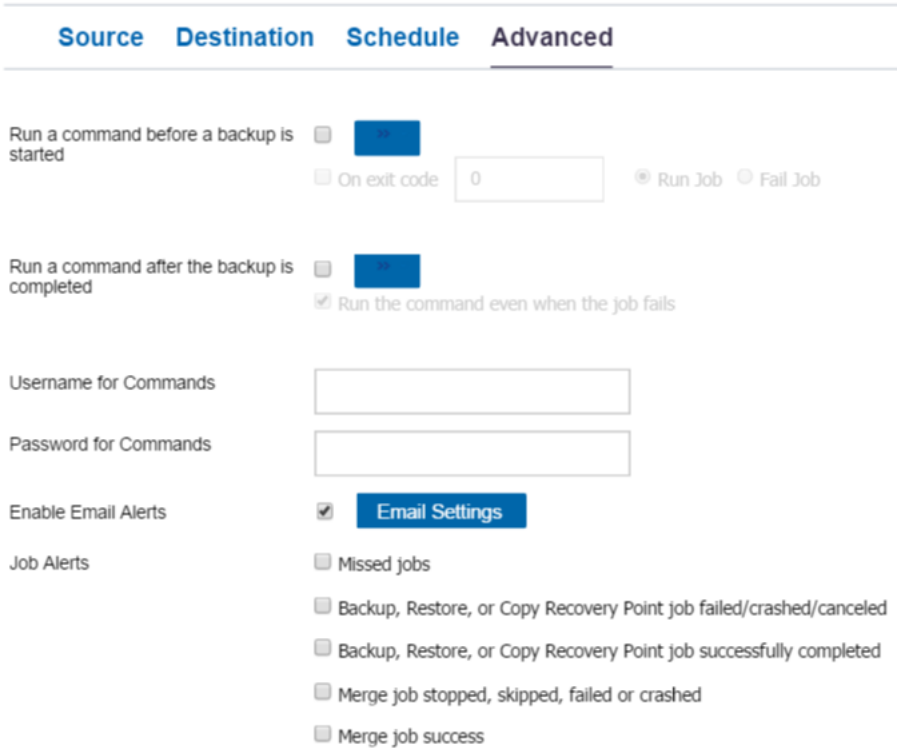
- In qualsiasi momento è possibile eseguire solo un processo di unione per un nodo.
- Se un processo di unione inizia, esso deve essere completato prima di poter avviare il processo di unione successivo. Ciò significa che se uno o più set di punti di ripristino vengono uniti, non è possibile aggiungere nuovi punti di ripristino a questo processo di unione finché il processo di unione dell'insieme corrente dei punti di ripristino non viene completato.

- Se un processo di unione sta elaborando più di un set di punti di ripristino (ad esempio set [1~4], set [5~11] e set [12~14] sono tre set distinti), il Recovery Point Server elabora tali set uno alla volta.
- Se un processo di unione viene ripreso dopo una pausa, il processo individua in quale punto era stato interrotto e riprende l'unione da tale punto.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda **Avanzate:**



Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

   Esegui un comando prima dell'avvio di un backup

   Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script all'interno del nodo proxy. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Processo con errore** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

   Esegui un comando al completamento di un backup

   Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso completo di archiviazione dello script.

   Esegui un comando anche quando il processo non riesce

Se questa casella di controllo è selezionata, lo script specificato in **Esegui comando al completamento del backup** viene eseguito anche quando il processo di backup produce un errore. In caso contrario, lo script viene eseguito solo quando il processo di backup viene completato correttamente.

Nome utente comandi

Consente di specificare il nome utente per eseguire i comandi.

Password comandi

Consente di specificare la password per eseguire i comandi.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere in un messaggio di posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy. Per ulteriori informazioni sulla configurazione delle impostazioni di posta elettronica, consultare la sezione Configurazione di posta elettronica e avvisi.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su **Salva.**

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: Se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo. È possibile aggiungere le attività **Copia punto di ripristino**, **Copia su nastro**, **Replica**, e **Replica da RPS remoto** come attività di completamento.

Il piano viene distribuito automaticamente sul nodo del server proxy.

Viene creato il piano di backup in linea di Exchange per il server proxy. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

(Facoltativo) Esecuzione di un backup manuale

In genere, in base alle impostazioni di pianificazione applicate, i backup vengono eseguiti automaticamente. In aggiunta al backup pianificato, un backup manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze. Se ad esempio si dispone di una pianificazione di ripetizione per backup completi e incrementali e si desidera apportare modifiche sostanziali al computer, è possibile eseguire un backup manuale immediato senza attendere l'esecuzione del backup pianificato successivo.

Per eseguire un backup manuale dei nodi di Exchange Online, procedere come segue:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   I nodi Exchange Online vengono mostrati nel riquadro centrale.
3. Selezionare i nodi Exchange Online (ad esempio, Mailbox@<organizationname.com>) di cui si desidera eseguire il backup e accertarsi che sia stato assegnato un piano. Il nome del nodo corrisponde all'account utilizzato durante l'aggiunta del nodo Exchange Online e alla sua connessione.
4. Fare clic con il pulsante destro del mouse sul nodo, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
5. Selezionare il tipo di backup che si desidera eseguire, quindi fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.
6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.
7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Il backup manuale è stato eseguito correttamente.

Per eseguire un backup manuale di un piano Exchange Online, procedere come segue:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Piani**, quindi fare clic su **Tutti i piani**.

   I piani di backup di Exchange Online vengono visualizzati nel riquadro centrale.
3. Selezionare il piano di cui si desidera eseguire il backup e ai quali è stato assegnato un piano.

4. Fare clic con il pulsante destro del mouse sul piano, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.

5. Selezionare il tipo di backup che si desidera eseguire, quindi fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.

6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.

7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Il backup manuale è stato eseguito correttamente.

Verifica del backup

Per verificare il processo di backup, confermare di avere creato correttamente il piano di backup. Dopo avere verificato che il piano è stato creato correttamente, confermare se il processo di backup è in esecuzione secondo quanto pianificato. È possibile verificare lo stato dei processi di backup dalla scheda **Processi**.

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Attenersi a uno dei seguenti metodi per verificare i processi di backup:

Metodo 1

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Tutti i processi completati**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Metodo 2

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Processi completati correttamente**.

   L'elenco dei processi di backup completati viene visualizzato nel riquadro centrale.
3. Fare clic sul processo che si desidera verificare.

   Il riquadro destro viene aggiornato.
4. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
5. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Configurazione per l'autenticazione a più fattori

Quando un'organizzazione dispone dell'autenticazione a più fattori (MFA) abilitata per gli utenti, utilizzare l'autenticazione moderna per aggiungere i nodi.

Nota: anche se l'autenticazione di base è abilitata sul tenant, è possibile utilizzare l'autenticazione moderna per aggiungere nodi. Per ulteriori informazioni sull'aggiunta di nodi a un piano mediante l'autenticazione moderna, consultare la sezione Autenticazione moderna.

Creazione di un piano di backup di SharePoint Online

La protezione di SharePoint viene utilizzata per eseguire il backup e ripristinare il sito di Microsoft SharePoint Online e l'elemento nell'elenco. SharePoint Online è uno dei prodotti principali di Microsoft Office 365. Per proteggere il contenuto di SharePoint, è necessario creare un piano.

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di un piano di backup di SharePoint Online
3. Verifica del piano di backup
4. Configurazione per l'autenticazione a più fattori

Verifica dei prerequisiti

Rivedere i prerequisiti seguenti prima di creare un piano di backup di SharePoint Online.

Creazione di un piano di backup di SharePoint Online:

Prerequisiti:

L'account di backup appartiene al gruppo Amministratori raccolta siti o è assegnato al ruolo di *amministratore di SharePoint*.

Per aggiungere un account al gruppo Amministratori raccolta siti, fare riferimento al seguente collegamento.

Creazione di un piano di backup di SharePoint Online mediante l'autenticazione di base (BA):

Rivedere i seguenti prerequisiti:

- Installare PowerShell versione 5.1 o versioni successive (appartenente a Windows Management Framework (WMF)) sul server proxy (computer a 64 bit).
- Installare i seguenti moduli PowerShell sul server proxy utilizzando la finestra PowerShell:
  - Per installare il modulo Azure , eseguire il comando seguente:

    Install-Module -Name AzureAD -Force
  - Per installare il modulo ExchangeOnlineManagement, eseguire il comando seguente:

    Install-Module -Name ExchangeOnlineManagement -Force

  Nota: quando si installano i moduli PowerShell utilizzando i comandi precedenti, è possibile che venga installata una versione più recente dei moduli in base alla versione GA del componente disponibile nel repository Microsoft.

Creazione di un piano di backup di SharePoint Online mediante l'autenticazione moderna (MA):

Verificare i prerequisiti prima di creare un piano utilizzando l'autenticazione moderna.

Creazione di un sito personale in SharePoint

In questa sezione vengono fornite informazioni su come creare un sito personale in SharePoint.

Effettuare le operazioni seguenti:

1. Accedere alla pagina di accesso di Microsoft, quindi accedere all'account di amministrazione di Microsoft Office 365.
2. Accedere alla pagina dell'**interfaccia di amministrazione di SharePoint**, quindi fare clic su **Altre funzionalità** nel riquadro sinistro.
3. In Pagina delle raccolte siti classiche, fare clic su **Apri**.

   Viene visualizzata la pagina Raccolte siti.
4. In Pagina delle raccolte siti classiche, fare clic su **Nuovo** > **Raccolta siti privata**.

   Viene visualizzata la finestra di dialogo Nuova raccolta siti.
5. Nella finestra di dialogo della nuova raccolta siti, fornire i dettagli seguenti, quindi fare clic su **OK**.
   - **Titolo**: digitare un nome per il sito.
   - **Indirizzo sito Web**: selezionare un nome di dominio e un percorso URL dagli elenchi a discesa, quindi immettere un nome URL per il sito.
   - **Selezione modello**: nella sezione Selezione modello, procedere come segue:
     - Dall'elenco a discesa **Selezionare una lingua**, selezionare una lingua per il sito.
     - In **Selezionare un modello**, selezionare il modello per il sito.
   - **Fuso orario**: selezionare il fuso orario in base alla posizione del sito.
   - **Amministratore**: digitare il nome della persona desiderata come amministratore del sito. È inoltre possibile utilizzare il pulsante Controlla nomi o Sfoglia per cercare gli utenti e impostarli come amministratori del sito.
   - **Quota di archiviazione**: immettere la dimensione (MB) del sito da allocare.
   - **Quota di risorse del server**: accettare la quota di risorse predefinita.

   Il sito personale viene creato in SharePoint.

Creazione di un piano di backup di SharePoint Online

Un piano di backup include un'attività **Backup: Office 365 SharePoint Online** che esegue un backup degli elementi di SharePoint Online (elenchi, librerie, documenti e così via) e archivia i dati in un archivio dati di deduplicazione o di non deduplicazione. Inoltre, questo piano di backup consente a UDP di rilevare e specificare gli elementi di SharePoint Online per i quali viene eseguita un'attività di backup. Ciascuna attività consiste di parametri che definiscono l'origine, la destinazione, la pianificazione, e altri dettagli di backup.

Effettuare le operazioni seguenti:

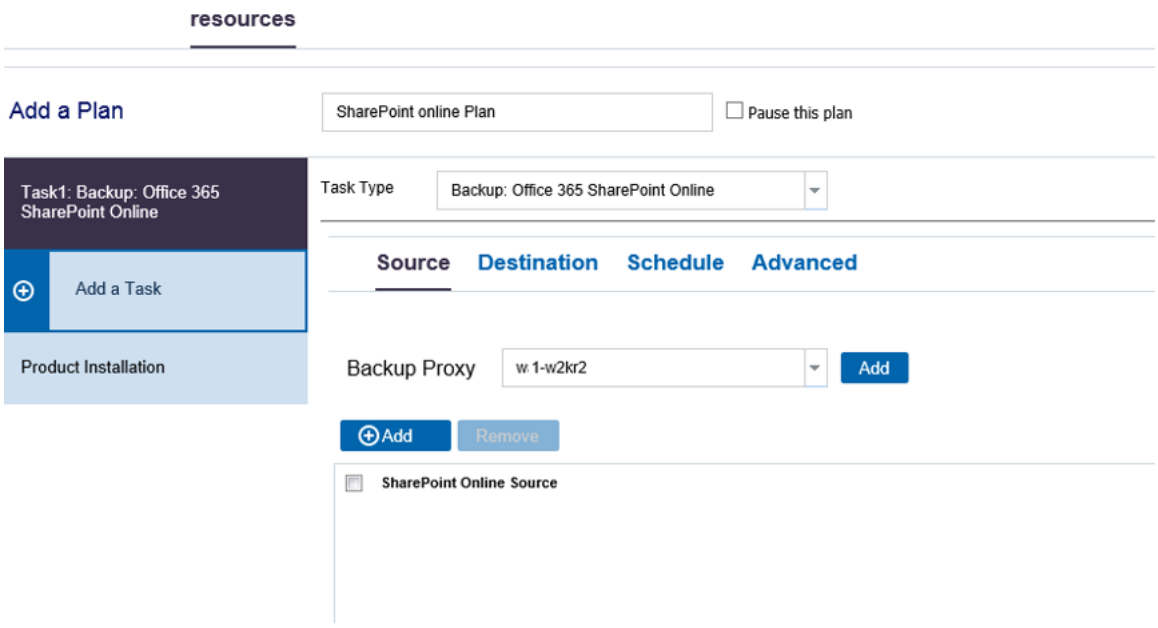
1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa Tipo di attività, selezionare **Backup: SharePoint Online Office 365**.



Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine di SharePoint Online che si desidera proteggere. È possibile selezionare più di un nodo di origine di SharePoint Online per un piano.

Nota: è possibile salvare un piano senza aggiungere nodi di origine. Il piano non verrà comunque distribuito a meno che vengano aggiunti altri nodi.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Origine**.
2. Selezionare **Proxy di backup** dall'elenco a discesa.
3. Aggiungere il nodo SharePoint Online utilizzando uno dei seguenti metodi:

   Metodo 1:

   a. Fare clic su **Aggiungi**, quindi su **Seleziona origine da proteggere in Arcserve UDP**.

      Viene visualizzata la finestra di dialogo Aggiungi nodi al piano.

      Nota: selezionare questa opzione solo se è già stato aggiunto il nodo SharePoint.

   b. Selezionare un nodo e fare clic su **Connetti**.

      Nota: Per individuare i nodi SharePoint Online che si desidera proteggere, utilizzare **Cerca**.

   Metodo 2:

   - Fare clic su **Aggiungi**, quindi selezionare **Aggiungi origine SharePoint Online**.

     Viene visualizzata la finestra di dialogo Aggiungi nodi a un piano.

     Nota:

     - Utilizzare questa opzione per rilevare e specificare gli elementi in linea per l'origine SharePoint Online.
     - A differenza di altri nodi, non è possibile aggiungere il nodo SharePoint Online dalla pagina Tutti i nodi. Durante la creazione o modifica di un piano, è possibile aggiungere un nodo SharePoint Online soltanto in un piano.

4. Per applicare l'autenticazione, eseguire una delle seguenti operazioni:

Autenticazione moderna

Per l'autenticazione moderna, è possibile eseguire un backup utilizzando il certificato di sicurezza.

Usa certificato di sicurezza

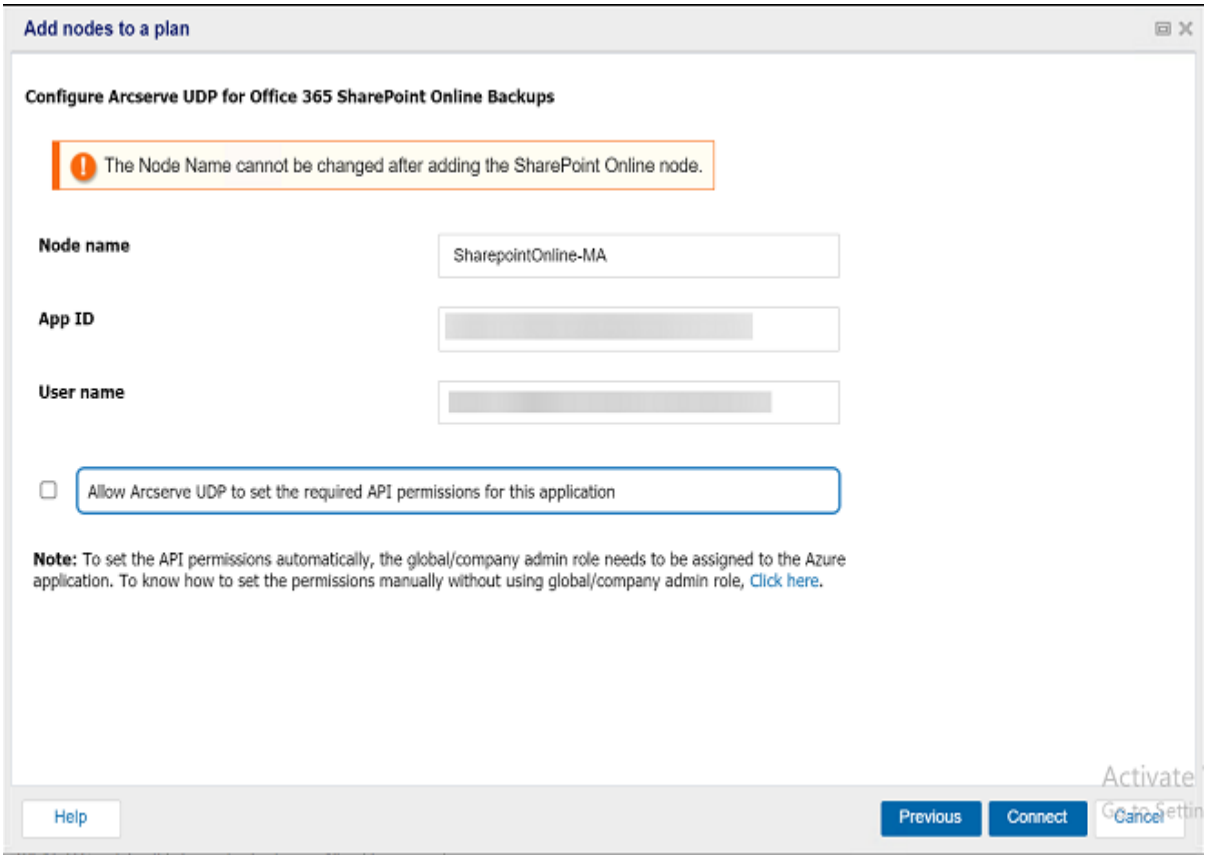
Nota: per impostazione predefinita, il piano di backup seleziona l'opzione **Usa certificato di sicurezza** per l'autenticazione moderna.

Effettuare le operazioni seguenti:

a. Per eseguire l'autenticazione dell'applicazione UDP con i certificati di protezione, consultare la sezione Download del certificato da UDP e caricamento in Azure.

b. Immettere le seguenti informazioni:

- Nome nodo
- ID app
- Nome utente



c. Per applicare automaticamente le autorizzazioni API, selezionare la casella di controllo **Consenti ad Arcserve UDP di impostare le autorizzazioni API richieste per questa applicazione**.

Nota: per applicare manualmente le autorizzazioni senza utilizzare il ruolo di amministratore globale/aziendale, consultare la sezione Configurazione manuale delle autorizzazioni API senza utilizzare il ruolo di amministratore globale/aziendale.

d. Fare clic su **Connetti**.

Note:

- Il nome del nodo di origine di SharePoint Online non può essere modificato dopo la creazione del nodo.
- È possibile utilizzare un singolo account per proteggere più nodi SharePoint Online.

Autenticazione di base

Per l'autenticazione di base, fornire le seguenti informazioni per procedere con il backup, quindi fare clic su **Connetti**:

- Nome nodo
- ID utente
- Password

5. Per proteggere gli elementi di SharePoint Online, procedere come segue, quindi fare clic su **Salva**.
   - Dall'elenco a discesa Tipo di sito, selezionare il tipo di sito che si desidera proteggere, ad esempio i siti SharePoint o i siti personali.
   - Per proteggere tutti i siti/siti secondari, procedere come segue:

     Note:

     - questa opzione è selezionata automaticamente per impostazione predefinita quando viene visualizzata la schermata Seleziona contenuto SharePoint Online.
       - Per proteggere tutti gli elementi nel tipo di sito selezionato, selezionare la casella di controllo **Proteggi tutti i siti/siti secondari**.
       - Per proteggere elementi specifici nel tipo di sito selezionato, deselezionare la casella di controllo **Proteggi tutti**

i siti/siti secondari, quindi selezionare gli elementi specifici che si desidera proteggere.

- Durante la configurazione del piano SharePoint Online esistente, se sono stati selezionati manualmente i siti per la protezione e si desidera selezionare la casella di controllo **Proteggi tutti i siti/siti secondari**, procedere come segue:
  a. Modificare il piano SharePoint Online esistente.
  b. Deselezionare i siti SharePoint selezionati manualmente per la protezione.
  c. Selezionare la casella di controllo **Proteggi tutti i siti/siti secondari**, quindi salvare il piano.

- Per escludere elementi specifici dalla protezione, selezionare la casella di controllo **Escludi siti selezionati**, quindi selezionare gli elementi specifici nel tipo di sito selezionato.

Le origini di SharePoint Online che si desidera proteggere vengono aggiunte al piano.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Destinazione**.

   Selezionare l'opzione **Arcserve UDP Recovery Point Server. Arcserve UDP Recovery Point Server** specifica che la destinazione di backup è un Recovery Point Server.

   Non è possibile archiviare i dati come set di ripristino.

2. Procedere come segue:

   a. Selezionare un Recovery Point Server.

   b. Selezionare un archivio dati di deduplicazione o di non deduplicazione.

      L'elenco mostra tutti gli archivi dati creati per il Recovery Point Server specificato.

   c. Fornire una password di sessione.

      Quando la destinazione del backup è un archivio dati RPS non crittografato, la password di sessione è facoltativa.

   d. Confermare la password di sessione.

   La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

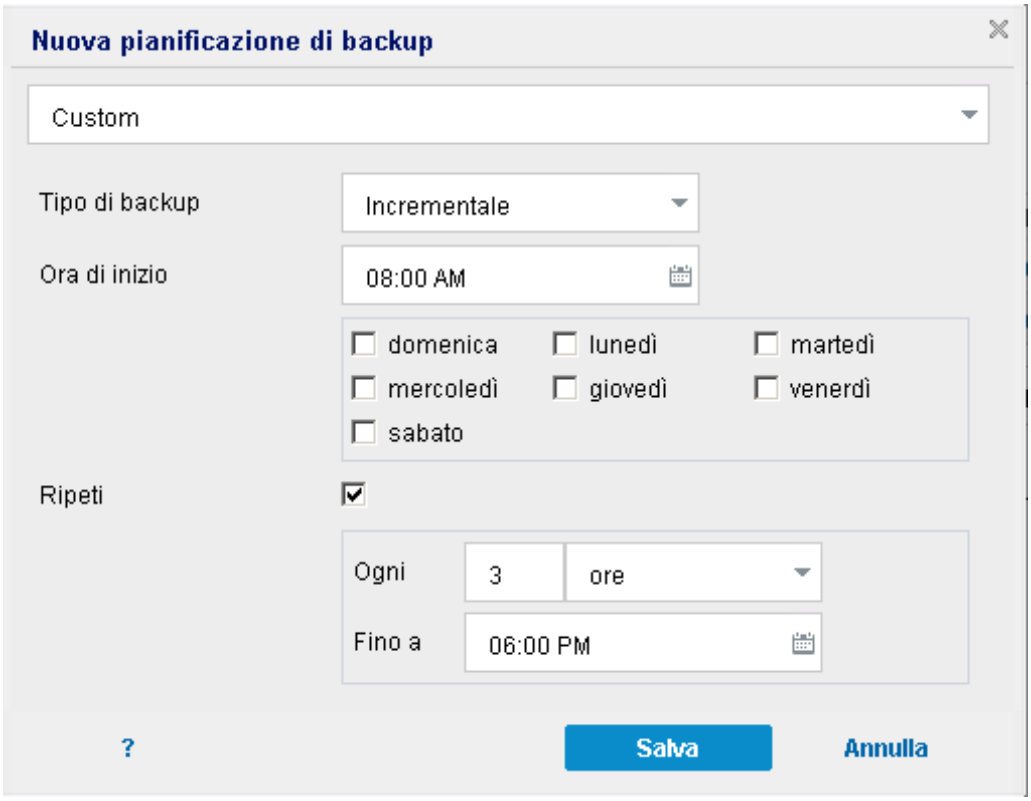
Effettuare le operazioni seguenti:

1. Aggiungere le pianificazioni di backup, di unione e di definizione del limite di velocità

   Aggiunta di una pianificazione di backup

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni di backup.

Incrementale

Specifica la pianificazione dei backup incrementali.

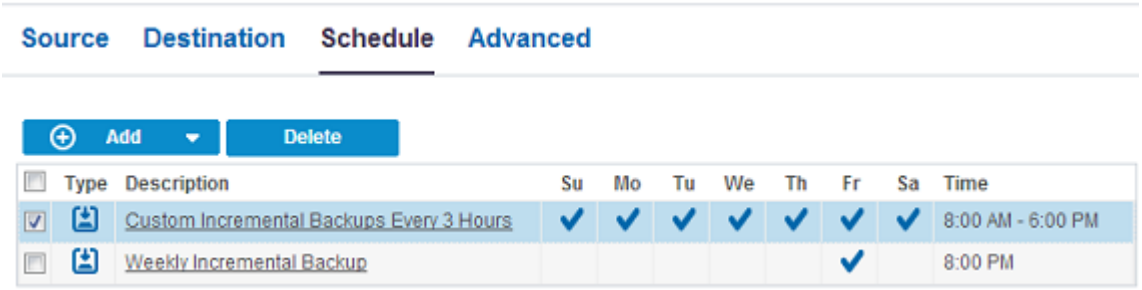
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di unione**.

La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

b. Specificare l'ora di inizio per il processo di unione.

c. Specificare **Fino a** per fornire un'ora di fine per il processo di unione.

d. Fare clic su **Salva**.

La pianificazione di unione specificata viene visualizzata nella pagina **Pianificazione**.

Aggiungi pianificazione del limite delle risorse

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

Viene visualizzata la finestra di dialogo **Aggiungi nuova pianificazione del limite delle risorse**.

b. Specificare il limite di velocità effettiva in MB per unità di minuti.

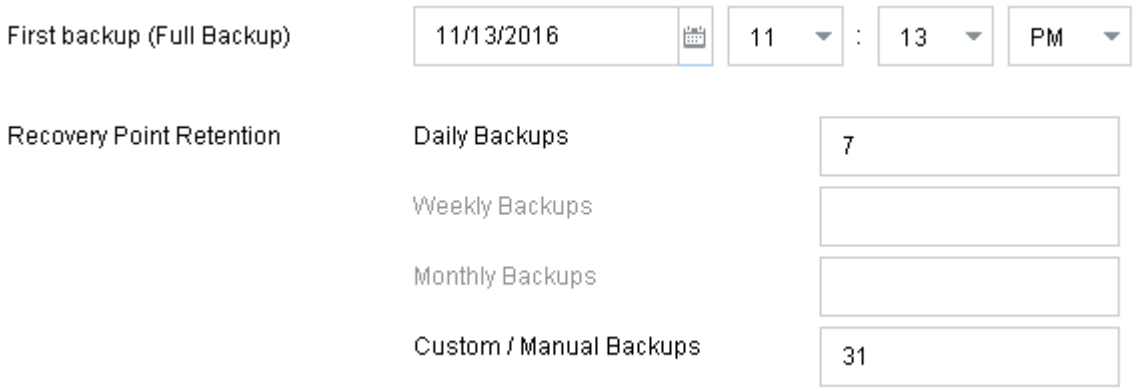
c. Specificare l'ora di inizio per il processo del limite di velocità effettiva del backup.

d. Specificare **Fino a** per fornire un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

La pianificazione del limite delle risorse specificata viene visualizzata nella pagina **Pianificazione**.

2. Specificare l'ora di inizio per il backup pianificato.



3. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

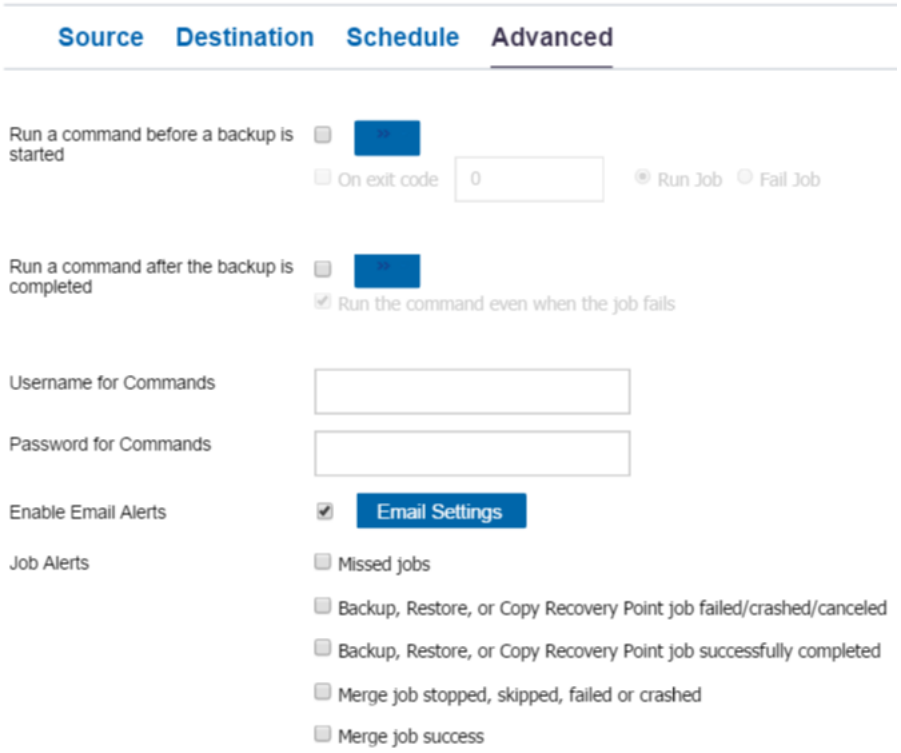
   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo **Pianificazione di backup**.

   Viene specificata la pianificazione.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda **Avanzate:**



Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

   Esegui un comando prima dell'avvio di un backup

   Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script all'interno del nodo proxy. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Processo con errore** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

   Esegui un comando al completamento di un backup

   Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso completo di archiviazione dello script.

   Esegui un comando anche quando il processo non riesce

Se questa casella di controllo è selezionata, lo script specificato in **Esegui comando al completamento del backup** viene eseguito anche quando il processo di backup produce un errore. In caso contrario, lo script viene eseguito solo quando il processo di backup viene completato correttamente.

Nome utente comandi

Consente di specificare il nome utente per eseguire i comandi.

Password comandi

Consente di specificare la password per eseguire i comandi.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere in un messaggio di posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy. Per ulteriori informazioni sulla configurazione delle impostazioni di posta elettronica, consultare la sezione Configurazione di posta elettronica e avvisi.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo proxy e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su **Salva.**

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo. È possibile aggiungere le attività **Copia punto di ripristino**, **Copia su nastro**, **Replica**, e **Replica da RPS remoto** come attività di completamento.

Il piano viene distribuito automaticamente sul nodo del server proxy.

Viene creato il piano di backup di SharePoint Online per il server proxy. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione.** È possibile eseguire anche un backup manuale in qualsiasi momento.

(Facoltativo) Esecuzione di un backup manuale

In genere, in base alle impostazioni di pianificazione applicate, i backup vengono eseguiti automaticamente. In aggiunta al backup pianificato, un backup manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze. Se ad esempio si dispone di una pianificazione di ripetizione per backup completi e incrementali e si desidera apportare modifiche sostanziali al computer, è possibile eseguire un backup manuale immediato senza attendere l'esecuzione del backup pianificato successivo.

Per eseguire un backup manuale dei nodi SharePoint Online, procedere come segue:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   I nodi SharePoint Online vengono mostrati nel riquadro centrale.
3. Selezionare i nodi SharePoint Online (ad esempio, Mailbox@<organizationname.com>) di cui si desidera eseguire il backup e accertarsi che sia stato assegnato un piano. Il nome del nodo corrisponde all'account utilizzato durante l'aggiunta del nodo SharePoint Online e alla sua connessione.
4. Fare clic con il pulsante destro del mouse sul nodo, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
5. Selezionare il tipo di backup che si desidera eseguire, quindi fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.
6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.
7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Il backup manuale è stato eseguito correttamente.

Per eseguire un backup manuale di un piano SharePoint Online, procedere come segue:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Piani**, quindi fare clic su **Tutti i piani**.

I piani di backup di SharePoint Online vengono visualizzati nel riquadro centrale.

3. Selezionare il piano di cui si desidera eseguire il backup e ai quali è stato assegnato un piano.
4. Fare clic con il pulsante destro del mouse sul piano, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
5. Selezionare il tipo di backup che si desidera eseguire, quindi fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.
6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.
7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Il backup manuale è stato eseguito correttamente.

Verifica del backup

Per verificare il processo di backup, confermare di avere creato correttamente il piano di backup. Dopo avere verificato che il piano è stato creato correttamente, confermare se il processo di backup è in esecuzione secondo quanto pianificato. È possibile verificare lo stato dei processi di backup dalla scheda **Processi**.

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Attenersi a uno dei seguenti metodi per verificare i processi di backup:

Metodo 1

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Tutti i processi completati**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Metodo 2

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Processi completati correttamente**.

   L'elenco dei processi di backup completati viene visualizzato nel riquadro centrale.
3. Fare clic sul processo che si desidera verificare.

   Il riquadro destro viene aggiornato.
4. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
5. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Configurazione per l'autenticazione a più fattori

Quando un'organizzazione dispone dell'autenticazione a più fattori (MFA) abilitata per gli utenti, utilizzare l'autenticazione moderna per aggiungere i nodi.

Nota: anche se l'autenticazione di base è abilitata sul tenant, è possibile utilizzare l'autenticazione moderna per aggiungere nodi. Per ulteriori informazioni sull'aggiunta di nodi a un piano mediante l'autenticazione moderna, consultare la sezione Autenticazione moderna.

Creazione di un piano di backup per OneDrive Microsoft Office 365

OneDrive, che fa parte del servizio cloud di Microsoft Office 365, semplifica le operazioni di archiviazione su cloud e la condivisione dei file. Per proteggere gli elementi di OneDrive (file, cartelle e così via) nel cloud Microsoft, è necessario creare un piano. Il piano per OneDrive è costituito da un'attività di backup, che consente di specificare i nodi di OneDrive da proteggere, la destinazione del backup e la pianificazione di backup.

Come procedere?

1. Verifica delle considerazioni e dei prerequisiti
2. Creazione di un piano di backup per OneDrive
3. (Facoltativo) Esecuzione di un backup manuale
4. Configurazione per l'autenticazione a più fattori

Verifica delle considerazioni e dei prerequisiti

Rivedere i prerequisiti e le considerazioni seguenti prima di creare un piano di backup di OneDrive.

Creazione di un piano di backup di OneDrive:

Prerequisito:

- L'esecuzione dello script PowerShell è abilitata sul server proxy. Se non è abilitata, eseguire il comando: *Set-ExecutionPolicy RemoteSigned*
- Il server proxy deve essere connesso a Microsoft Azure.

Considerazioni:

Negli Stati Uniti, in Cina e in Germania i servizi cloud Microsoft sono diversi a causa delle normative nazionali per sui cloud. Per ulteriori dettagli, consultare questo collegamento. Durante la distribuzione del prodotto in tali aree, è necessario modificare le impostazioni.

Effettuare le operazioni seguenti:

1. Aprire il file di configurazione disponibile nel percorso di installazione $UDP.

   $/Engine/Bin/Office365/Arcserve.Office365.Onedrive.json

2. Trovare l'impostazione **Region**, quindi impostare il valore su Germany, China

o US Government.

Valore predefinito: Normal

Creazione di un piano di backup di OneDrive mediante l'autenticazione di base (BA):

Verificare quanto segue:

- Installare PowerShell versione 5.1 o versioni successive (appartenente a Windows Management Framework (WMF)) sul server proxy (computer a 64 bit).
- Installare i seguenti moduli PowerShell sul server proxy utilizzando la finestra PowerShell:
  - Per installare il modulo Azure , eseguire il comando seguente:

    Install-Module -Name AzureAD -Force
  - Per installare il modulo ExchangeOnlineManagement, eseguire il comando seguente:

    Install-Module -Name ExchangeOnlineManagement -Force

  Nota: quando si installano i moduli PowerShell utilizzando i comandi precedenti, è possibile che venga installata una versione più recente dei moduli in base alla versione GA del componente disponibile nel repository Microsoft.

Creazione di un piano di backup di OneDrive mediante l'autenticazione moderna (MA):

Verificare i prerequisiti prima di creare un piano utilizzando l'autenticazione moderna.

Creazione di un piano di backup per OneDrive

Un piano di backup include un'attività di backup che esegue un backup degli elementi dati di OneDrive (file, cartelle e così via) e memorizza i dati in un archivio dati con o senza deduplicazione. Inoltre, questo piano di backup consente a UDP di rilevare e specificare i gruppi OneDrive per i quali viene eseguita un'attività di backup. Ciascuna attività consiste di parametri che definiscono l'origine, la destinazione, la pianificazione, e altri dettagli di backup.

Effettuare le operazioni seguenti:

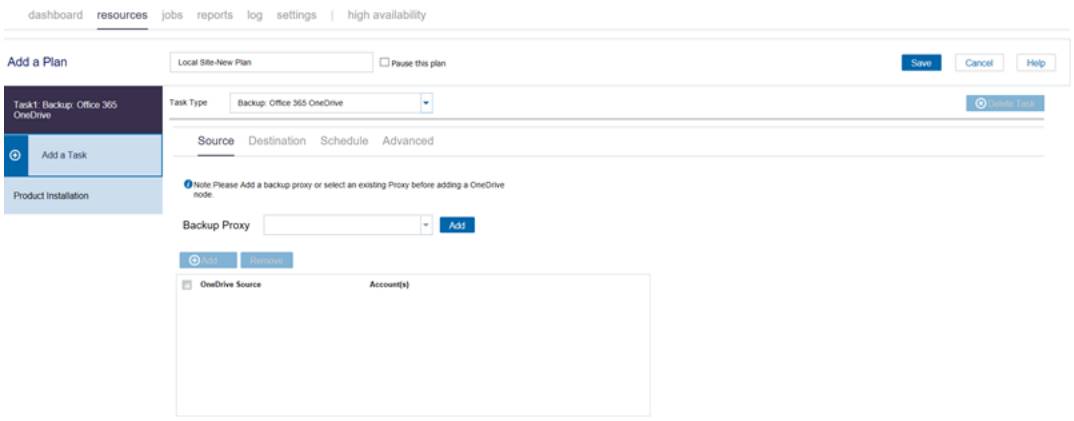
1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa Tipo di attività, selezionare **Backup: Office 365 OneDrive**.



Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine di OneDrive che si desidera proteggere. È possibile selezionare più nodi di origine di OneDrive per piano. Se non sono stati aggiunti nodi di origine alla console, è possibile aggiungerli dalla pagina Origine di OneDrive.

Nota: è possibile salvare un piano senza aggiungere nodi di origine. Il piano non verrà comunque distribuito a meno che vengano aggiunti altri nodi.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Origine**.
2. Selezionare **Proxy di backup** dall'elenco a discesa.
3. Aggiungere il nodo di OneDrive utilizzando uno dei seguenti metodi:

   Metodo 1

   a. Fare clic su **Aggiungi**, quindi su **Seleziona origine da proteggere in Arcserve UDP**.

      Viene visualizzata la finestra di dialogo Aggiungi nodi al piano.

   b. Selezionare un nodo e fare clic su **Connetti**.

      Nota: per ricercare i nodi di OneDrive che si desidera proteggere, è possibile utilizzare anche il campo di ricerca.

   c. Selezionare la casella di controllo per la **protezione completa degli account OneDrive** per proteggere tutti gli account OneDrive in tutte le pagine. Per selezionare solo alcuni account, fare clic sulla freccia a destra della casella di controllo e specificare gli account.

      Gli account OneDrive selezionati vengono aggiunti.

Metodo 2

a. Fare clic su **Aggiungi**, quindi su **Aggiungi origine OneDrive**.

Note:

- Utilizzare questa opzione per rilevare e specificare i gruppi di distribuzione per OneDrive.
- Diversamente da altri nodi, il nodo OneDrive non può essere aggiunto dalla pagina Tutti i nodi. È possibile aggiungere un nodo OneDrive soltanto in un piano o quando si modifica un piano.

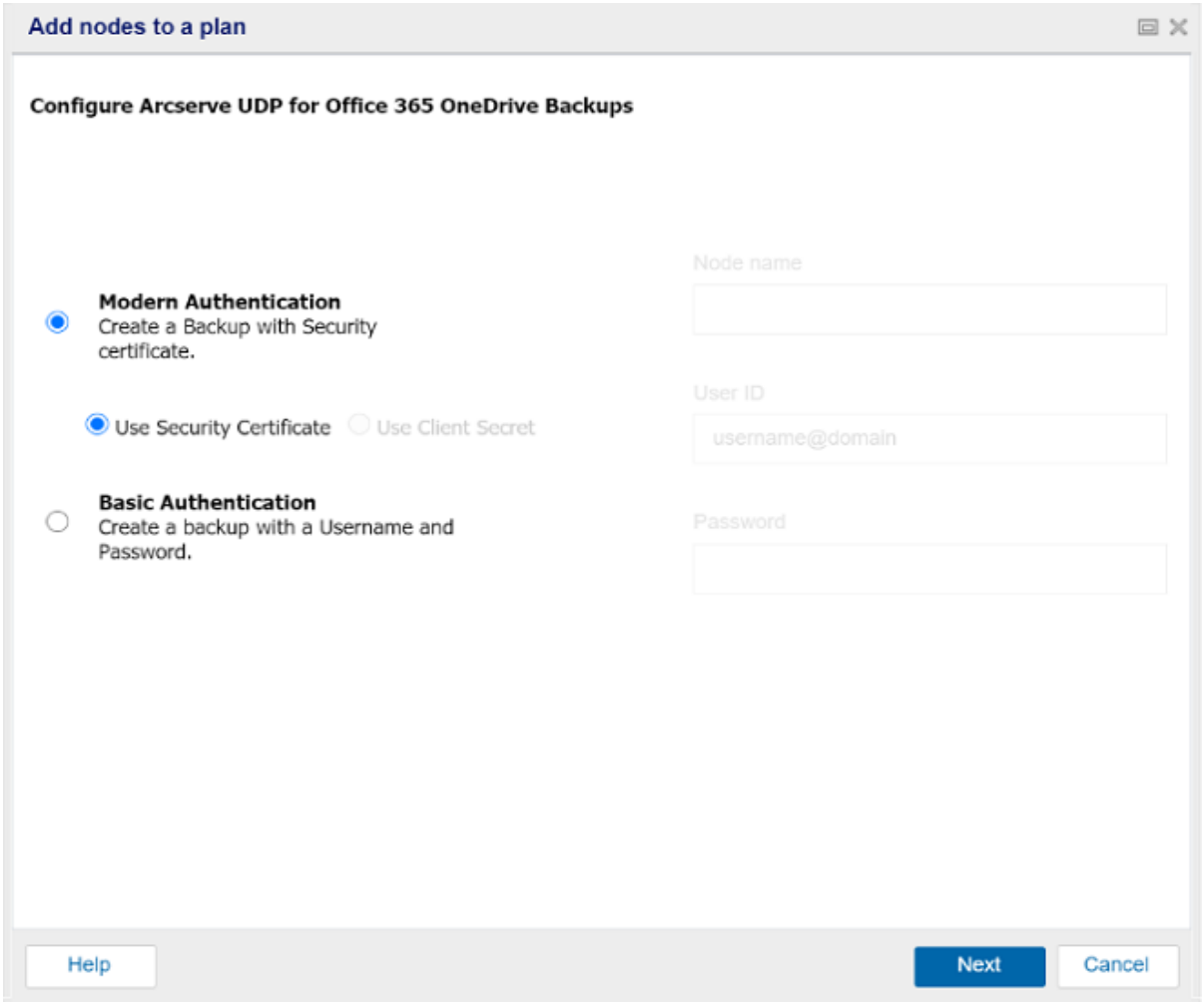
b. Per aggiungere il nodo OneDrive dal piano, specificare il nome del nodo, l'ID utente e la password. Non è possibile modificare il nome del nodo dopo aver creato il nodo OneDrive. Uno stesso account utente (account servizio) di OneDrive può essere utilizzato da più nodi di OneDrive.

Nota: si consiglia di selezionare l'account utente degli amministratori di Azure Active Directory.

4. Per applicare l'autenticazione, eseguire una delle seguenti operazioni:

Autenticazione moderna

Per l'autenticazione moderna, è possibile eseguire un backup utilizzando il certificato di sicurezza.



Usa certificato di sicurezza

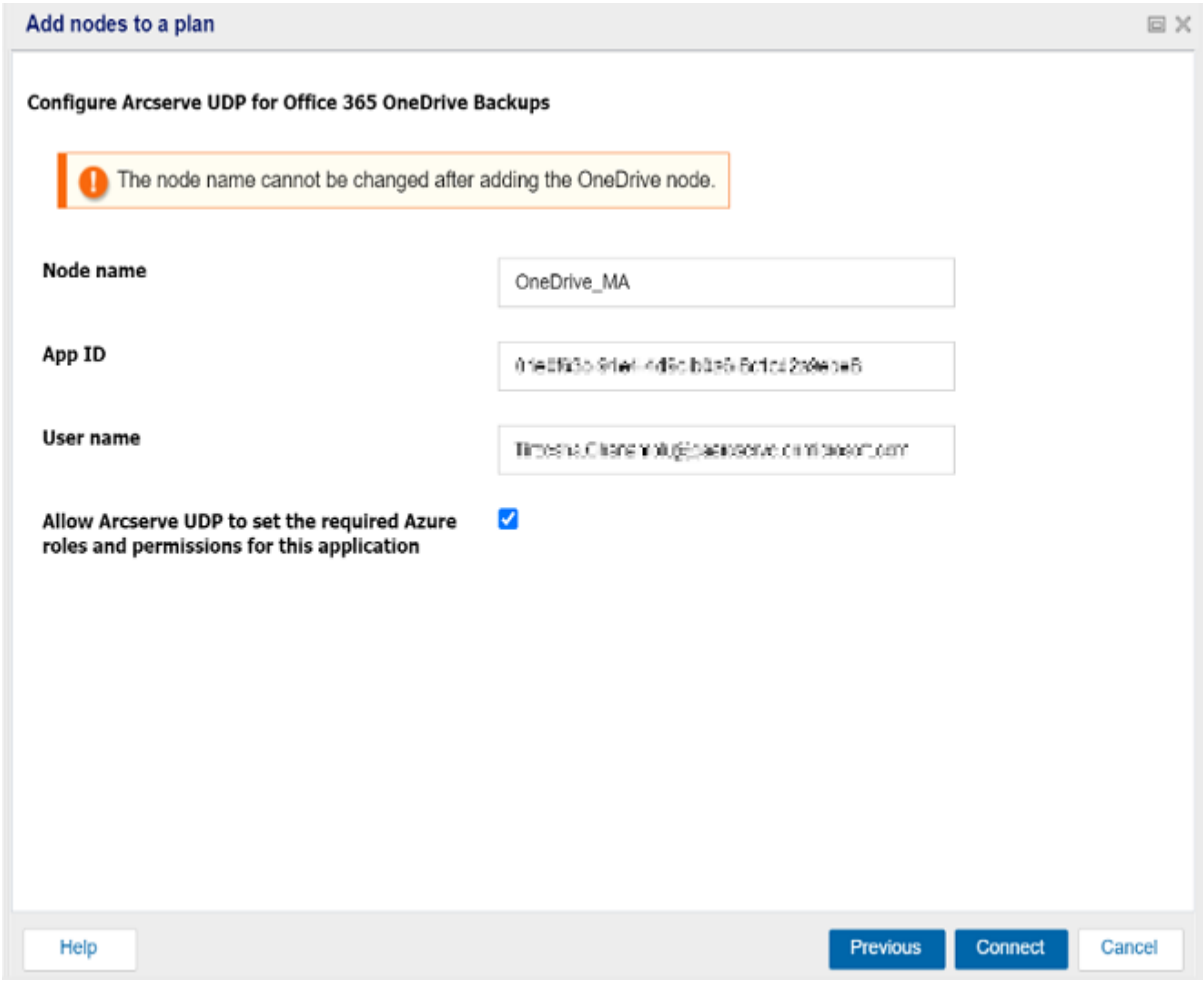
Nota: per impostazione predefinita, il piano di backup seleziona l'opzione **Usa certificato di sicurezza** per l'autenticazione moderna.

Effettuare le operazioni seguenti:

a. Per eseguire l'autenticazione dell'applicazione UDP con i certificati di protezione, consultare la sezione Download del certificato da UDP e caricamento in Azure.

b. Immettere le seguenti informazioni:

- Nome nodo
- ID app
- Nome utente



Nota: i nomi dei nodi di OneDrive non possono essere modificati dopo la creazione di un nodo.

c. Per applicare automaticamente le autorizzazioni API, selezionare la casella di controllo **Consenti ad Arcserve UDP di impostare le autorizzazioni API richieste per questa applicazione**.

   Nota: per applicare manualmente le autorizzazioni senza utilizzare il ruolo di amministratore globale/aziendale, consultare la sezione Configurazione manuale delle autorizzazioni API senza utilizzare il ruolo di amministratore globale/aziendale.

d. Fare clic su **Connetti**.

Autenticazione di base

Per l'autenticazione di base, per procedere con il backup attenersi alla procedura riportata di seguito:

a. Selezionare Autenticazione di base, immettere il nome del nodo, il nome utente e la password, quindi fare clic su **Connetti**.

   L'URL di Arcserve UDP viene aperto in un browser e richiede l'autorizzazione per tutti i dati di lettura/scrittura di Arcserve UDP dal portale OneDrive.

b. Nel browser, utilizzare le credenziali di amministratore di Microsoft Azure per effettuare l'accesso.

   Viene aperto il portale Azure.

c. Dal portale di Microsoft Azure, procedere come segue per configurare l'applicazione UDP:

   I. Fare clic su **Autorizzazioni API**.

   ii. Nel riquadro destro, fare clic sul pulsante **Concedi autorizzazioni per**.

   iii. Fare clic su **Sì** per acconsentire alla concessione delle autorizzazioni.

   iv. Dopo aver concesso l'autorizzazione, in Arcserve UDP accedere ad **Aggiungi un piano > Aggiungi nodi a un piano**, quindi fare clic sul pulsante **Avanti**.

   Nota: se si chiude l'URL di concessione delle autorizzazioni e si desidera riaprirlo, fare clic sul pulsante **Qui** nella schermata Aggiungi nodo al piano di UDP.

Arcserve UDP elenca tutti gli account del titolare corrente.

5. Per proteggere gli account OneDrive, eseguire una delle operazioni seguenti:

   - Per proteggere tutti gli account e i gruppi OneDrive, selezionare la casella di controllo **Proteggi tutti gli account OneDrive**.

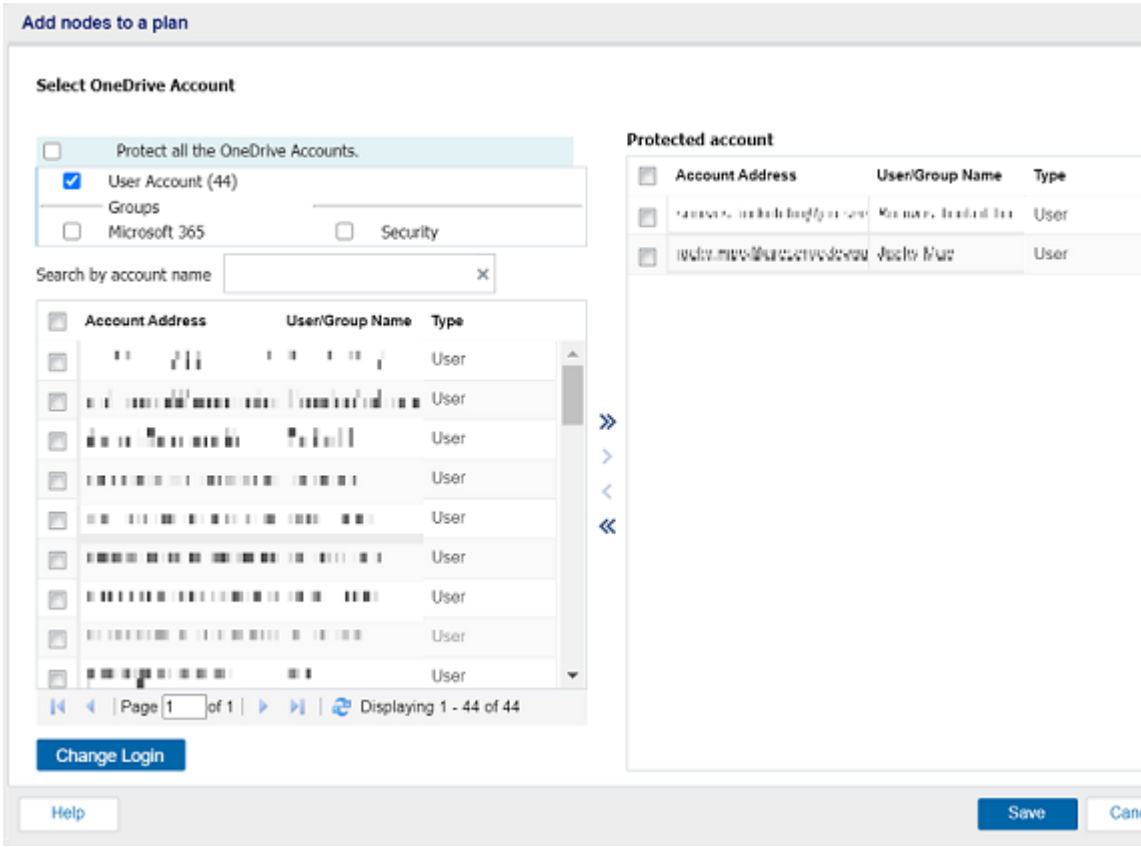
     Nota: questa opzione viene selezionata automaticamente per impostazione predefinita quando viene visualizzata la schermata Seleziona account OneDrive.

   - Per l'account utente, procedere come segue:

     a. Selezionare la casella di controllo **Account utente**.

        Viene visualizzato un elenco di account utente.

     b. (Facoltativo) Per cercare un account dall'elenco, nel campo Cerca per nome account, immettere il nome dell'account.



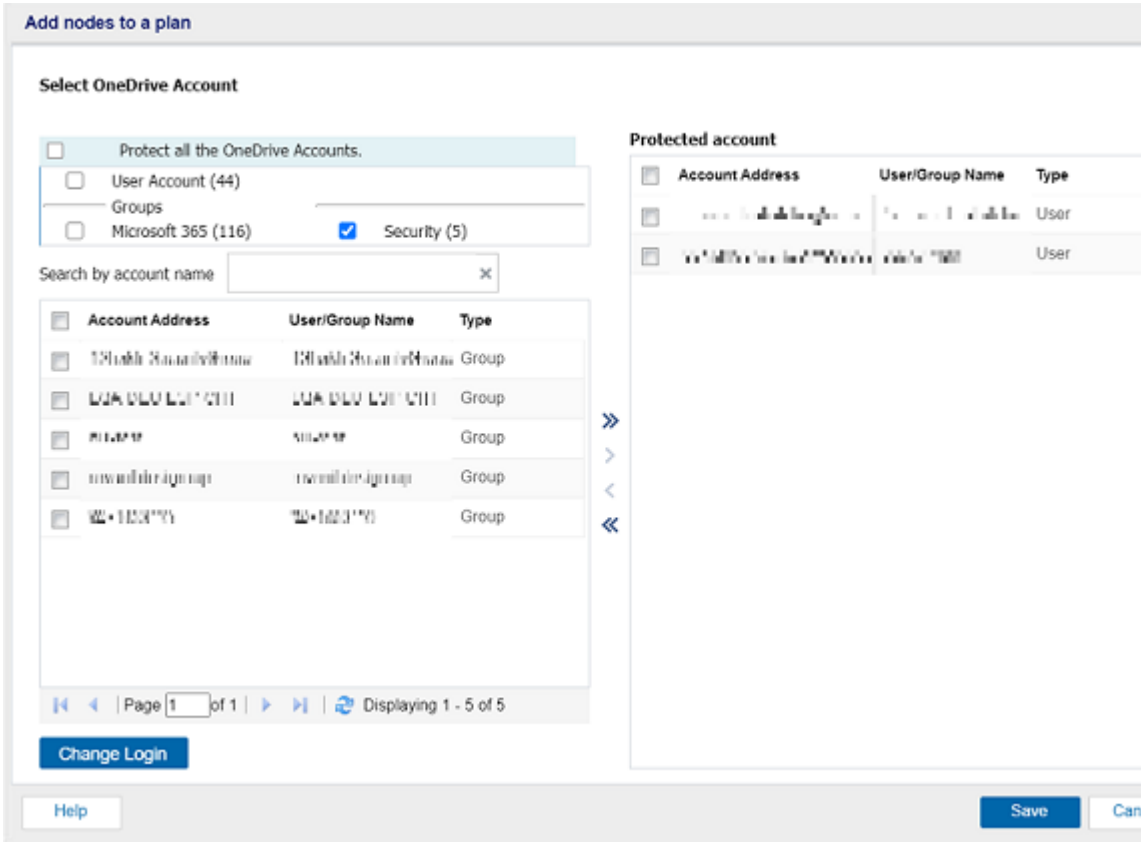
c. Dall'elenco degli account utente, selezionare gli account che si desidera proteggere.

d. Fare clic sulla freccia destra (>) per spostare gli account selezionati nell'elenco degli account protetti.

- Per i gruppi, procedere come segue:

a. Selezionare la casella di controllo **Microsoft 365** o **Sicurezza**.

In base alla selezione, viene visualizzato un elenco di gruppi.



b. (Facoltativo) Per cercare un account dall'elenco, nel campo Cerca per nome account, immettere il nome dell'account.

c. Dall'elenco dei gruppi, selezionare i gruppi che si desidera proteggere.

d. Fare clic sulla freccia destra (>) per spostare i gruppi selezionati nell'elenco degli account protetti.

6. Fare clic su **Salva**.

   Gli account OneDrive selezionati vengono aggiunti.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Destinazione**.

   L'opzione **Recovery Point Server di Arcserve UDP** viene selezionata automaticamente. **Arcserve UDP Recovery Point Server** specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono

archiviati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.

2. Fornire i dettagli seguenti:
   a. Selezionare un Recovery Point Server.
   b. Selezionare un archivio dati di deduplicazione o di non deduplicazione. L'elenco mostra tutti gli archivi dati creati per il Recovery Point Server specificato.
   c. Fornire una password di sessione. Quando la destinazione del backup è un archivio dati RPS non crittografato, la password di sessione è facoltativa.
   d. Confermare la password di sessione.

   La destinazione viene specificata. Ora specificare i dettagli in Pianificazione e Avanzate.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

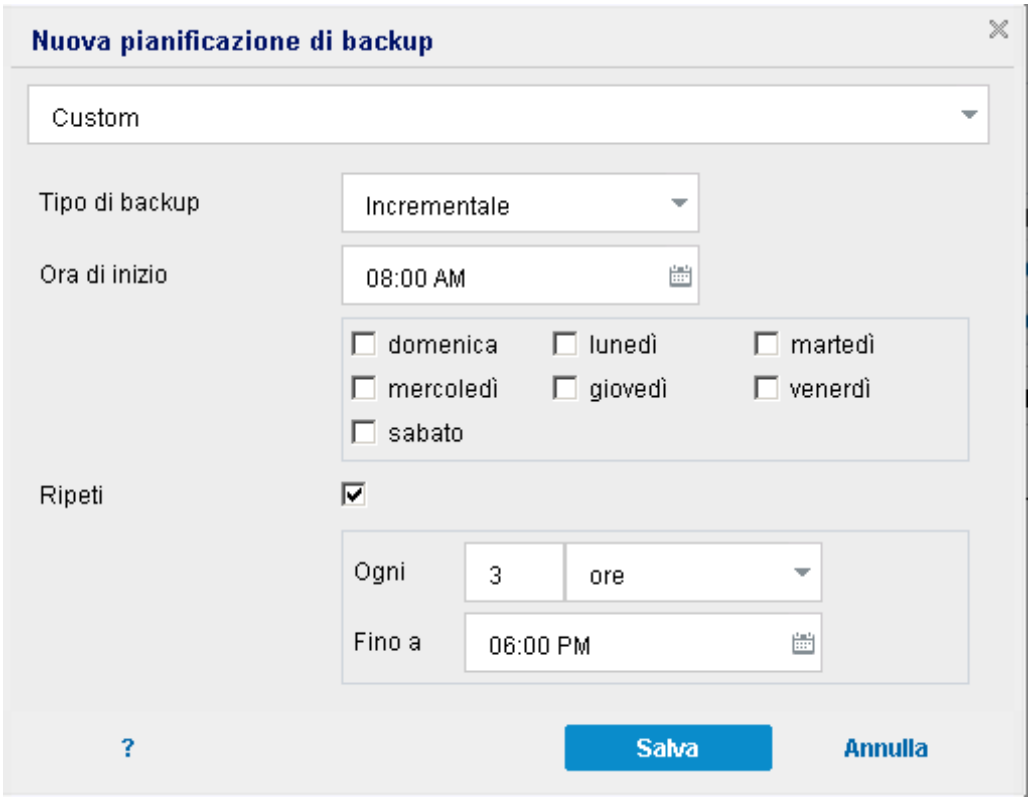
Effettuare le operazioni seguenti:

1. Aggiungere le pianificazioni di backup, di unione e di definizione del limite di velocità

   Aggiunta di una pianificazione di backup

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni di backup.

Incrementale

Specifica la pianificazione dei backup incrementali.

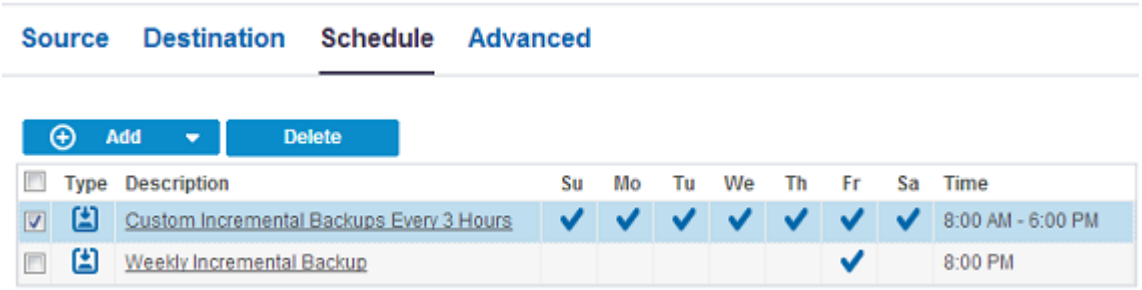
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup con dimensioni molto ridotte. Questa opzione è la soluzione ottimale per l'esecuzione del backup.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di unione**.

La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

b. Specificare l'ora di inizio per l'avvio del processo di unione.

c. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

d. Fare clic su **Salva**.

La pianificazione di unione specificata viene visualizzata nella pagina **Pianificazione**.

Aggiungi pianificazione del limite delle risorse

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

Viene visualizzata la finestra di dialogo **Aggiungi nuova pianificazione del limite delle risorse**.

b. Specificare il limite di velocità effettiva in MB per unità di minuti.

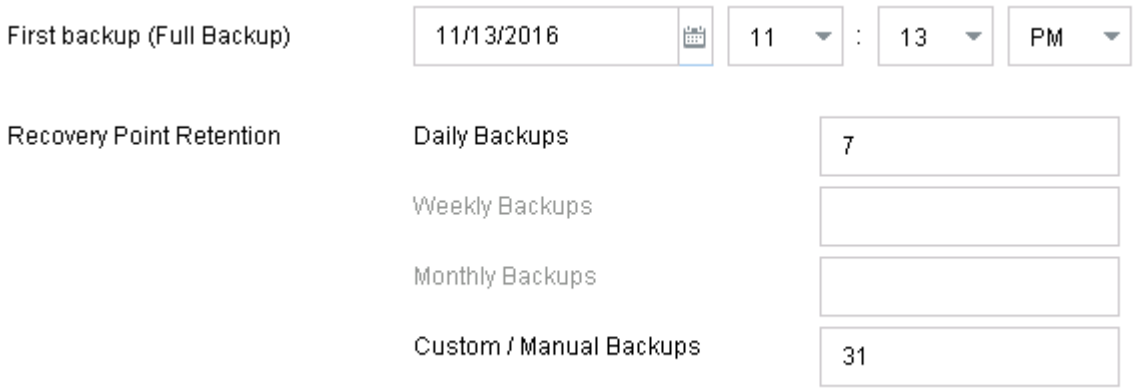
c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

La pianificazione del limite delle risorse specificata viene visualizzata nella pagina **Pianificazione**.

2. Specificare l'ora di inizio per il backup pianificato.



3. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

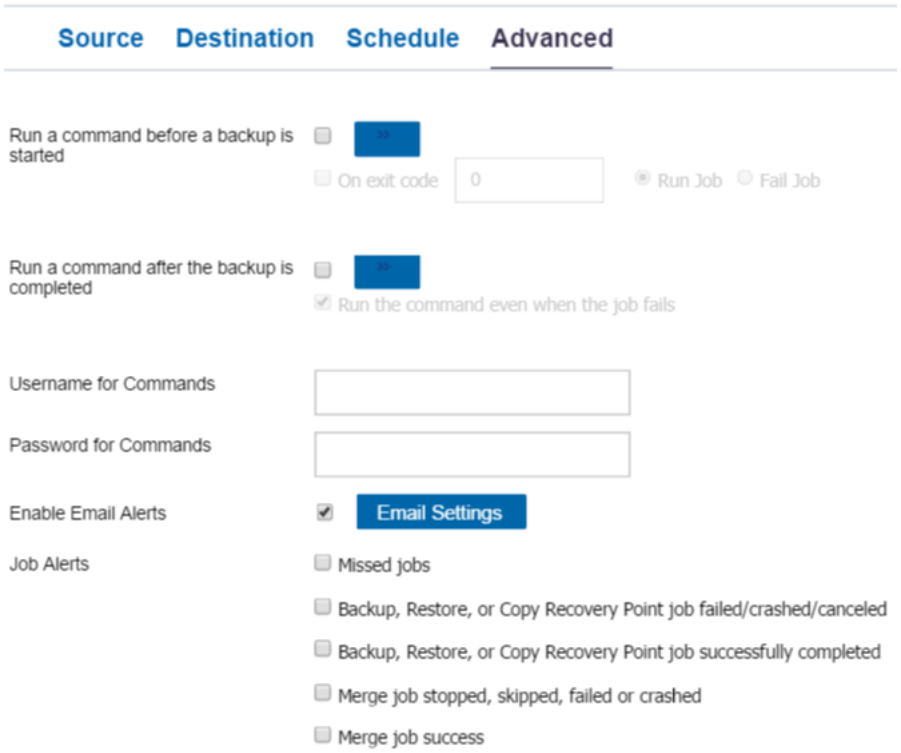
   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo **Pianificazione di backup**.

   Viene specificata la pianificazione. Specificare i dettagli in Avanzate.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda **Avanzate:**



Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

   Esegui un comando prima dell'avvio di un backup

   Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script all'interno del nodo proxy. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Processo con errore** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

   Esegui un comando al completamento di un backup

   Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso completo di archiviazione dello script.

   Esegui un comando anche quando il processo non riesce

   Se questa casella di controllo è selezionata, lo script specificato in **Esegui comando al completamento del backup** viene eseguito anche quando il processo di backup produce un errore. In caso contrario, lo script viene eseguito solo quando il processo di backup viene completato correttamente.

   Nome utente comandi

   Consente di specificare il nome utente per eseguire i comandi.

Password comandi

Consente di specificare la password per eseguire i comandi.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere in un messaggio di posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy. Per ulteriori informazioni sulla configurazione delle impostazioni di posta elettronica, consultare la sezione Configurazione di posta elettronica e avvisi.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo proxy e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su **Salva.**

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo. È possibile aggiungere le attività **Copia punto di ripristino**, **Copia su nastro**, **Replica**, e **Replica da RPS remoto** come attività di completamento.

Il piano viene distribuito automaticamente sul nodo del server proxy.

Viene creato il piano di backup in linea di Exchange per il server proxy. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

(Facoltativo) Esecuzione di un backup manuale

In genere, in base alle impostazioni di pianificazione applicate, i backup vengono eseguiti automaticamente. In aggiunta al backup pianificato, un backup manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze. Se ad esempio si dispone di una pianificazione di ripetizione per backup completi e incrementali e si desidera apportare modifiche sostanziali al computer, è possibile eseguire un backup manuale immediato senza attendere l'esecuzione del backup pianificato successivo. È possibile inoltrare il processo di backup sia dalla console, sia dall'interfaccia utente del proxy. Utilizzando Monitoraggio processi, è possibile visualizzare lo stato del processo e annullare il processo in corso.

Per eseguire un backup manuale dei nodi OneDrive, Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   I nodi di OneDrive vengono mostrati nel riquadro centrale.
3. Selezionare i nodi di OneDrive di cui si desidera eseguire il backup e a cui è stato assegnato un piano.
4. Nel riquadro centrale, fare clic su **Azioni**, **Esegui backup**.

   Verrà visualizzata la finestra di dialogo **Esegui un backup immediato**.
5. Selezionare un tipo di backup e assegnare facoltativamente un nome al processo di backup.
6. Fare clic su **OK**.

   Il processo di backup viene eseguito.

Effettuare le operazioni seguenti: per eseguire il backup manuale di un piano OneDrive

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   I piani di backup di OneDrive vengono visualizzati nel riquadro centrale.
3. Selezionare il piano di cui si desidera eseguire il backup e ai quali è stato assegnato un piano.
4. Nel riquadro centrale, fare clic su **Azioni**, **Esegui backup**.

   Verrà visualizzata la finestra di dialogo **Esegui un backup immediato**.
5. Selezionare un tipo di backup e assegnare facoltativamente un nome al processo di backup.

6. Fare clic su **OK**.

   Il processo di backup viene eseguito.

   Il backup manuale è stato eseguito correttamente. A questo punto, è possibile verificare il backup.

Verifica del backup

Per verificare il processo di backup, confermare di avere creato correttamente il piano di backup. Dopo avere verificato che il piano è stato creato correttamente, confermare se il processo di backup è in esecuzione secondo quanto pianificato. È possibile verificare lo stato dei processi di backup dalla scheda **Processi**.

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

   Attenersi a uno dei seguenti metodi per verificare i processi di backup:

   Metodo 1

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Tutti i processi completati**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

   Metodo 2

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Processi completati correttamente**.

   L'elenco dei processi di backup completati viene visualizzato nel riquadro centrale.
3. Fare clic sul processo che si desidera verificare.

   Il riquadro destro viene aggiornato.
4. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
5. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Configurazione per l'autenticazione a più fattori

Quando un'organizzazione dispone dell'autenticazione a più fattori (MFA) abilitata per gli utenti, utilizzare l'autenticazione moderna per aggiungere i nodi.

Nota: anche se l'autenticazione di base è abilitata sul tenant, è possibile utilizzare l'autenticazione moderna per aggiungere nodi. Per ulteriori informazioni sull'aggiunta di nodi a un piano mediante l'autenticazione moderna, consultare la sezione Autenticazione moderna.

Gestione del backup e del ripristino di Microsoft Teams

In questa sezione vengono fornite informazioni su come eseguire il backup e il ripristino dei dati di Microsoft Teams utilizzando Exchange Online e SharePoint Online. Arcserve UDP fornisce il backup dei messaggi (chat) e dei file condivisi tra i canali privati, pubblici e di gruppo.

Ogni volta che si crea un canale privato, pubblico e di gruppo in Microsoft Teams, viene creato automaticamente un sito SharePoint Online. Questo sito SharePoint Online dispone di una cartella della raccolta documenti predefinita, in cui vengono salvati automaticamente tutti i file condivisi in tutte le conversazioni. È inoltre possibile personalizzare le autorizzazioni e le opzioni di protezione per le informazioni sensibili.

La presente sezione descrive i seguenti argomenti:

Esecuzione del backup e ripristino dei messaggi di Microsoft Teams (chat) mediante Exchange Online

È possibile eseguire il backup di singole chat utilizzando la casella di posta dell'utente nel backup del nodo UDP Exchange Online. Tutti i messaggi vengono archiviati nel server Exchange Online nella cartella TeamsMessagesData, contenuta in una cartella principale. In questa sezione vengono fornite informazioni su come eseguire il backup e il ripristino dei messaggi di Microsoft Teams (chat) mediante Exchange Online.

La presente sezione descrive i seguenti argomenti:

Esecuzione del backup di messaggi di Microsoft Teams (chat) utilizzando Exchange Online

In questa sezione vengono fornite informazioni su come eseguire il backup dei messaggi di Microsoft Teams (chat) mediante Exchange Online.

La presente sezione descrive i seguenti argomenti:

Creazione di un piano di backup di Exchange Online

Exchange Online è un'applicazione di posta elettronica ospitata su cloud di Microsoft. Per proteggere gli elementi di posta di Exchange Online (messaggi di posta elettronica, gli elementi calendario, contatti e così via) dal cloud Microsoft, è necessario creare un piano. Il piano di backup per Exchange Online consiste in un'attività di backup. Questa attività di backup consente di specificare i nodi Exchange Online che si desidera proteggere, la destinazione di backup e la pianificazione dei backup.

La presente sezione descrive i seguenti argomenti:

Verifica delle considerazioni e dei prerequisiti

Rivedere i prerequisiti e le considerazioni seguenti prima di creare un piano di backup di Exchange Online.

Creazione di un piano di backup di Exchange Online:

Prerequisiti:

Per l'account di backup:

- Utilizzare un account del servizio di backup con autorizzazioni di amministratore globale.
- Aggiungere le autorizzazioni di rappresentazione per l'utente di backup all'account di backup di Exchange Online per la connessione dell'organizzazione Exchange Online e l'esecuzione del backup e del ripristino.

  Nota: se non si aggiunge l'account di backup al gruppo del ruolo Discovery Management e non vengono assegnate le autorizzazioni di rappresentazione dell'applicazione, il backup non riesce.

- Associare l'account utente di backup con una casella di posta di Exchange Online.

Per il proxy di backup:

- Accedere alla Console.
- Installare l'agente Arcserve UDP sul computer proxy in cui si desidera eseguire il backup o il ripristino.

Considerazioni:

- Durante il backup di un ampio set di utenti, è possibile utilizzare i gruppi di Exchange per migliorare il backup e l'ottimizzazione.
- L'impostazione predefinita per il backup in linea di Exchange utilizza 4 thread di backup (un thread per utente) alla volta. È inoltre possibile modificare i thread nel file di configurazione di *Engine\BIN\Office365\Arcserve.Office365.Exchange.config* nel modo seguente:

  ```
  <!--#region for multi thread--> <!Valore predefinito --MultiThreadEnable: 0. Se attivato, impostare su 1.--> <add key-y="MultiThreadEnable" value ="1"/> <!--impostare quanti thread verranno utilizzati per i backup della casella di posta. default value is 4--> <add key-
  ```

```
="MaxDegreeOfParallelismForMailbox" value="4"/> <!--#endregion-
->
```

Si consiglia di impostare il valore da 1 a 5. Il valore massimo possibile è 10. Tuttavia, si consiglia di non impostare il valore da 6 a 10.

Nota: UDP 8.0 supporta quanto segue:

- Casella di posta dell'utente
- Casella di posta condivisa
- Cartelle pubbliche abilitate per la posta
- Caselle di posta della stanza
- Caselle di posta dell'apparecchiatura
- Caselle di posta di gruppo

Nota: per ulteriori informazioni sulle procedure consigliate per Exchange Online, consultare la sezione Problemi correlati a Exchange Online.

Creazione di un piano di backup di Exchange Online mediante l'autenticazione di base (BA):

Rivedere i seguenti prerequisiti:

- Installare PowerShell versione 5.1 o versioni successive (appartenente a Windows Management Framework (WMF)) sul server proxy (computer a 64 bit).
- Installare i seguenti moduli PowerShell sul server proxy utilizzando la finestra PowerShell:
  - Per installare il modulo Azure , eseguire il comando seguente:

    Install-Module -Name AzureAD -Force
  - Per installare il modulo ExchangeOnlineManagement, eseguire il comando seguente:

    Install-Module -Name ExchangeOnlineManagement -Force

Nota: quando si installano i moduli PowerShell utilizzando i comandi precedenti, è possibile che venga installata una versione più recente dei moduli in base alla versione GA del componente disponibile nel repository Microsoft.

Creazione di un piano di backup di Exchange Online mediante l'autenticazione moderna (MA):

Verificare i prerequisiti prima di creare un piano utilizzando l'autenticazione moderna.

Aggiunta di un ruolo e di un gruppo obbligatori all'account di backup di Exchange Online per l'esecuzione di backup e ripristini

Aggiungere l'account di backup al gruppo del ruolo di gestione del rilevamento e assegnarvi le autorizzazioni di rappresentazione dell'applicazione.

Effettuare le operazioni seguenti:

1. Aggiungere il ruolo e il gruppo necessari tramite una delle seguenti modalità:

   Mediante il portale Office 365

a. Accedere al Portale di Office 365 con i privilegi di amministratore o con un account in possesso delle autorizzazioni di amministrazione globale.

   Viene visualizzata la pagina dell'interfaccia di amministrazione di Exchange.

b. Accedere alle **autorizzazioni** e dall'elenco a discesa Aggiungi, fare doppio clic su **Gestione individuazione**.

   Viene visualizzata la finestra di dialogo Gestione individuazione.

   Nota: i membri del gruppo del ruolo Gestione individuazione possono eseguire le ricerche nelle caselle di posta della struttura di Exchange per i dati che soddisfano determinati criteri.

c. In **Ruoli**, fare clic sul segno **+** per aggiungere il ruolo ApplicationImpersonation.

   Viene visualizzata la finestra di dialogo Selezionare un ruolo.

d. Dall'elenco a discesa **Nome visualizzato**, selezionare **ApplicationImpersonation**.

   Nota: il ruolo ApplicationImpersonation consente alle applicazioni di rappresentare gli utenti in un'organizzazione allo scopo di eseguire le attività per conto dell'utente.

e. Fare clic su **Aggiungi** per aggiungere il ruolo ApplicationImpersonation, quindi fare clic su **OK**.

f. Nella finestra di dialogo Gestione individuazione, in **Membri**, fare clic sul segno **+** per aggiungere l'account di backup come membro.

Viene visualizzata la finestra di dialogo Selezionare membri.

g. Dall'elenco a discesa Nome, selezionare l'account di backup, fare clic su **Aggiungi** per aggiungere il membro, quindi fare clic su **OK**.

   L'account di backup selezionato viene visualizzato in **Membri** della finestra di dialogo **Gestione rilevamento**.

h. Fare clic su **Salva**.

Utilizzo di Powershell in remoto

a. Per connettersi al titolare di Exchange Online tramite PowerShell remoto, consultare il seguente collegamento.

b. Dopo aver effettuato la connessione, per aggiungere l'account di backup come membro del gruppo del ruolo di Gestione rilevamento, utilizzare il seguente comando:

   `"Add-RoleGroupMember" cmdlet`

   Ad esempio: Add-RoleGroupMember "discovery management" -member use-rName@domain.onmicrosoft.com.

c. Per assegnare il ruolo di rappresentazione dell'applicazione all'account di backup, utilizzare il seguente comando:

   `"New-ManagementRoleAssignment" cmdlet`

   Esempio:

   New-ManagementRoleAssignment -Name: impersonationAssignmentName -Role:ApplicationImpersonation - User: "username@domain.onmicrosoft.com"

Il ruolo ApplicationImpersonation e il gruppo Membri vengono aggiunti all'account di backup di Exchange Online.

Creazione di un piano di backup di Exchange Online

Un piano di backup include un'attività di backup che esegue un backup degli elementi di posta elettronica di Exchange Online (messaggi di posta elettronica, calendari, contatti e così via) e archivia i dati in un archivio dati di deduplicazione o non di deduplicazione. Inoltre, questo piano di backup consente a UDP di rilevare e specificare i gruppi di Exchange Online per i quali viene eseguita un'attività di backup. Ciascuna attività consiste di parametri che definiscono l'origine, la destinazione, la pianificazione, e altri dettagli di backup.

Effettuare le operazioni seguenti:

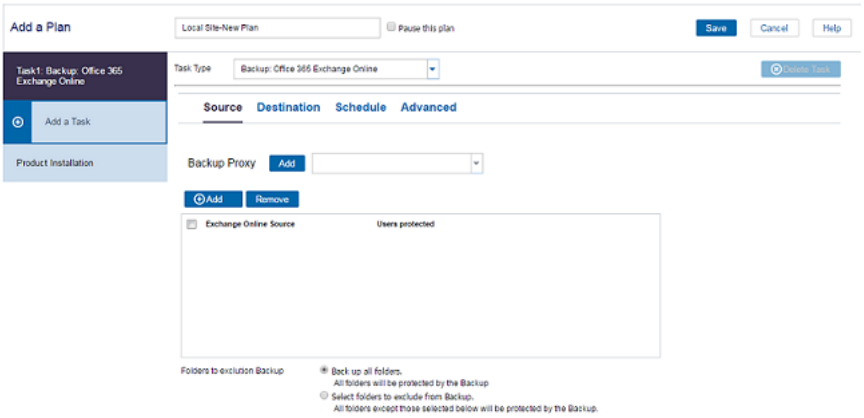
1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa Tipo di attività, selezionare **Backup: Exchange Online Office 365**.



Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

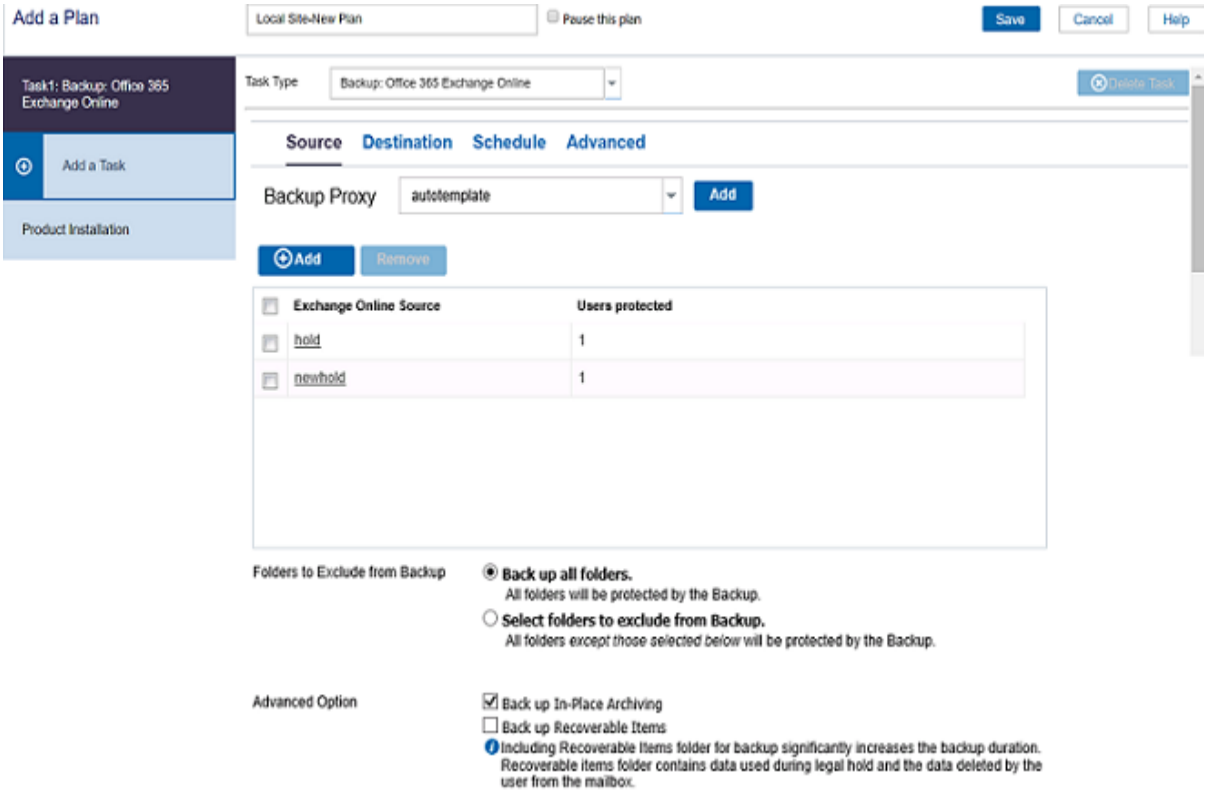
La pagina Origine consente di specificare i nodi di origine di Exchange Online che si desidera proteggere. È possibile selezionare più di un nodo di origine di Exchange Online per un piano. Se non sono stati aggiunti nodi di origine alla Console, è possibile aggiungerli dalla pagina Origine.

Nota: È possibile salvare un piano senza aggiungere nodi di origine. Il piano non verrà comunque distribuito a meno che vengano aggiunti altri nodi.

È inoltre possibile gestire i nodi Exchange Online utilizzando il supporto della casella di posta della cartella pubblica per la protezione Exchange Online.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Origine**.



2. Per il proxy di backup, eseguire una delle seguenti operazioni:
   - Dall'elenco a discesa, selezionare un proxy di backup esistente.
   - Per aggiungere un nuovo proxy di backup, fare clic su **Aggiungi** accanto all'elenco a discesa.
3. Aggiungere il nodo Exchange Online utilizzando una delle seguenti opzioni:

   Metodo 1

a. Fare clic su **Aggiungi**, quindi su **Seleziona origine da proteggere in Arcserve UDP**.

   Viene visualizzata la finestra di dialogo Aggiungi nodi al piano.

b. Selezionare un nodo e fare clic su **Connetti**.

   Nota: È inoltre possibile ricercare i nodi Exchange Online che si desidera proteggere nel campo di **ricerca**.

c. Selezionare la casella di controllo di **protezione completa delle origini di Office 365 Exchange** per proteggere tutti gli account di Exchange Online in tutte le pagine.

   Nota: Per aggiungere tutti gli account di Exchange Online all'elenco protetto, è possibile fare clic sulla freccia verso destra (>).

   Gli account di Exchange Online selezionati vengono aggiunti.

Metodo 2

- Fare clic su **Aggiungi**, quindi selezionare **Aggiungi origine Exchange Online**.

  Viene visualizzata la finestra di dialogo Aggiungi nodi a un piano.

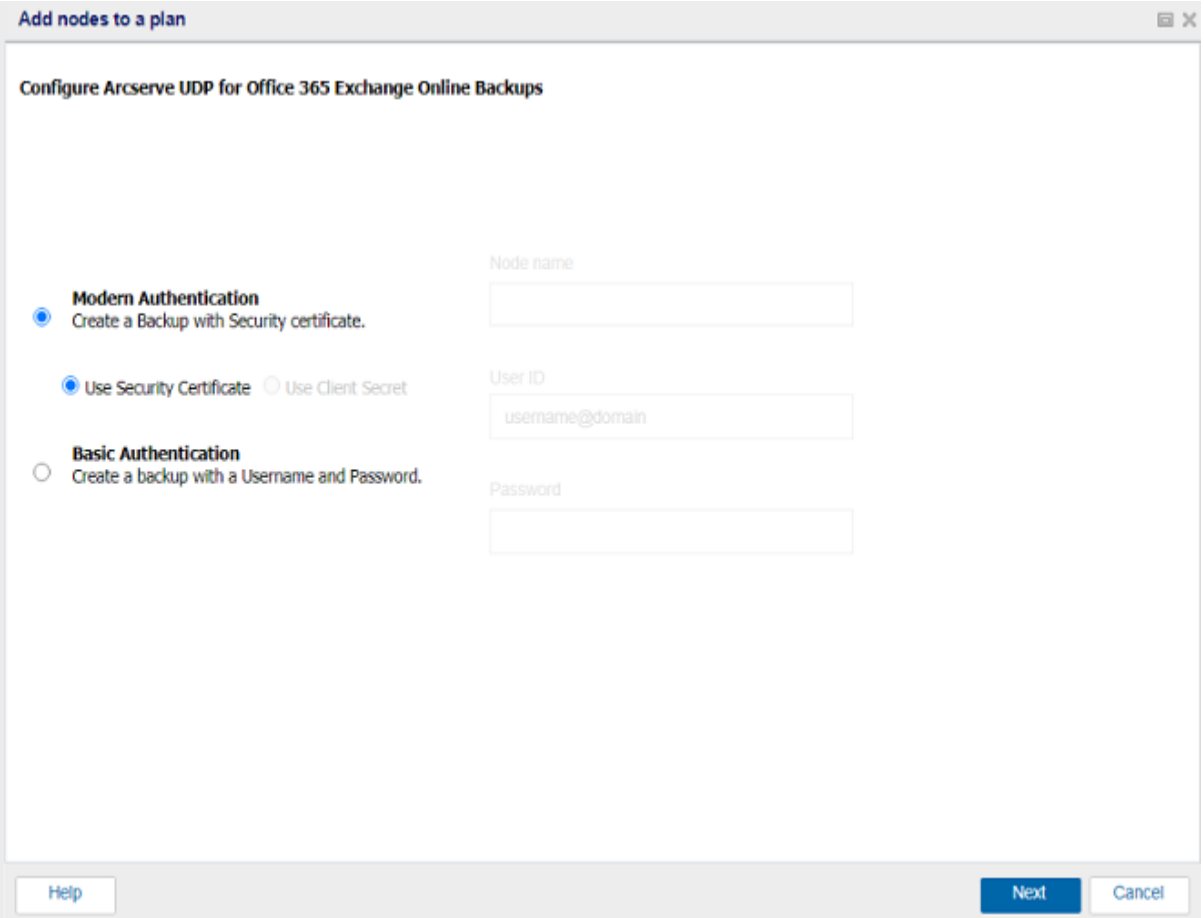
  Nota: A differenza di altri nodi, non è possibile aggiungere il nodo Exchange Online dalla pagina **Tutti i nodi**. È possibile aggiungere un nodo Exchange Online soltanto in un piano o con la modifica di un piano.

  Più nodi Exchange Online possono utilizzare lo stesso account utente (account servizio) di Exchange Online.

4. Per applicare l'autenticazione, eseguire una delle seguenti operazioni:

   Autenticazione moderna

   Per l'autenticazione moderna, è possibile eseguire un backup utilizzando il certificato di sicurezza.



Usa certificato di sicurezza

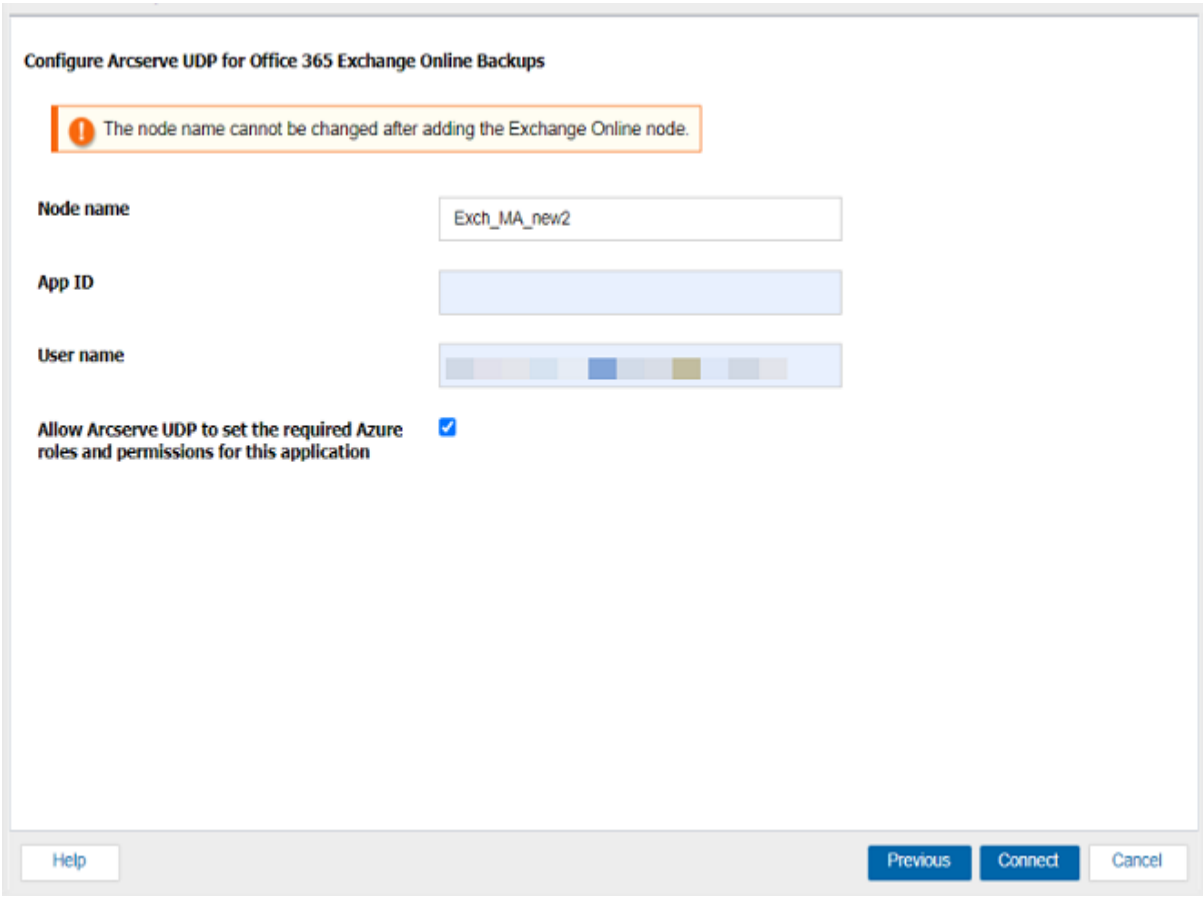
Nota: per impostazione predefinita, il piano di backup seleziona l'opzione **Usa certificato di sicurezza** per l'autenticazione moderna.

Effettuare le operazioni seguenti:

a. Per eseguire l'autenticazione dell'applicazione UDP con i certificati di protezione, consultare la sezione Download del certificato da UDP e caricamento in Azure.

b. Immettere le seguenti informazioni:

   - Nome nodo
   - ID app
   - Nome utente



c. Per applicare automaticamente le autorizzazioni API, selezionare la casella di controllo **Consenti ad Arcserve UDP di impostare le autorizzazioni API richieste per questa applicazione**.

   Nota: per applicare manualmente le autorizzazioni senza utilizzare il ruolo di amministratore globale/aziendale, consultare la sezione Configurazione manuale delle autorizzazioni API senza utilizzare il ruolo di amministratore globale/aziendale.

d. Fare clic su **Connetti**.

Note:

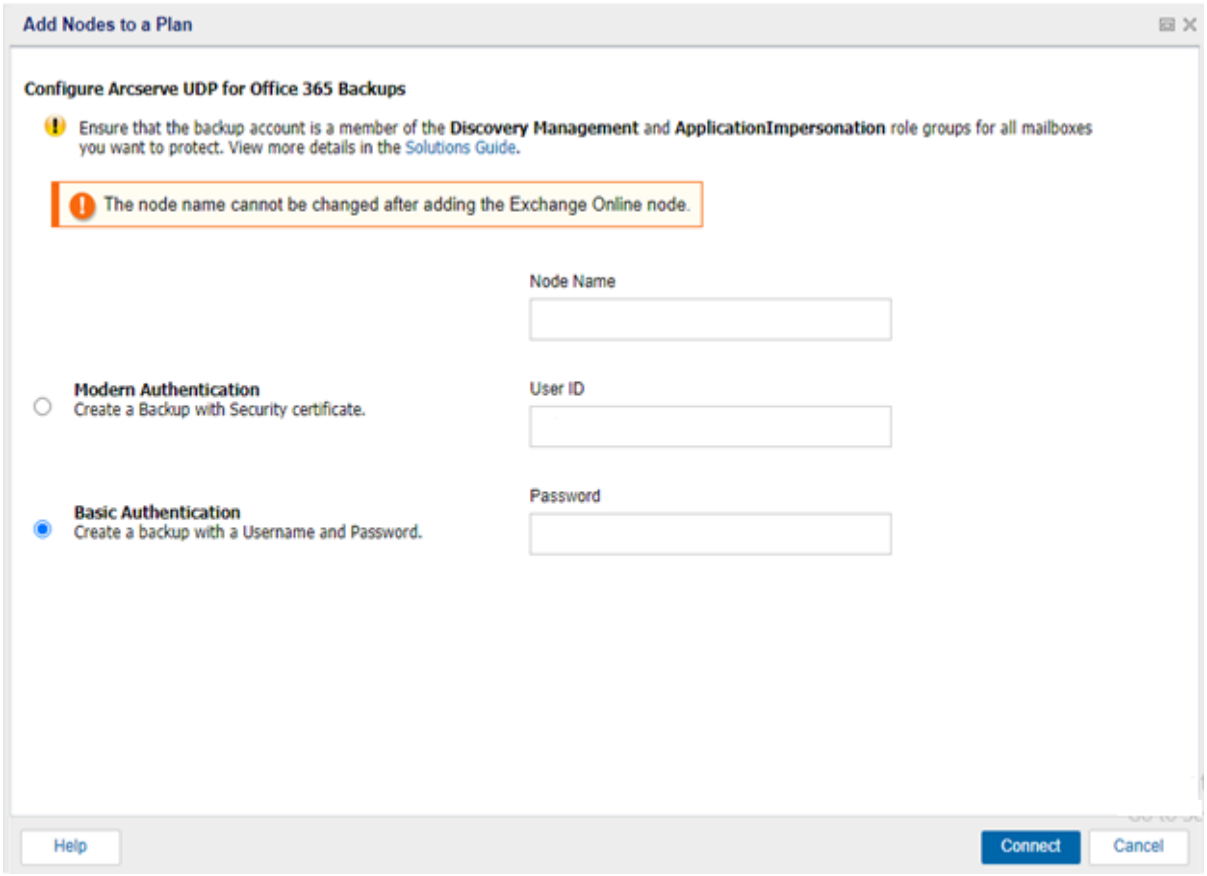
- Il nome del nodo di Exchange Online non può essere modificato dopo aver aggiunto il nodo.
- Immettere il nome utente dell'account di backup di Exchange Online in grado di soddisfare i prerequisiti nel campo **Nome utente amministratore**.
- L'autenticazione moderna non si applica nei seguenti casi:

- I clienti che utilizzano Microsoft 365 (Office 365) per le istanze Arcserve Cloud Hybrid o Arcserve Cloud Backup for Office 365, create prima del 18 ottobre 2020, non consentono l'autenticazione moderna.
- I clienti che continuano a utilizzare l'autenticazione di base.

Autenticazione di base

Per l'autenticazione di base, fornire le seguenti informazioni per procedere con il backup, quindi fare clic su **Connetti**:

- Nome nodo
- ID utente
- Password



Nota: aggiornando o modificando l'account utente, il numero di caselle di posta protette potrebbe risultare modificato. Verificare che l'account del servizio nuovo/aggiornato disponga dei diritti di impersonificazione per la protezione delle caselle di posta elettronica.

5. Per proteggere le caselle di posta di Exchange Online, eseguire una delle operazioni seguenti:

   - Per proteggere tutte le caselle di posta e i gruppi di Exchange Online, selezionare la casella di controllo **Proteggere tutte le origini di Office 365 Exchange**.

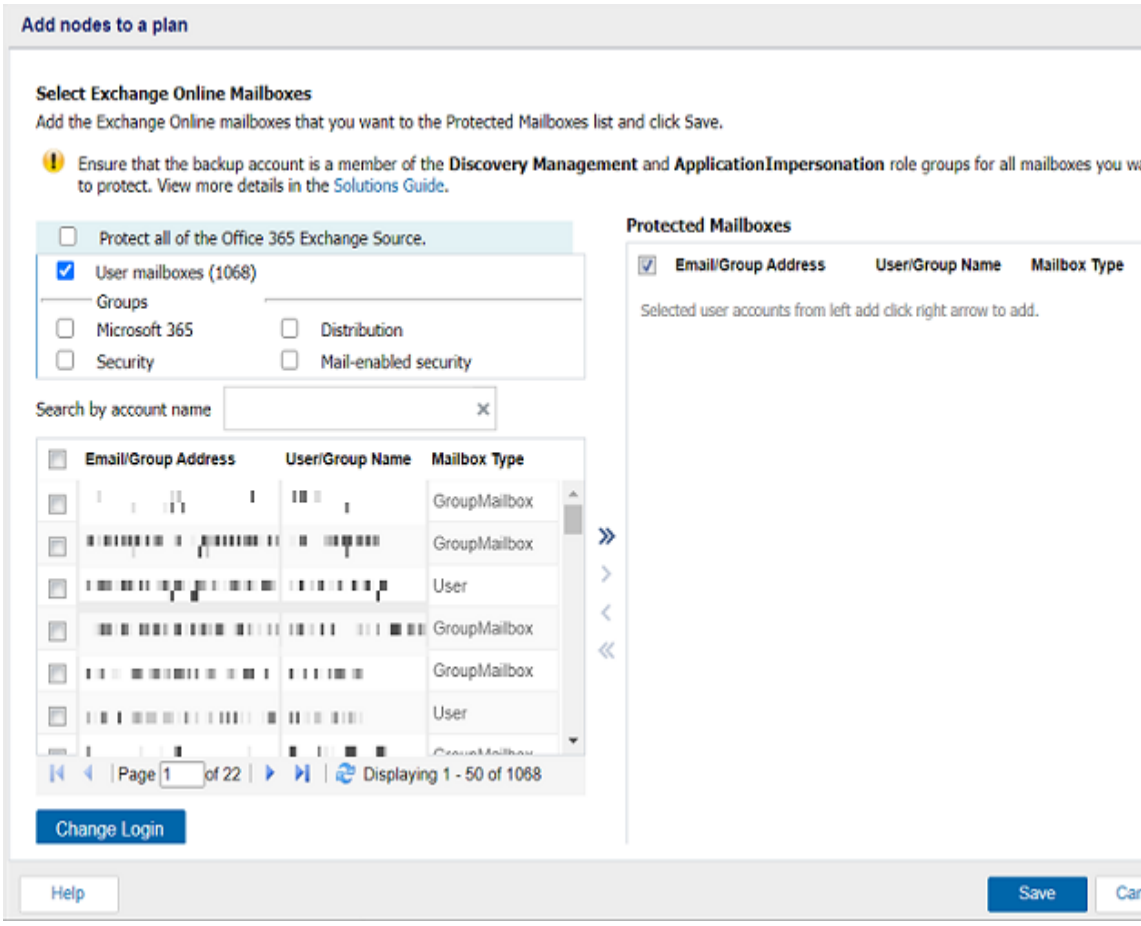
     Nota: questa opzione è selezionata automaticamente per impostazione predefinita quando viene visualizzata la schermata Seleziona caselle di posta Exchange Online.

   - Per le caselle di posta degli utenti, procedere come segue:

     a. Selezionare la casella di controllo **Caselle di posta dell'utente**.

        Viene visualizzato l'elenco delle caselle di posta dell'utente.

     b. (Facoltativo) Per cercare un account dall'elenco, nel campo Cerca per nome account, immettere il nome dell'account.



     c. Dall'elenco delle caselle di posta dell'utente, selezionare le caselle di posta che si desidera proteggere.

d. Fare clic sulla freccia destra (>) per spostare le caselle di posta selezionate nell'elenco Caselle di posta protette.

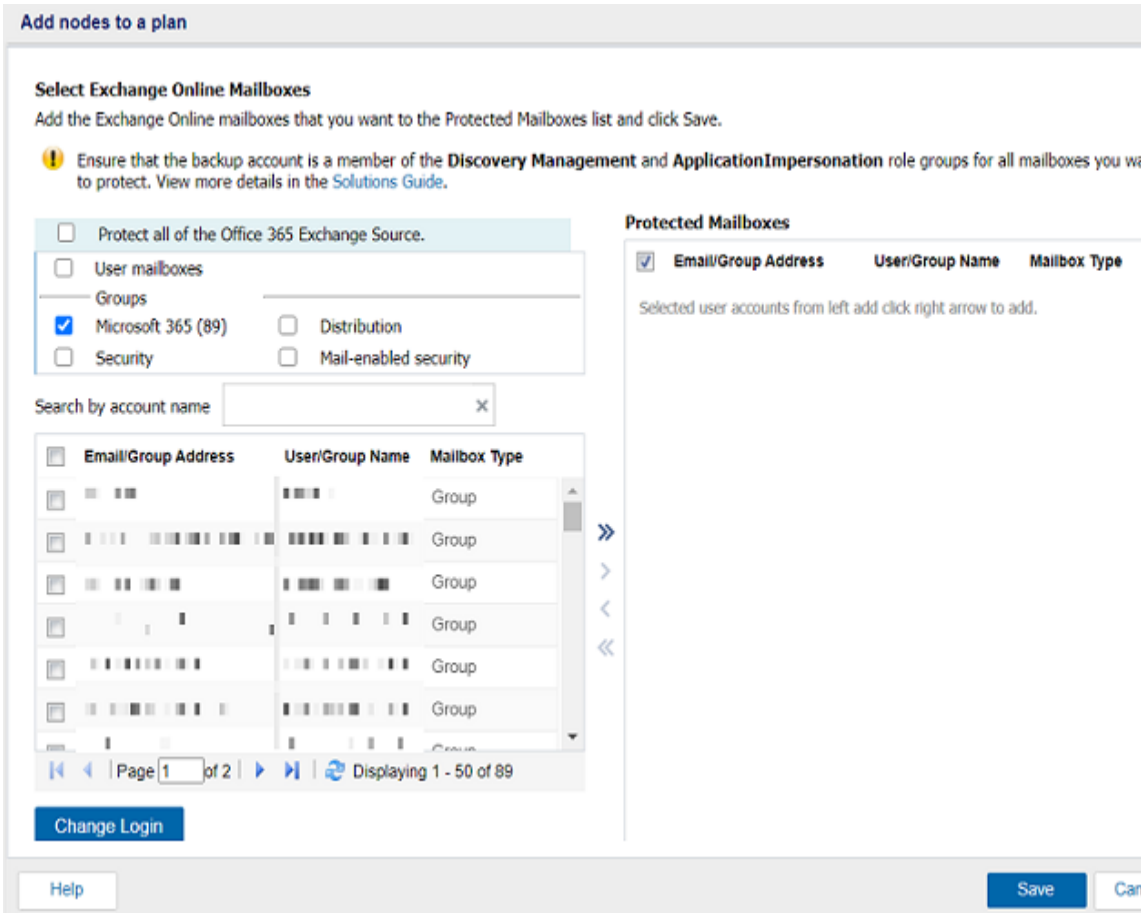
- Per i gruppi, procedere come segue:

a. Selezionare la casella di controllo **Microsoft 365**.

Viene visualizzato l'elenco dei gruppi.

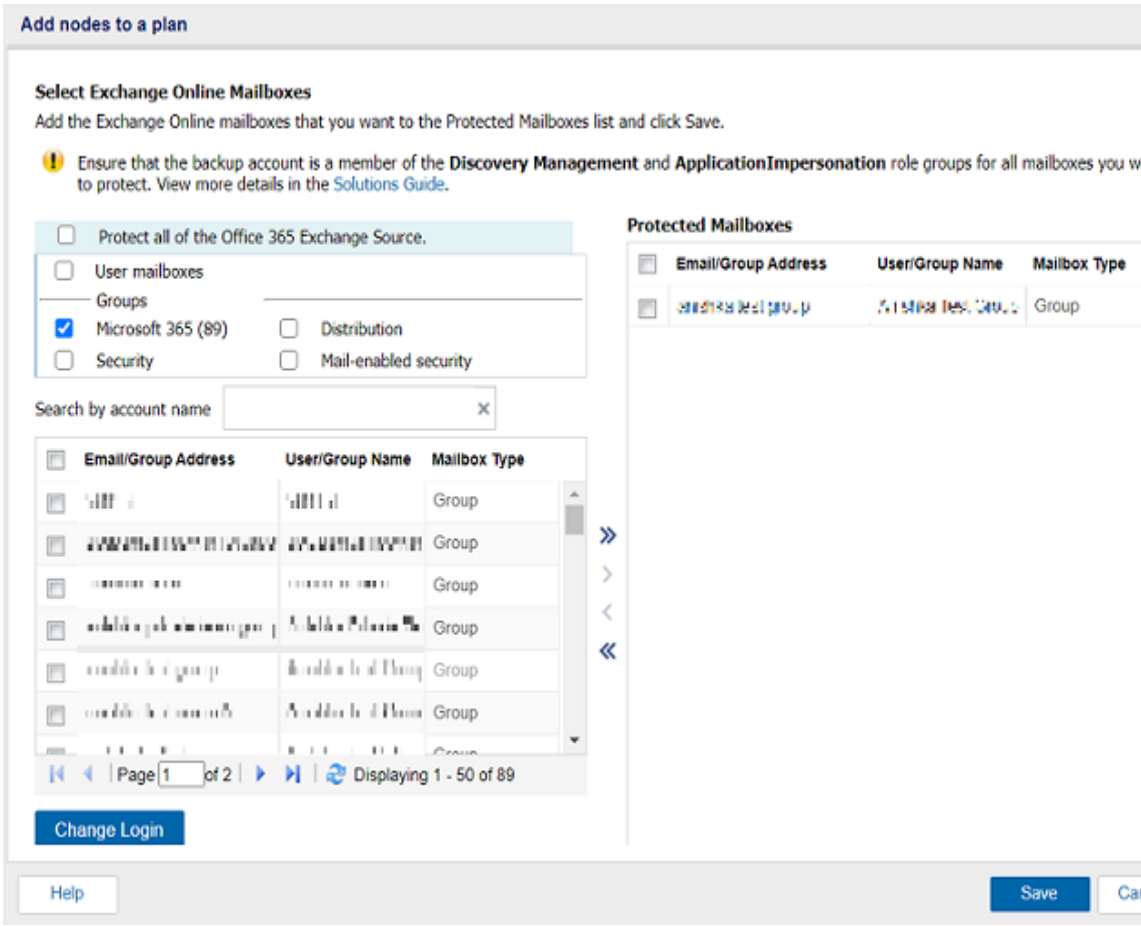
Nota: se si desidera selezionare i gruppi insieme ai gruppi secondari quali **Distribuzione**, **Protezione** o **Protezione abilitata per la posta elettronica**, selezionare la casella di controllo **Microsoft 365**, quindi la casella di controllo corrispondente al gruppo secondario.

b. (Facoltativo) Per cercare un account dall'elenco, nel campo Cerca per nome account, immettere il nome dell'account.



c. Dall'elenco dei gruppi, selezionare i gruppi che si desidera proteggere.

d. Fare clic sulla freccia destra (>) per spostare i gruppi selezionati nell'elenco Caselle di posta protette.



6. Fare clic su **Salva**.
7. Nella scheda Origini, accedere a **Cartelle da escludere dal backup**, quindi selezionare la casella di controllo desiderata.
8. Da Opzione avanzata, selezionare la casella di controllo desiderata.
   - Per consentire alla protezione di Exchange Online di supportare la casella di posta di archiviazione, selezionare la casella di controllo **Archiviazione sul posto di backup**.

     Nota: Per ulteriori informazioni sulla casella di posta di archiviazione, consultare il seguente collegamento.
   - Selezionare la casella di controllo **Backup degli elementi recuperabili** per consentire la protezione della casella di posta che attiva la funzionalità Blocco sul posto o Blocco per controversia legale.

Nota: Per l'archiviazione Blocco sul posto e Blocco per controversia legale per Exchange Online, consultare il seguente collegamento.

Nota: Per attivare entrambe le funzionalità contemporaneamente nella casella di posta per eseguire il backup degli elementi recuperabili nella casella di posta di archiviazione, selezionare entrambe le opzioni **Archiviazione sul posto di backup** e **Backup degli elementi recuperabili**.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Destinazione**.
2. Selezionare l'opzione **Arcserve UDP Recovery Point Server. Arcserve UDP Recovery Point Server** specifica che la destinazione di backup è un Recovery Point Server. Se si seleziona questa opzione, i dati vengono archiviati come punti di ripristino. Non è possibile archiviare i dati come set di ripristino.
3. Fornire i dettagli seguenti:
    a. Selezionare un Recovery Point Server.
    b. Selezionare un archivio dati di deduplicazione o di non deduplicazione. L'elenco mostra tutti gli archivi dati creati per il Recovery Point Server specificato.
    c. Fornire una password di sessione. Quando la destinazione del backup è un archivio dati RPS non crittografato, la password di sessione è facoltativa.
    d. Confermare la password di sessione.

La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

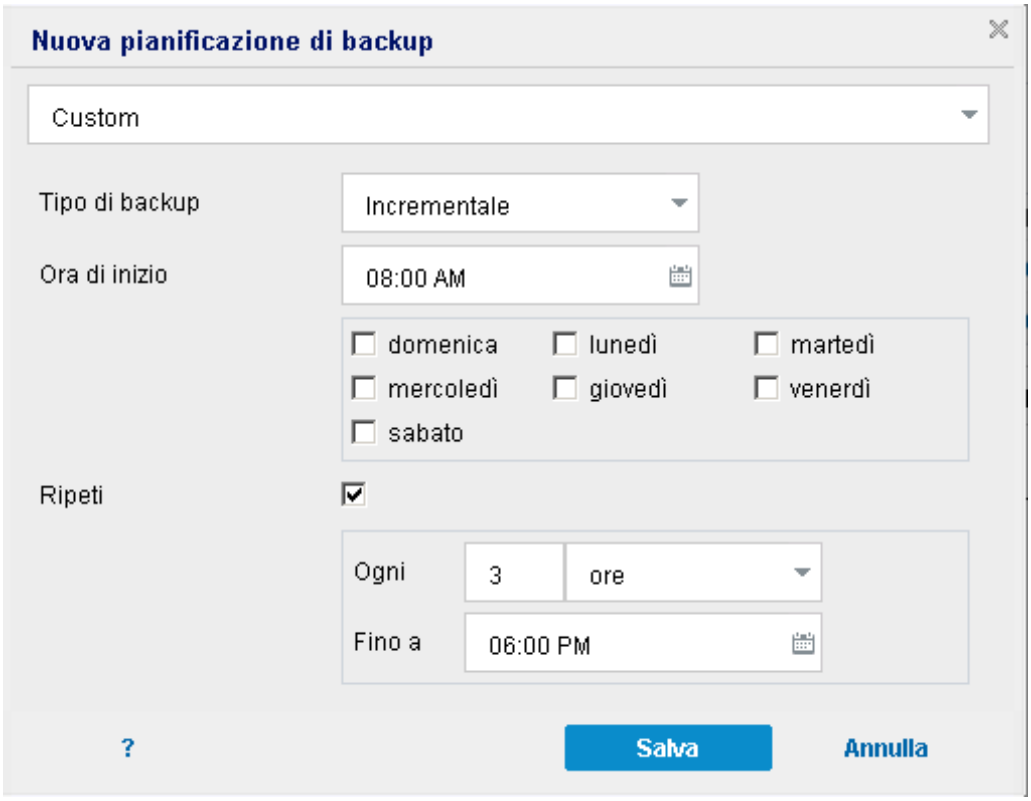
Effettuare le operazioni seguenti:

1. Aggiungere le pianificazioni di backup, di unione e di definizione del limite di velocità.

   Aggiunta di una pianificazione di backup

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni del backup.

Incrementale

Specifica la pianificazione dei backup incrementali.

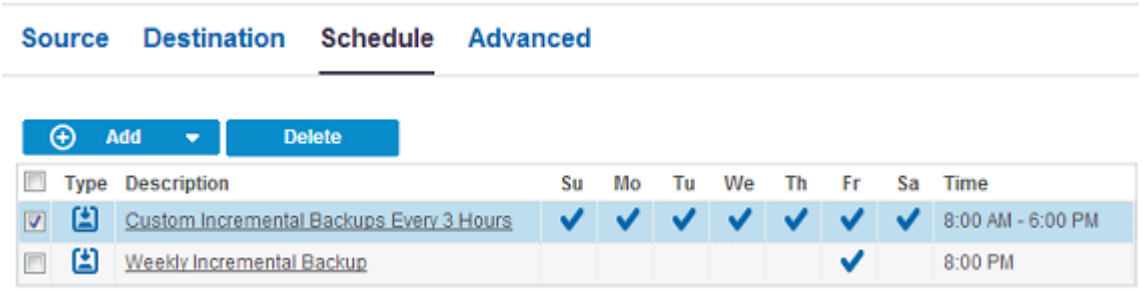
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali presentano il vantaggio di essere particolarmente rapidi e di generare immagini di backup con dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di unione**.

La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

b. Specificare l'ora di inizio per l'avvio del processo di unione.

c. Specificare **Fino a** per specificare un'ora di fine per il processo di unione.

d. Fare clic su **Salva**.

La pianificazione di unione specificata viene visualizzata nella pagina **Pianificazione**.

Aggiungi pianificazione del limite delle risorse

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

Viene visualizzata la finestra di dialogo **Aggiungi nuova pianificazione del limite delle risorse**.

b. Specificare il limite di velocità effettiva in MB per unità di minuti.

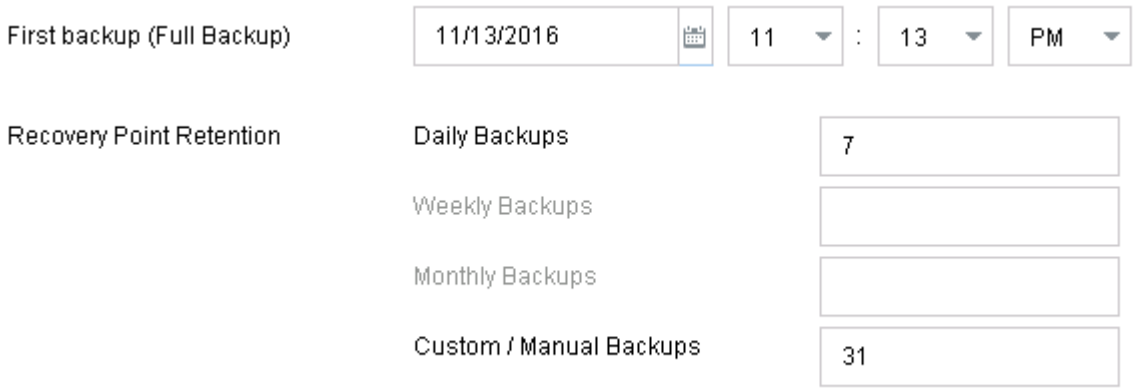
c. Specificare l'ora di inizio per l'avvio del processo del limite di velocità effettiva del backup.

d. Compilare il campo **Fino a** per specificare un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

La pianificazione del limite delle risorse specificata viene visualizzata nella pagina **Pianificazione**.

2. Specificare l'ora di inizio per il backup pianificato.



3. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo **Pianificazione di backup**.

   Viene specificata la pianificazione.

Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione

L'opzione di pianificazione consente di specificare una pianificazione personalizzata o una pianificazione giornaliera/settimanale/mensile o entrambe. Nella pianificazione personalizzata è possibile configurare la pianificazione del backup per ciascun giorno della settimana e aggiungere fino a quattro pianificazioni di backup ogni giorno. È possibile selezionare un giorno specifico di una settimana e creare un intervallo di tempo per definire quando eseguire il backup e la frequenza.

Pianificazione	Processo supportato	Commenti
Backup	Processo di backup	Definire gli intervalli di tempo per eseguire i processi di backup.
Limitazione della velocità di backup	Processo di backup	Definire gli intervalli di tempo per controllare la velocità di backup.
Unione	Processo di unione	Definire quando unire i processi.
Pianificazione quotidiana	Processo di backup	Definire quando eseguire processi di backup quotidiani.
Pianificazione settimanale	Processo di backup	Definire quando eseguire processi di backup settimanali.
Pianificazione mensile	Processo di backup	Definire quando eseguire processi di backup mensili.

È inoltre possibile specificare le impostazioni di memorizzazione per i punti di ripristino.

Nota: All'interno di ogni piano è necessario configurare le impostazioni di conservazione per controllare il modo in cui i nodi assegnati a tale piano vengono memorizzati nell'archivio dati di destinazione.

Le pianificazioni per i backup giornalieri/settimanali/mensili sono indipendenti dalla pianificazione personalizzata e gli uni dagli altri. È possibile configurare di eseguire solo il backup giornaliero, il backup settimanale o il backup mensile senza configurare la pianificazione personalizzata.

Pianificazione del processo di backup

È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del backup. Un intervallo di tempo valido è dalle 00:00 alle 23:59. Non è possibile specificare un intervallo di tempo come ad esempio dalle 18:00 alle 06:00. In tali casi, si devono specificare manualmente due intervalli di tempo diversi.

Per ogni intervallo di tempo l'ora di inizio è inclusa e l'ora di fine è esclusa. Ad esempio, si è configurato il backup incrementale da eseguire ogni ora tra le 06:00 e le 09:00 e il backup inizierà alle 06:00. Ciò significa che il backup verrà eseguito alle 06:00, alle 07:00 e 08:00, ma NON alle 09:00.

Nota: Se si desidera eseguire il processo di backup ripetutamente fino al termine della giornata, impostare la pianificazione fino alle 00:00. Ad esempio, per eseguire un processo di backup ogni 15 minuti per l'intera giornata, impostare la pianificazione dalle 00:00 alle 00:00 ogni 15 minuti.

Pianificazione del limite delle risorse di backup

La pianificazione del limite delle risorse di backup consente di controllare la velocità effettiva di backup, che a sua volta controlla l'utilizzo delle risorse (I/O del disco, CPU, larghezza di banda della rete) del server di cui si esegue il backup. Questo è utile se non si desidera influire sulle prestazioni del server durante i normali orari di ufficio. È possibile aggiungere quattro intervalli di tempo al giorno nella propria pianificazione del limite delle risorse di backup. Per ogni intervallo di tempo è possibile specificare un valore, in MB per minuto. Questo valore viene utilizzato per controllare la velocità effettiva di backup. I valori validi sono compresi tra 1 MB/minuto a 99999 MB/minuto.

Se un processo di backup si estende oltre il tempo specificato, il limite della velocità cambia in conformità all'intervallo di tempo specificato. Ad esempio, il limite delle risorse di backup definito è 500 MB/minuto dalle 08:00 alle 20:00 e 2500 MB/minuto dalle 20:00 alle 22:00. Se un processo di backup inizia alle 19:00 e viene eseguito per tre ore, dalle 19:00 alle 20:00 il limite della velocità è pari a 500 MB/minuto e dalle 20:00 alle 22:00 a 2500 MB/minuto.

Se non si definisce alcuna pianificazione del backup e della sua velocità effettiva, il backup viene eseguito il più rapidamente possibile.

Pianificazione di unione

Consente di unire i punti di ripristino in base alla pianificazione fornita.

Considerare i punti seguenti per il processo di unione:

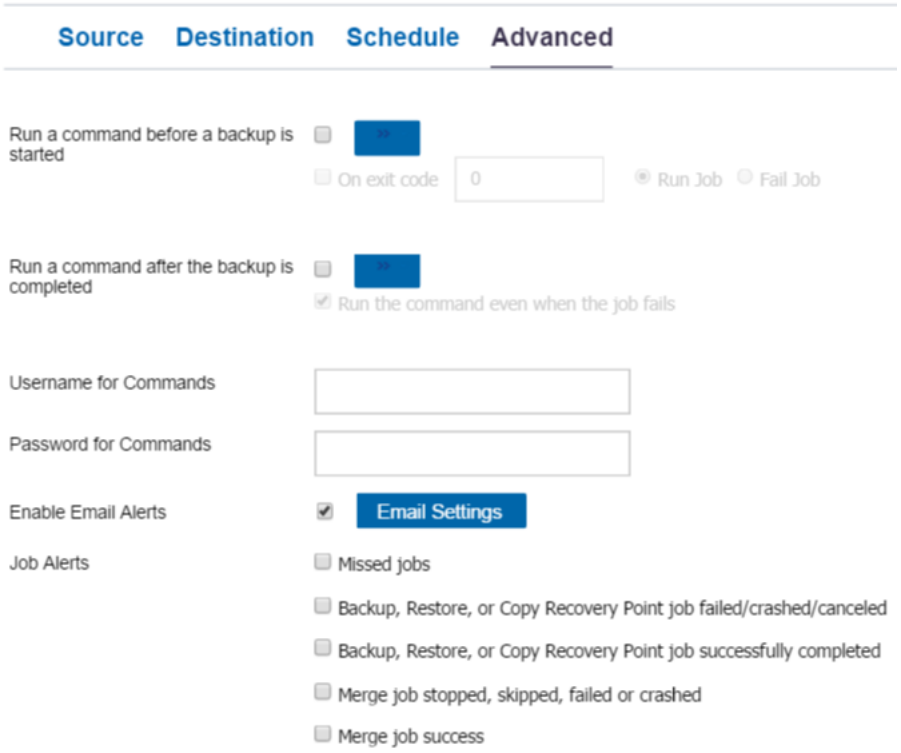
- In qualsiasi momento è possibile eseguire solo un processo di unione per un nodo.
- Se un processo di unione inizia, esso deve essere completato prima di poter avviare il processo di unione successivo. Ciò significa che se uno o più set di punti di ripristino vengono uniti, non è possibile aggiungere nuovi punti di ripristino a questo processo di unione finché il processo di unione dell'insieme corrente dei punti di ripristino non viene completato.

- Se un processo di unione sta elaborando più di un set di punti di ripristino (ad esempio set [1~4], set [5~11] e set [12~14] sono tre set distinti), il Recovery Point Server elabora tali set uno alla volta.
- Se un processo di unione viene ripreso dopo una pausa, il processo individua in quale punto era stato interrotto e riprende l'unione da tale punto.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda **Avanzate:**



Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

   Esegui un comando prima dell'avvio di un backup

   Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script all'interno del nodo proxy. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Processo con errore** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

   Esegui un comando al completamento di un backup

   Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso completo di archiviazione dello script.

   Esegui un comando anche quando il processo non riesce

Se questa casella di controllo è selezionata, lo script specificato in **Esegui comando al completamento del backup** viene eseguito anche quando il processo di backup produce un errore. In caso contrario, lo script viene eseguito solo quando il processo di backup viene completato correttamente.

Nome utente comandi

Consente di specificare il nome utente per eseguire i comandi.

Password comandi

Consente di specificare la password per eseguire i comandi.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere in un messaggio di posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy. Per ulteriori informazioni sulla configurazione delle impostazioni di posta elettronica, consultare la sezione Configurazione di posta elettronica e avvisi.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo proxy e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su **Salva.**

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo. È possibile aggiungere le attività **Copia punto di ripristino**, **Copia su nastro**, **Replica**, e **Replica da RPS remoto** come attività di completamento.

Il piano viene distribuito automaticamente sul nodo del server proxy.

Viene creato il piano di backup in linea di Exchange per il server proxy. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione**. È possibile eseguire anche un backup manuale in qualsiasi momento.

(Facoltativo) Esecuzione di un backup manuale

In genere, i backup vengono eseguiti automaticamente e vengono controllati attraverso le impostazioni di pianificazione. In aggiunta al backup pianificato, un backup manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze. Se ad esempio si dispone di una pianificazione di ripetizione per backup completi e incrementali e si desidera apportare modifiche sostanziali al computer, è necessario eseguire un backup manuale immediato senza attendere l'esecuzione del backup pianificato successivo.

Per eseguire un backup manuale dei nodi di Exchange Online, procedere come segue:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   I nodi Exchange Online vengono mostrati nel riquadro centrale.
3. Selezionare i nodi Exchange Online di cui si desidera eseguire il backup e ai quali è stato assegnato un piano (ad esempio, Mailbox@<organizationname.com>). Il nome del nodo corrisponde all'account utilizzato durante l'aggiunta del nodo Exchange Online e alla sua connessione.
4. Fare clic con il pulsante destro del mouse sul nodo, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
5. Selezionare il tipo di backup che si desidera eseguire, quindi fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.
6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.
7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Il backup manuale è stato eseguito correttamente.

Per eseguire un backup manuale di un piano Exchange Online, procedere come segue:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   I piani di backup di Exchange Online vengono visualizzati nel riquadro centrale.
3. Selezionare il piano di cui si desidera eseguire il backup e ai quali è stato assegnato un piano.

4. Fare clic con il pulsante destro del mouse sul piano, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.

5. Selezionare il tipo di backup che si desidera eseguire, quindi fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.

6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.
7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Il backup manuale è stato eseguito correttamente.

Verifica del backup

Per verificare il backup, confermare di avere creato correttamente il piano di backup. Dopo avere verificato che il piano è stato creato correttamente, confermare se il processo di backup è in esecuzione secondo quanto pianificato. È possibile verificare lo stato dei processi di backup dalla scheda **Processi**.

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Attenersi a uno dei seguenti metodi per verificare i processi di backup:

Metodo 1

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Tutti i Processi**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Metodo 2

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Processi completati correttamente**.

   L'elenco dei processi di backup completati viene visualizzato nel riquadro centrale.
3. Fare clic sul processo che si desidera verificare.

   Il riquadro destro viene aggiornato.
4. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
5. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Ripristino dei messaggi di Microsoft Teams (chat) mediante Exchange Online

È possibile ripristinare i messaggi di Microsoft Teams (chat) utilizzando Exchange Online da Microsoft Cloud utilizzando qualsiasi computer. È possibile ripristinare i dati dal punto di ripristino nella posizione originale o in una posizione alternativa.

Per eseguire il ripristino dei dati della casella di posta di Exchange Online, procedere come segue:

1. Selezione degli elementi della casella di posta di Exchange Online da ripristinare
2. Definizione delle opzioni di ripristino
3. Ripristino degli elementi recuperabili
4. Ripristino del contenuto del punto di ripristino
5. Verifica del corretto ripristino del contenuto

Selezione degli elementi di posta elettronica di Exchange Online da ripristinare

È possibile ripristinare i dati di posta elettronica di Exchange Online da un punto di ripristino. Quando si seleziona una data di ripristino e poi l'ora, vengono visualizzati tutti i punti di ripristino associati per tale durata. È possibile individuare e selezionare i contenuti di backup (applicazioni incluse) da ripristinare.

Effettuare le operazioni seguenti:

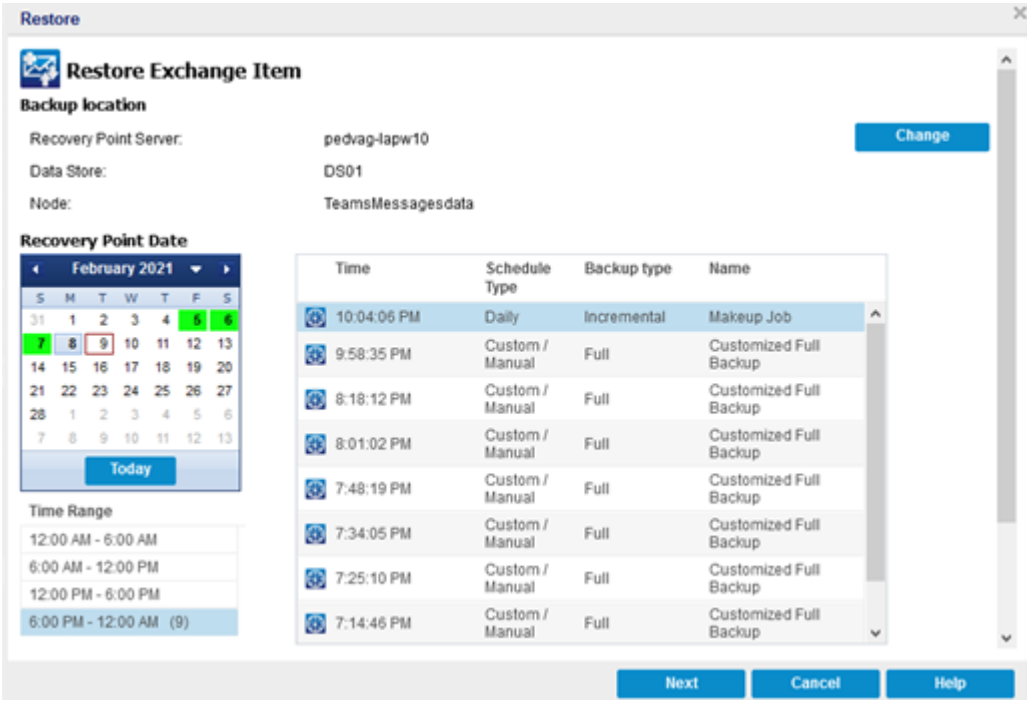
1. Accedere ad Arcserve UDP.
2. Fare clic sulla scheda **Risorse**.
3. Selezionare **Tutti i nodi** nel riquadro sinistro.

   Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.
4. Nel riquadro centrale, selezionare il nodo SharePoint Online e fare clic su **Azioni**.
5. Fare clic su **Ripristina** dall'elenco a discesa Azioni.

   Verrà visualizzata la finestra di dialogo di ripristino della posta di Exchange.

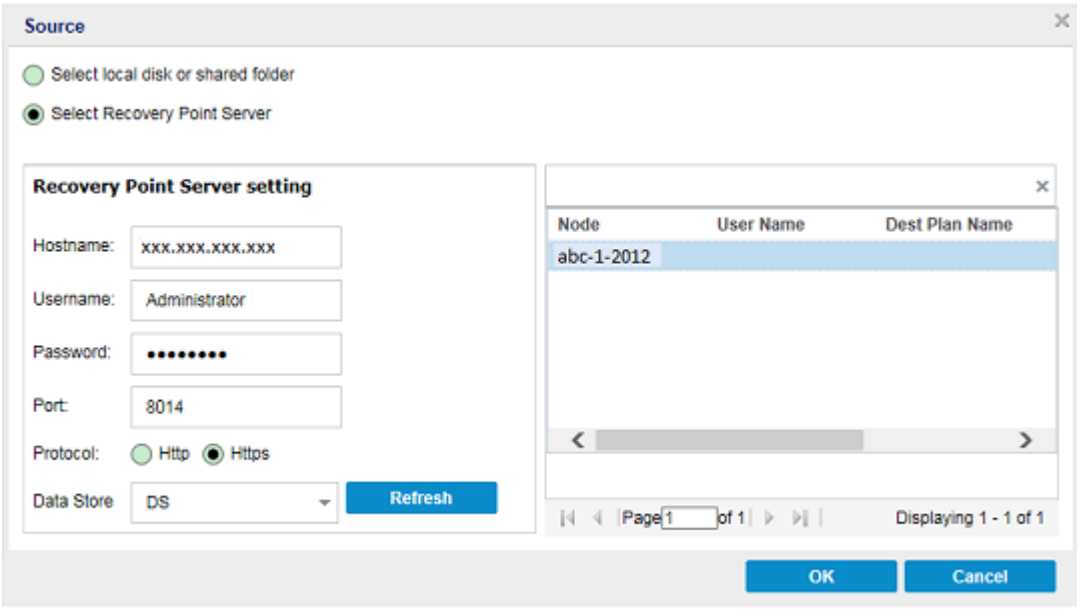
   Nota: L'utente viene connesso automaticamente al nodo dell'agente e viene aperta la finestra di dialogo **Ripristina elemento Exchange**.

   È possibile visualizzare i dettagli del Recovery Point Server in Posizione di backup.



6. (Facoltativo) Per modificare la posizione di backup, fare clic su **Modifica**.

   Viene visualizzata la finestra di dialogo Origine. È possibile selezionare la posizione di backup in questa finestra di dialogo.



   Nota: quando si aggiunge un'attività di copia su nastro al piano e si desidera ripristinare il punto di ripristino del backup di copia su nastro, selezionare il punto di ripristino dal backup di copia su nastro. Per ulteriori informazioni, consultare la sezione Ricerca del punto di ripristino di copia su nastro per il ripristino.

7. Per specificare l'origine, selezionare una delle seguenti opzioni, quindi fare clic su **OK**:

   Selezione di un disco locale o una cartella condivisa

   Nota: in Arcserve UDP, si consiglia di non selezionare l'opzione **Seleziona un disco locale o una cartella condivisa**.

   Selezione di un Recovery Point Server

   a. Specificare i dettagli dell'impostazione Recovery Point Server e fare clic su **Aggiorna**.

      Tutti gli agenti vengono elencati nella colonna Data Protection Agent (Agente di protezione dati) nella finestra di dialogo Origine.

   b. Selezionare l'agente dall'elenco visualizzato, quindi fare clic su **OK**.

      I punti di ripristino vengono elencati nella finestra di dialogo di ripristino dell'elemento di Exchange.

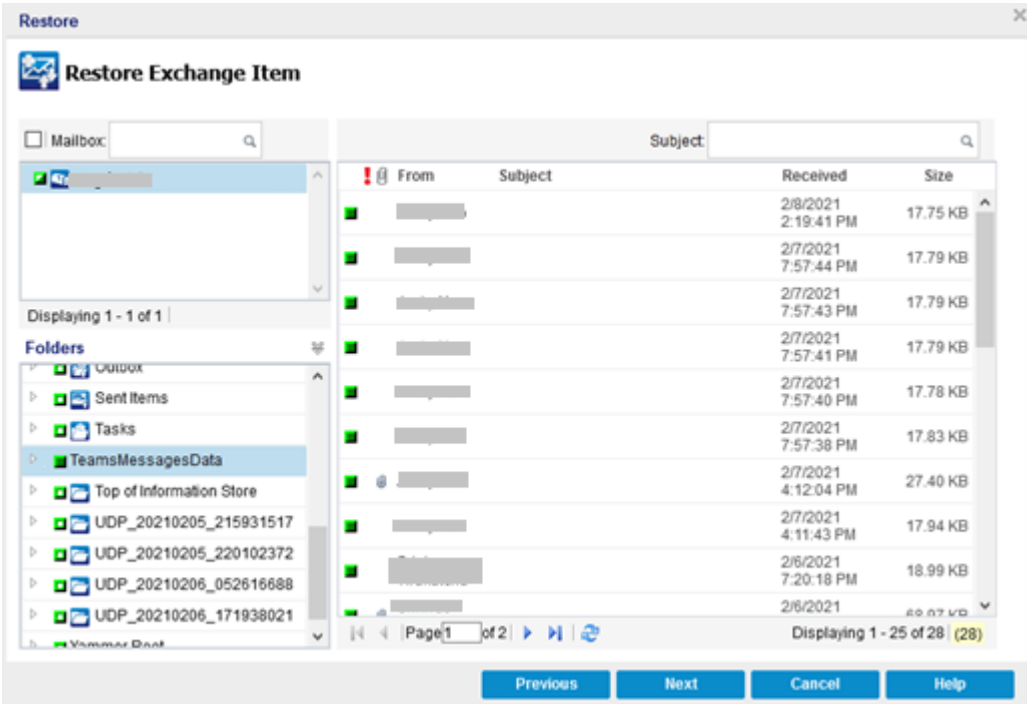
Nota: Dal punto di ripristino **Cartella**, è possibile che venga visualizzato un numero elevato di cartelle con lo stesso nome con i nodi Exchange Online. Ciò accade poiché il GUID viene modificato e la nuova cartella del punto di ripristino viene creata con l'eliminazione di un nodo e con la sua aggiunta nel piano di verifica.

8. Selezionare la data nel calendario per l'immagine di backup che si desidera ripristinare, quindi fare clic su **Avanti**.

   Tutte le date contenenti punti di ripristino per l'origine di backup specificata sono evidenziate in verde.

   Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito (completo, incrementale o di verifica) e al nome del backup.

9. Nel riquadro **Casella di posta**, fare clic sulla casella di posta che si desidera ripristinare.



   Nel riquadro Cartelle vengono visualizzati tutti i messaggi di posta corrispondenti.

10. Selezionare la cartella **TeamsMessagesData**, quindi fare clic su **Avanti**.

    Note:

    - È possibile selezionare l'intero contenuto oppure parte del contenuto dell'oggetto di Exchange da ripristinare. Per selezionare parte del contenuto, espandere l'oggetto e fare clic sulla casella di controllo del contenuto.
    - È possibile selezionare più oggetti di Exchange da ripristinare.

Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

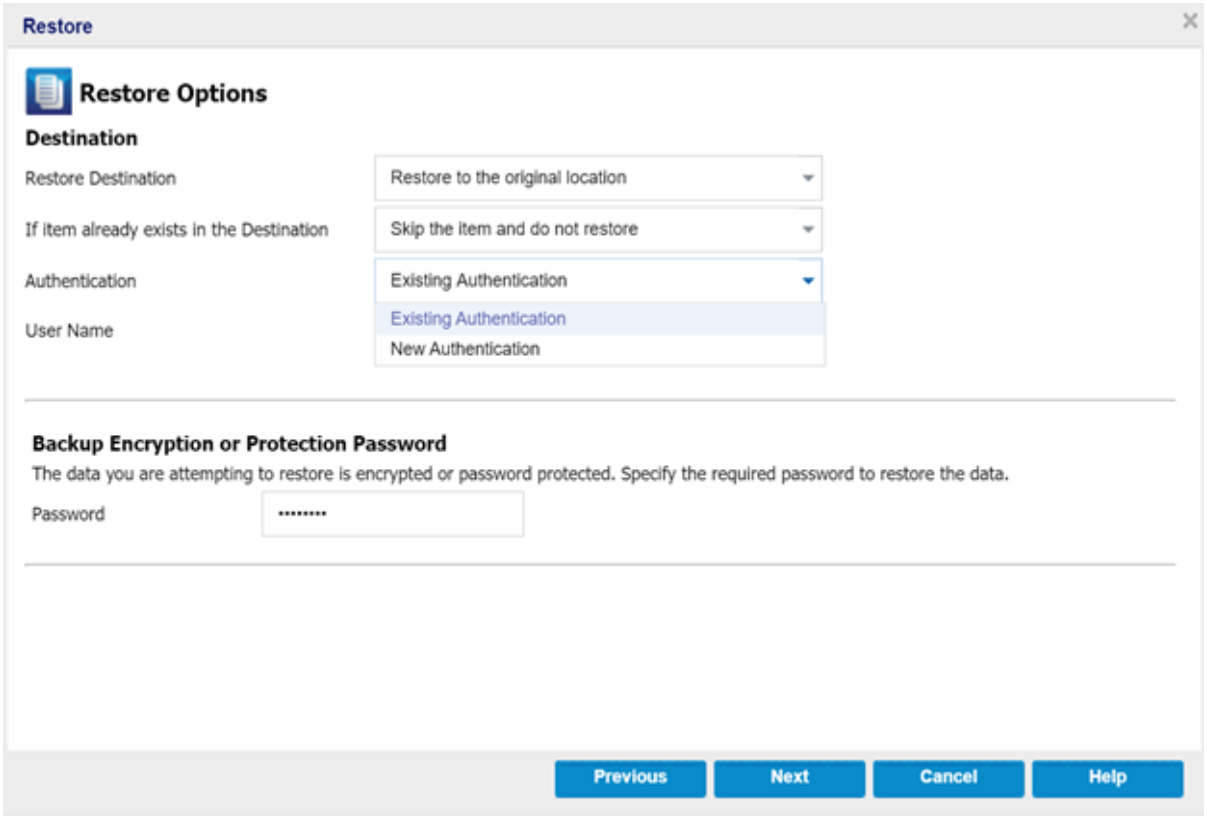
Gli elementi di posta di Exchange Online da ripristinare sono selezionati. A questo punto, è possibile definire le opzioni di ripristino.

Definizione delle opzioni di ripristino

Dopo avere specificato le informazioni di Exchange Online da ripristinare, definire le opzioni di ripristino per il contenuto selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo Opzioni di ripristino, selezionare la destinazione di ripristino.



Le opzioni di destinazione disponibili sono:

Ripristina in posizione originale

Consente di ripristinare i dati di posta elettronica nella stessa posizione da cui è stato eseguito un backup.

Note:

- Se si esegue il ripristino nella posizione originale, i dati non vengono visualizzati nei messaggi di Teams. Non si tratta di un ripristino completo nella posizione originale in quanto non è possibile eseguire il ripristino della cartella principale.

- Se si ripristina un elemento di posta nella posizione originale mediante l'opzione di sovrascrittura due volte, dopo il secondo ripristino, il primo elemento di posta ripristinato non viene sovrascritto. Di conseguenza, nella posizione originale sono presenti due elementi di posta analoghi.
- Se si ripristina un elemento di posta nella posizione originale mediante l'opzione Ignora e nella cartella originale esiste già un elemento analogo a quello ripristinato, il processo di backup risulterà incompleto.

Ripristina in posizione alternativa

Consente di ripristinare i dati di posta elettronica in un'altra casella di posta o in un'altra cartella nella casella di posta originale. Quando si seleziona questa opzione, è possibile selezionare la destinazione.

2. Specificare una delle opzioni seguenti dall'elenco a discesa **Se l'elemento esiste già nella destinazione**:

Ignora elemento e non ripristinare

Consente di ignorare gli elementi senza eseguire il ripristino.

Impostazione predefinita: Ignora elemento e non ripristinare.

Sovrascrivi elemento nella destinazione

Sovrascrive l'elemento nella destinazione.

Nota: L'elenco a discesa Se l'elemento esiste già nella destinazione è disponibile se si seleziona l'opzione **Ripristina in posizione originale** dall'elenco a discesa Ripristina destinazione.

Autenticazione

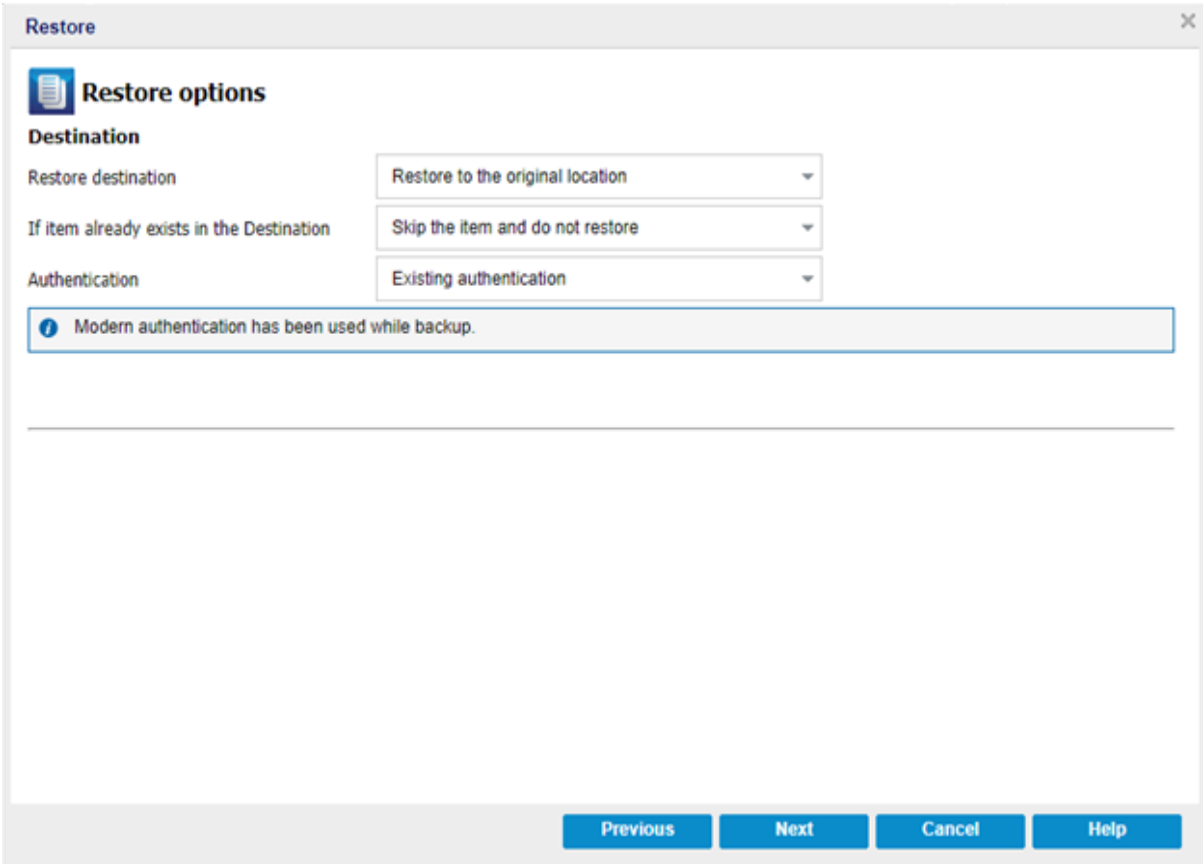
Convalida e identifica l'account utente. Selezionare una delle seguenti opzioni:

- **Autenticazione esistente**

  Quando si seleziona l'autenticazione esistente, viene utilizzato il tipo di autenticazione selezionato durante la creazione del nodo.

  - Se l'autenticazione del nodo è di base, i parametri quali Nome utente, Password e Crittografia di backup o Password di protezione [se crittografata] vengono caricati automaticamente per procedere con il ripristino.
  - Se l'autenticazione del nodo è moderna, vengono caricati automaticamente parametri quali Nome utente, Crittografia di bac-

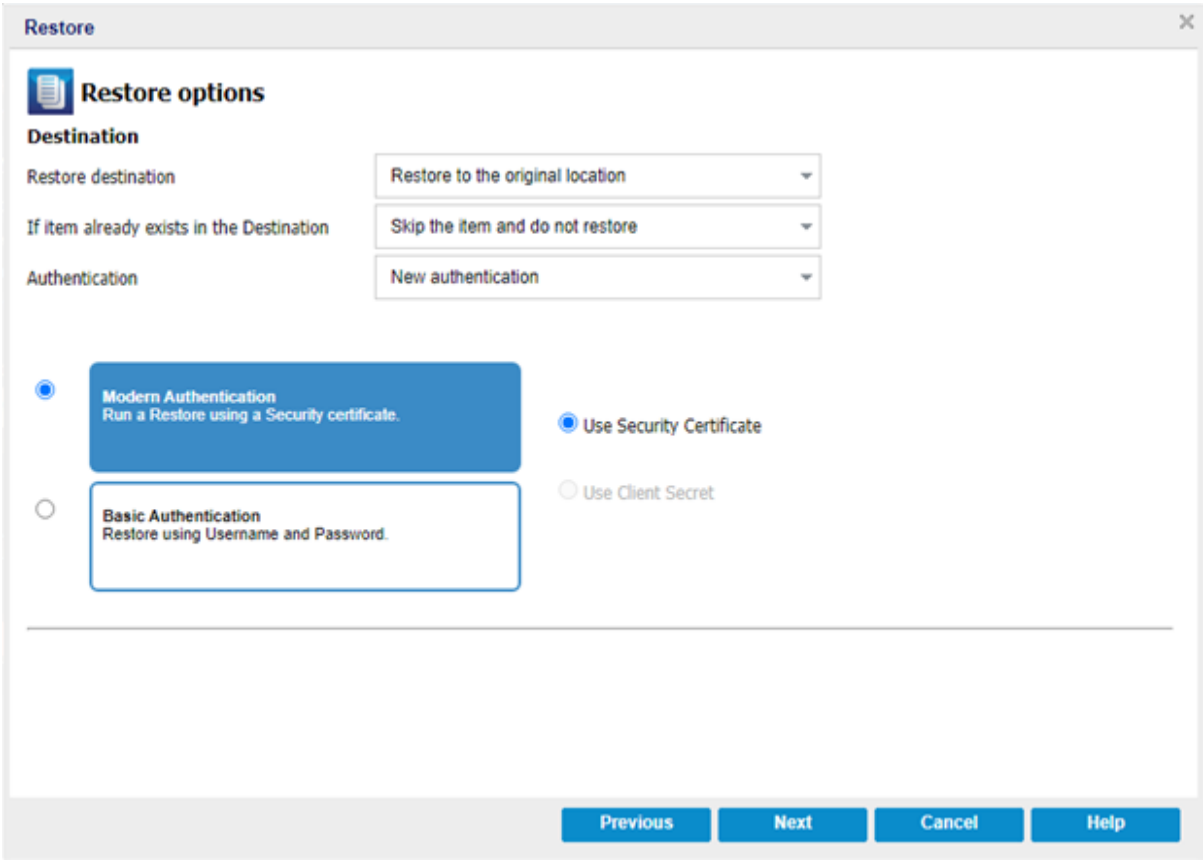
kup o Password di protezione [se crittografata] per procedere con il ripristino.



- **Nuova autenticazione**

  Durante il ripristino, è possibile selezionare una delle seguenti opzioni per modificare il tipo di autenticazione:

  - Autenticazione moderna
  - Autenticazione di base



3. Per applicare l'autenticazione, eseguire una delle seguenti operazioni:

   Autenticazione moderna

   Per l'autenticazione moderna, è possibile eseguire un ripristino utilizzando un certificato di sicurezza.

   Usa certificato di sicurezza

   Nota: per impostazione predefinita, il piano di backup seleziona l'opzione **Usa certificato di sicurezza** per l'autenticazione moderna.

   Effettuare le operazioni seguenti:

   a. Per eseguire l'autenticazione utilizzando un certificato auto-firmato, consultare la sezione Download del certificato da UDP e caricamento in Azure.

   b. Immettere l'ID applicazione e il nome utente.

   c. Per applicare i ruoli e le autorizzazioni richiesti, selezionare la casella di controllo **Consentire ad Arcserve UDP di impostare i ruoli e le autorizzazioni di Azure richiesti per questa applicazione**, quindi fare clic su **Avanti**.

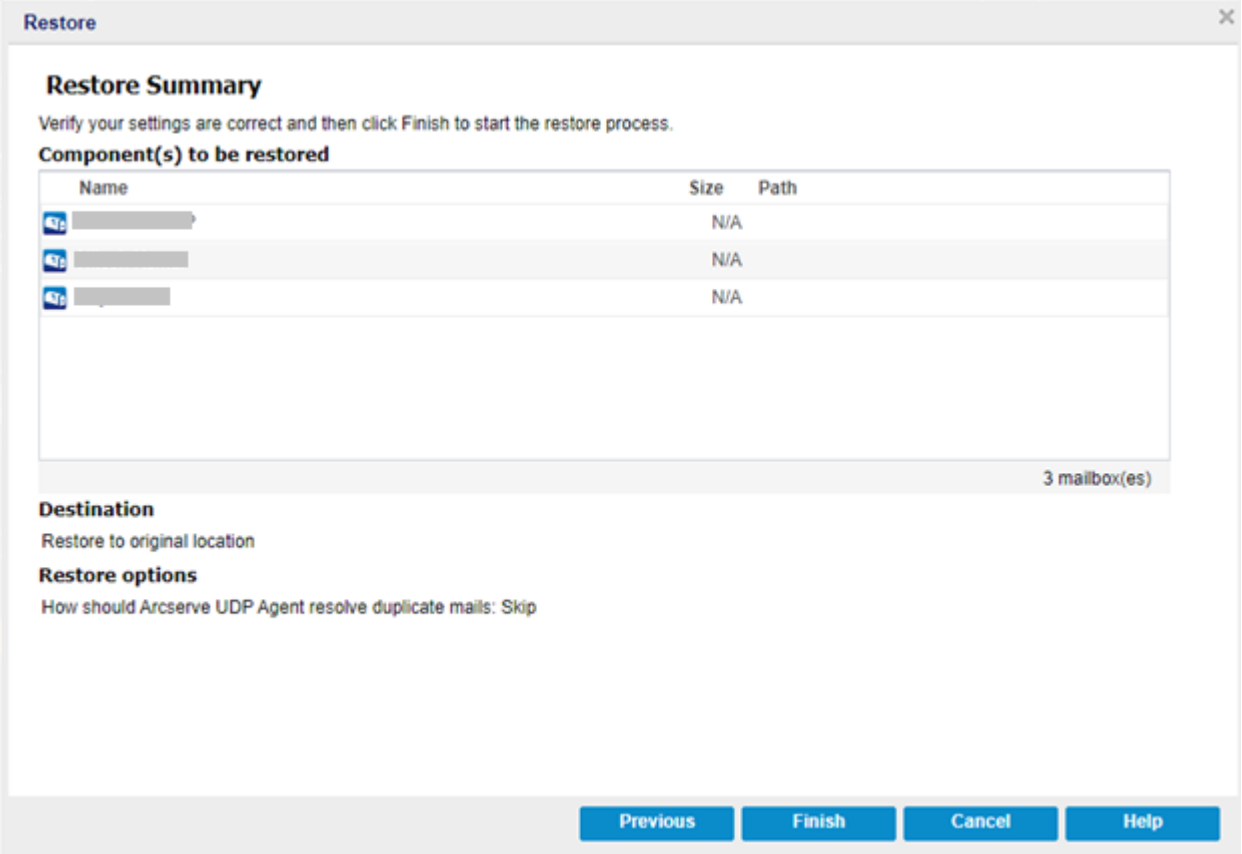
Autenticazione di base

Per l'autenticazione di base, immettere l'ID utente e la password per procedere con il ripristino.

Nota: questa opzione non riesce se l'autenticazione moderna è abilitata sul tenant o sull'account.

4. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo Riepilogo ripristino.



5. Nella finestra Riepilogo ripristino, verificare le impostazioni, quindi fare clic su **Fine**.

Le opzioni di ripristino vengono definite per ripristinare le informazioni di Exchange Online.

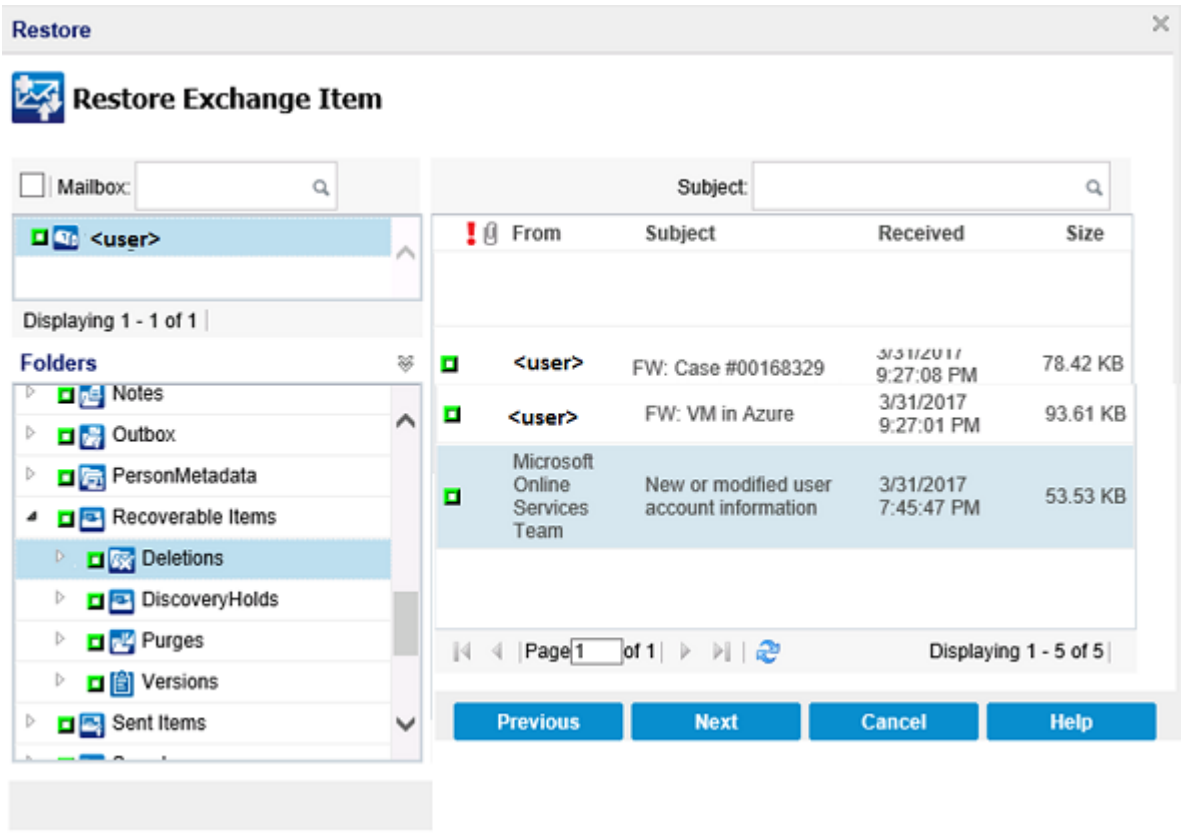
Ripristino degli elementi recuperabili

È possibile ripristinare gli elementi recuperabili dalla casella di posta che consente di utilizzare la funzionalità Blocco sul posto o Blocco per controversia legale, dall'interfaccia utente del nodo Exchange Online per individuare una sessione di backup. Per abilitare questa funzionalità, consultare la sezione Definizione dell'origine.

Dopo aver abilitato la funzionalità, mediante la procedura guidata di ripristino è possibile ripristinare gli elementi recuperabili.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo Ripristina elemento Exchange, selezionare le cartelle desiderate in **Elementi ripristinabili** e fare clic su **Avanti**.



Verrà visualizzata la finestra Opzioni di ripristino.

2. Dalla schermata Opzioni di ripristino, eseguire le seguenti operazioni e fare clic su **Avanti**:
   - Selezionare Ripristina destinazione.
   - Ignorare o sovrascrivere se l'elemento esiste già nella destinazione.

È possibile eseguire un ripristino originale o alternativo.

Ripristino originale

Gli elementi recuperabili vengono ripristinati nella cartella *UDP_RecoverableItems_yyyyMMdd_HHmmssfff* creata nella casella di posta di destinazione. Le opzioni Ignora e Sovrascrivi per il ripristino non sono applicabili a questi elementi.

Ripristino alternativo

Come in una casella di posta utente, consente di ripristinare gli elementi selezionati nel percorso di destinazione in una cartella con indicazione di data univoca, ad esempio *denominata /restore_yyyyMMdd-mmssff*.

- Fornire l'ID utente e la password della destinazione in cui si desidera eseguire il ripristino.

Gli elementi recuperabili selezionati vengono ripristinati.

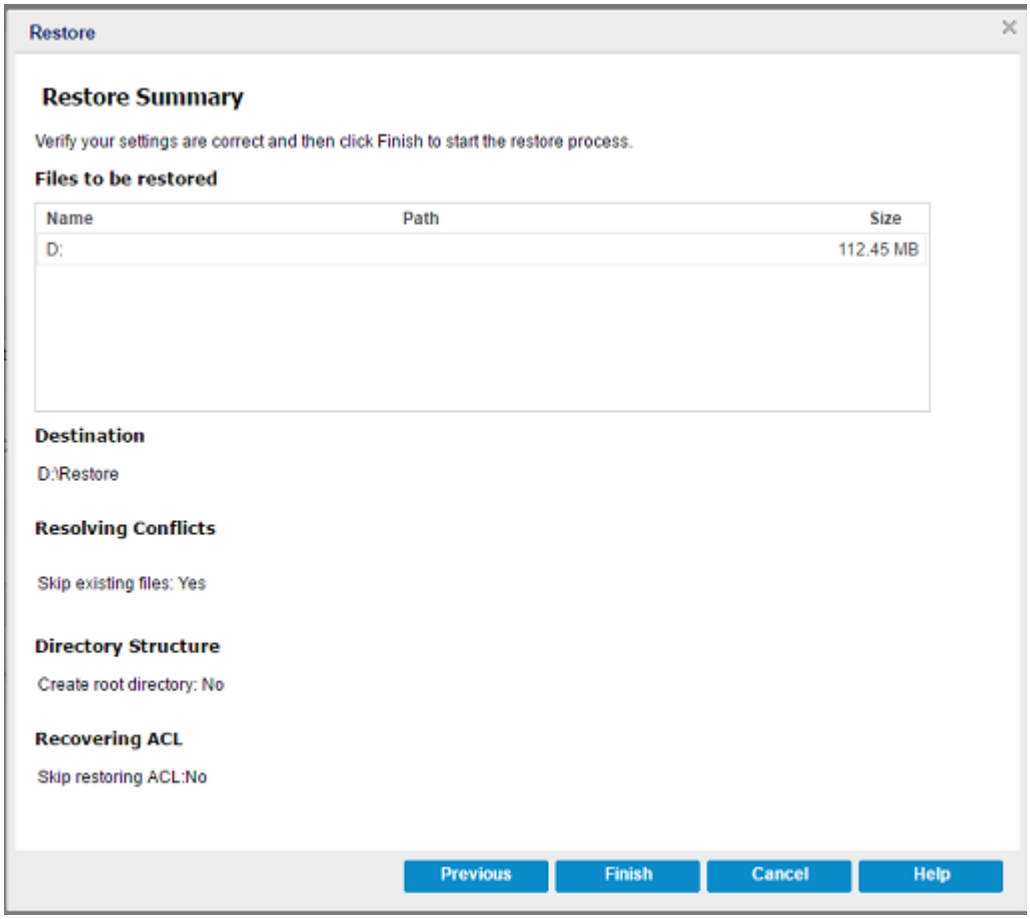
Il contenuto del punto di ripristino viene archiviato.

Ripristino del contenuto del punto di ripristino

Una volta definite le opzioni di ripristino, verificare che le impostazioni siano corrette e confermare il processo di ripristino. Il **riepilogo di ripristino** consente di verificare tutte le opzioni di ripristino definite e, se necessario, modificarle.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo Riepilogo ripristino, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



- Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
- Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

Il contenuto del punto di ripristino viene archiviato.

Verifica del corretto ripristino del contenuto

Una volta completato il processo di ripristino, verificare il ripristino del contenuto nella destinazione specificata.

Effettuare le operazioni seguenti:

1. Accedere alla casella di posta di destinazione.
2. Verificare l'elemento della casella di posta ripristinato.
3. Verificare che il contenuto sia stato ripristinato.

   Il contenuto ripristinato è stato verificato correttamente.

Esecuzione del backup e del ripristino dei file di Microsoft Teams utilizzando SharePoint Online

Ogni volta che si crea un canale privato, pubblico e di gruppo in Microsoft Teams, viene creato automaticamente un sito SharePoint Online. Questo sito SharePoint Online dispone di una cartella della raccolta documenti predefinita, in cui vengono salvati automaticamente tutti i file condivisi in tutte le conversazioni. È inoltre possibile personalizzare le autorizzazioni e le opzioni di protezione per le informazioni sensibili.

Quando si crea un gruppo in Microsoft Teams, viene creato automaticamente un sito di SharePoint Online denominato **Team - Nome_gruppo**. Tutti i file condivisi nei canali pubblici vengono salvati in questo sito.

Quando si crea un canale privato nel gruppo Microsoft Teams, viene creato un altro sito di SharePoint Online con denominato **Teams_Nome_gruppo - Nome_canale_privato** per tale canale, oltre al sito creato per il gruppo Teams.

In questa sezione vengono fornite informazioni su come eseguire il backup e il ripristino dei file di Microsoft Teams utilizzando SharePoint Online.

La presente sezione descrive i seguenti argomenti:

Esecuzione del backup dei file di Microsoft Teams utilizzando SharePoint Online

In questa sezione vengono fornite informazioni su come eseguire il backup dei file Microsoft Teams mediante SharePoint Online.

La presente sezione descrive i seguenti argomenti:

Creazione di un piano di backup di SharePoint Online

La protezione di SharePoint viene utilizzata per eseguire il backup e ripristinare il sito di Microsoft SharePoint Online e l'elemento nell'elenco. SharePoint Online è uno dei prodotti principali di Microsoft Office 365. Per proteggere il contenuto di SharePoint, è necessario creare un piano.

La presente sezione descrive i seguenti argomenti:

Verifica dei prerequisiti

Rivedere i prerequisiti seguenti prima di creare un piano di backup di SharePoint Online.

Creazione di un piano di backup di SharePoint Online:

Prerequisiti:

L'account di backup appartiene al gruppo Amministratori raccolta siti o è assegnato al ruolo di *amministratore di SharePoint*.

Per aggiungere un account al gruppo Amministratori raccolta siti, fare riferimento al seguente collegamento.

Creazione di un piano di backup di SharePoint Online mediante l'autenticazione di base (BA):

Rivedere i seguenti prerequisiti:

- Installare PowerShell versione 5.1 o versioni successive (appartenente a Windows Management Framework (WMF)) sul server proxy (computer a 64 bit).
- Installare i seguenti moduli PowerShell sul server proxy utilizzando la finestra PowerShell:
  - Per installare il modulo Azure , eseguire il comando seguente:

    Install-Module -Name AzureAD -Force
  - Per installare il modulo ExchangeOnlineManagement, eseguire il comando seguente:

    Install-Module -Name ExchangeOnlineManagement -Force

  Nota: quando si installano i moduli PowerShell utilizzando i comandi precedenti, è possibile che venga installata una versione più recente dei moduli in base alla versione GA del componente disponibile nel repository Microsoft.

Creazione di un piano di backup di SharePoint Online mediante l'autenticazione moderna (MA):

Verificare i prerequisiti prima di creare un piano utilizzando l'autenticazione moderna.

Creazione di un piano di backup di SharePoint Online

Un piano di backup include un'attività **Backup: Office 365 SharePoint Online** che esegue un backup degli elementi di SharePoint Online (elenchi, librerie, documenti e così via) e archivia i dati in un archivio dati di deduplicazione o di non deduplicazione. Inoltre, questo piano di backup consente a UDP di rilevare e specificare gli elementi di SharePoint Online per i quali viene eseguita un'attività di backup. Ciascuna attività consiste di parametri che definiscono l'origine, la destinazione, la pianificazione, e altri dettagli di backup.

Effettuare le operazioni seguenti:

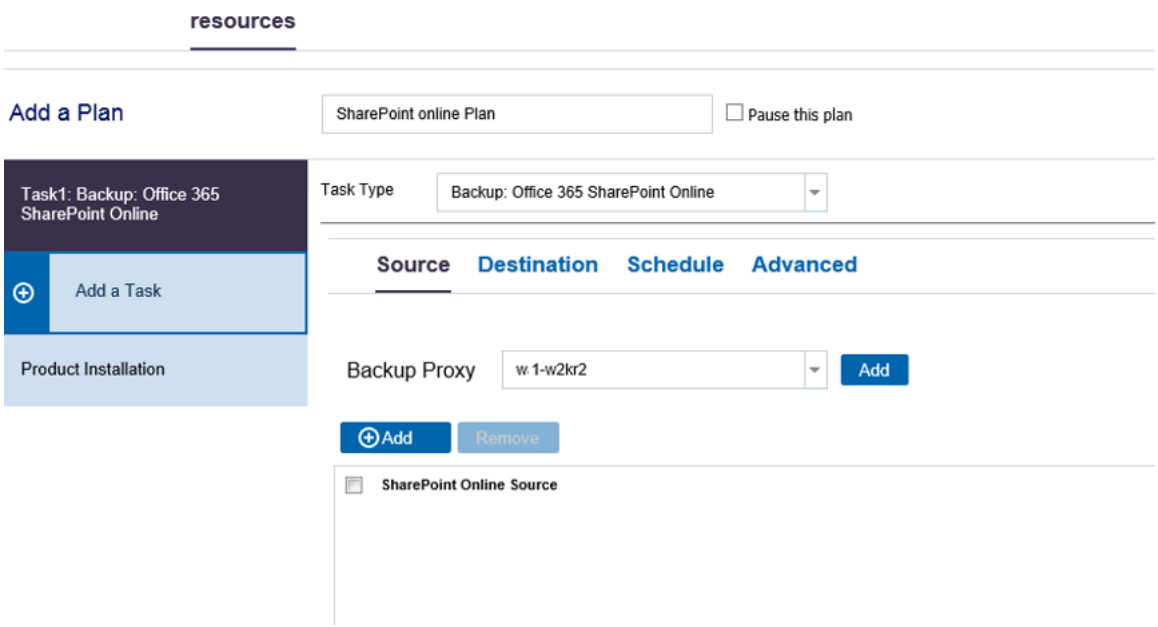
1. Fare clic sulla scheda **Risorse** della console.
2. Dal riquadro sinistro, accedere a **Piani**, quindi fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina Aggiungi un piano.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa Tipo di attività, selezionare **Backup: SharePoint Online Office 365**.



Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine di SharePoint Online che si desidera proteggere. È possibile selezionare più di un nodo di origine di SharePoint Online per un piano.

Nota: è possibile salvare un piano senza aggiungere nodi di origine. Il piano non verrà comunque distribuito a meno che vengano aggiunti altri nodi.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Origine**.
2. Selezionare **Proxy di backup** dall'elenco a discesa.
3. Aggiungere il nodo SharePoint Online utilizzando uno dei seguenti metodi:

   Metodo 1:

   a. Fare clic su **Aggiungi**, quindi su **Seleziona origine da proteggere in Arcserve UDP**.

      Viene visualizzata la finestra di dialogo Aggiungi nodi al piano.

      Nota: selezionare questa opzione solo se è già stato aggiunto il nodo SharePoint.

   b. Selezionare un nodo e fare clic su **Connetti**.

      Nota: Per individuare i nodi SharePoint Online che si desidera proteggere, utilizzare **Cerca**.

   Metodo 2:

   - Fare clic su **Aggiungi**, quindi selezionare **Aggiungi origine SharePoint Online**.

     Viene visualizzata la finestra di dialogo Aggiungi nodi a un piano.

     Nota:

     - Utilizzare questa opzione per rilevare e specificare gli elementi in linea per l'origine SharePoint Online.
     - A differenza di altri nodi, non è possibile aggiungere il nodo SharePoint Online dalla pagina Tutti i nodi. Durante la creazione o modifica di un piano, è possibile aggiungere un nodo SharePoint Online soltanto in un piano.
4. Per applicare l'autenticazione, eseguire una delle seguenti operazioni:

Autenticazione moderna

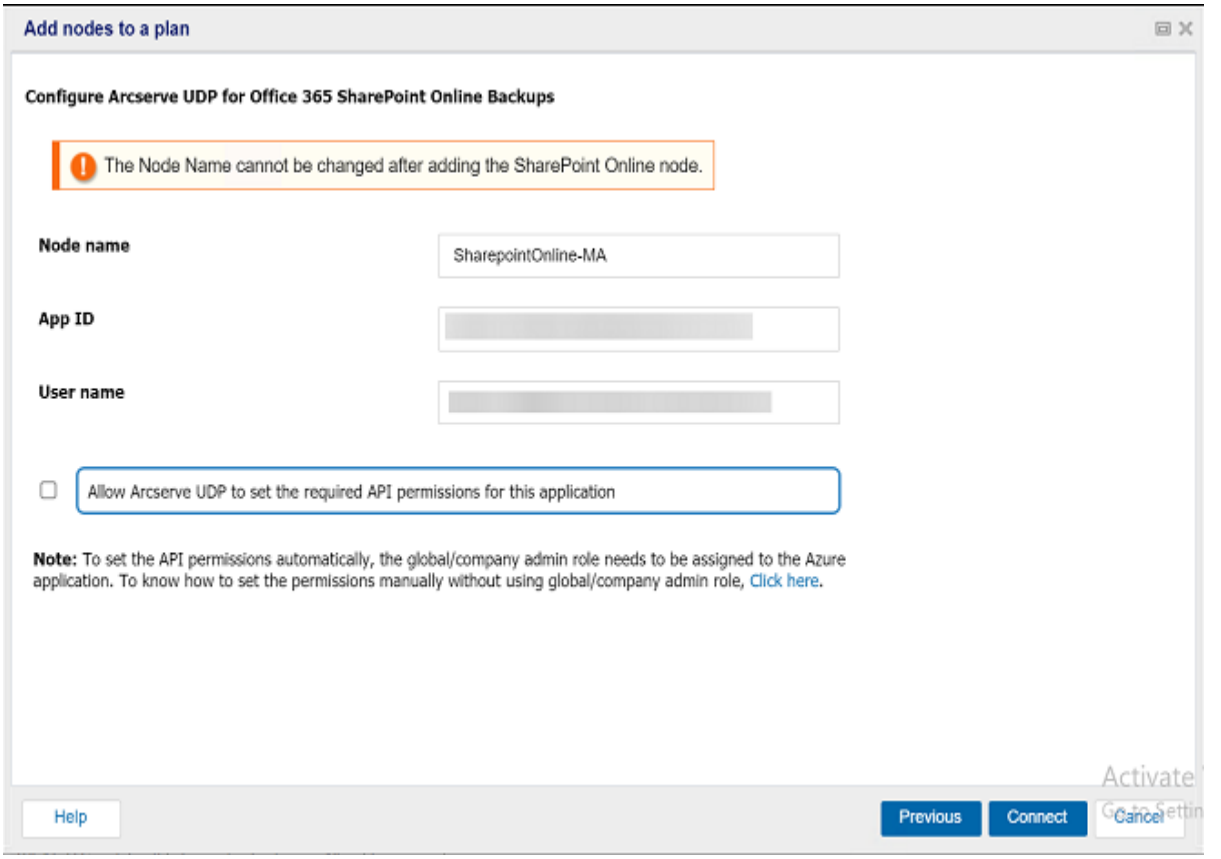
Per l'autenticazione moderna, è possibile eseguire un backup utilizzando il certificato di sicurezza.

Usa certificato di sicurezza

Nota: per impostazione predefinita, il piano di backup seleziona l'opzione **Usa certificato di sicurezza** per l'autenticazione moderna.

Effettuare le operazioni seguenti:

1. Per eseguire l'autenticazione dell'applicazione UDP con i certificati di protezione, consultare la sezione Download del certificato da UDP e caricamento in Azure.
2. Immettere le seguenti informazioni:
   - Nome nodo
   - ID app
   - Nome utente



c. Per applicare automaticamente le autorizzazioni API, selezionare la casella di controllo **Consenti ad Arcserve UDP di impostare le autorizzazioni API richieste per questa applicazione**.

Nota: per applicare manualmente le autorizzazioni senza utilizzare il ruolo di amministratore globale/aziendale, consultare la sezione Configurazione manuale delle autorizzazioni API senza utilizzare il ruolo di amministratore globale/aziendale.

d. Fare clic su **Connetti**.

Note:

- Il nome del nodo di origine di SharePoint Online non può essere modificato dopo la creazione del nodo.
- È possibile utilizzare un singolo account per proteggere più nodi SharePoint Online.
- Immettere la password dell'applicazione se l'autenticazione a più fattori è abilitata e il tenant è impostato per utilizzare l'autenticazione di base.

Autenticazione di base

Per l'autenticazione di base, fornire le seguenti informazioni per procedere con il backup, quindi fare clic su **Connetti**:

- Nome nodo
- URL di raccolta siti
- ID utente
- Password

5. Per proteggere gli elementi SharePoint Online, procedere come segue:
   - Dall'elenco a discesa Tipo di sito, selezionare il tipo di sito che si desidera proteggere, ad esempio i siti SharePoint o i siti personali.
   - Per proteggere tutti i siti/siti secondari, procedere come segue:

     Note:

     - questa opzione è selezionata automaticamente per impostazione predefinita quando viene visualizzata la schermata Seleziona contenuto SharePoint Online.
       - Per proteggere tutti gli elementi nel tipo di sito selezionato, selezionare la casella di controllo **Proteggi tutti i**

siti/siti secondari.

- Per proteggere elementi specifici nel tipo di sito selezionato, deselezionare la casella di controllo **Proteggi tutti i siti/siti secondari**, quindi selezionare gli elementi specifici che si desidera proteggere.

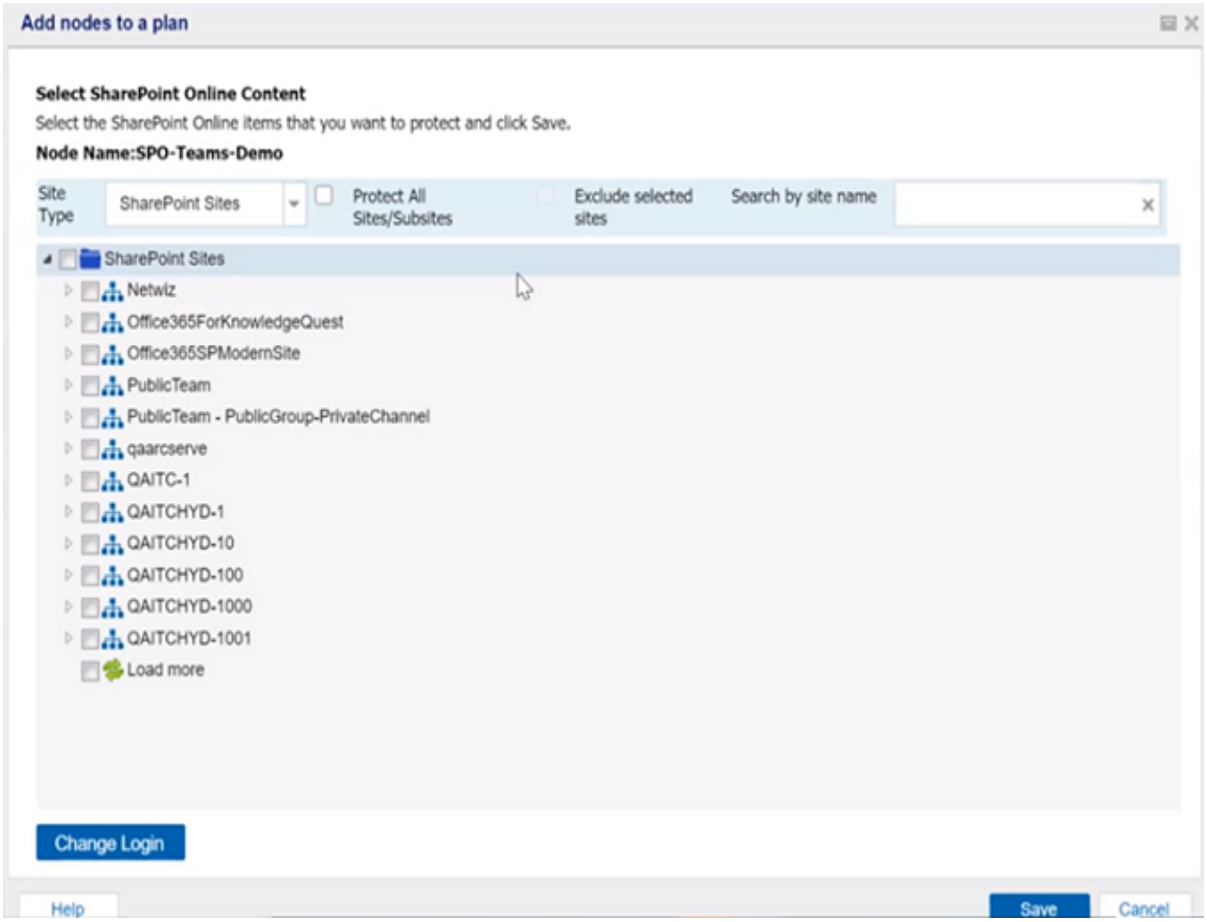
- Durante la configurazione del piano SharePoint Online esistente, se sono stati selezionati manualmente i siti per la protezione e si desidera selezionare la casella di controllo **Proteggi tutti i siti/siti secondari**, procedere come segue:

  a. Modificare il piano SharePoint Online esistente.

  b. Deselezionare i siti SharePoint selezionati manualmente per la protezione.

  c. Selezionare la casella di controllo **Proteggi tutti i siti/siti secondari**, quindi salvare il piano.

- Per escludere elementi specifici dalla protezione, selezionare la casella di controllo **Escludi siti selezionati**, quindi selezionare gli elementi specifici nel tipo di sito selezionato.



6. Fare clic su **Salva**.

   Le origini di SharePoint Online che si desidera proteggere vengono aggiunte al piano.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Destinazione**.

   L'opzione Arcserve UDP Recovery Point Server specifica che la destinazione di backup è un Recovery Point Server.

   Non è possibile archiviare i dati come set di ripristino.

2. Procedere come segue:

   a. Selezionare un Recovery Point Server.

   b. Selezionare un archivio dati di deduplicazione o di non deduplicazione.

      L'elenco mostra tutti gli archivi dati creati per il Recovery Point Server specificato.

   c. Fornire una password di sessione.

      Quando la destinazione del backup è un archivio dati RPS non crittografato, la password di sessione è facoltativa.

   d. Confermare la password di sessione.

   La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito la pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Nota: per ulteriori informazioni sulle impostazioni di pianificazione e memorizzazione, consultare la sezione Nozioni fondamentali sulla pianificazione anticipata e la memorizzazione.

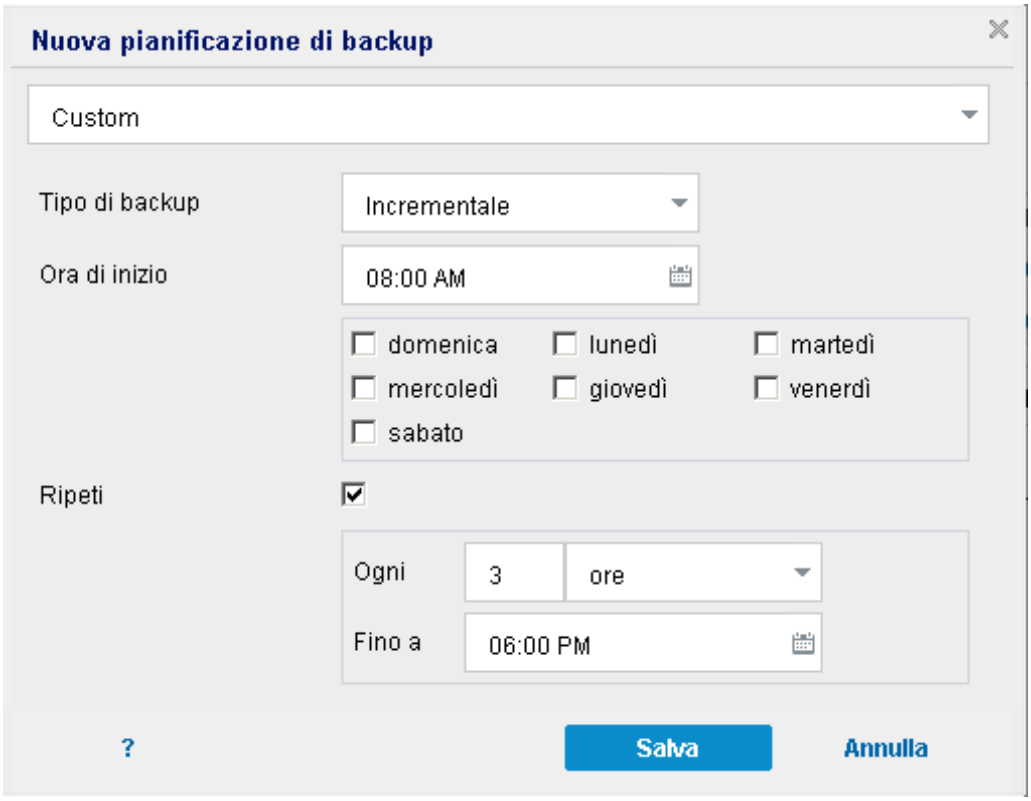
Effettuare le operazioni seguenti:

1. Aggiungere le pianificazioni di backup, di unione e di definizione del limite di velocità.

   Aggiunta di una pianificazione di backup

   a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo **Nuova pianificazione di backup**.



b. Selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

c. Selezionare il Tipo di backup.

Completo

Specifica la pianificazione dei backup completi. Arcserve UDP esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base alla pianificazione specificata. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni del backup.

Incrementale

Specifica la pianificazione dei backup incrementali.

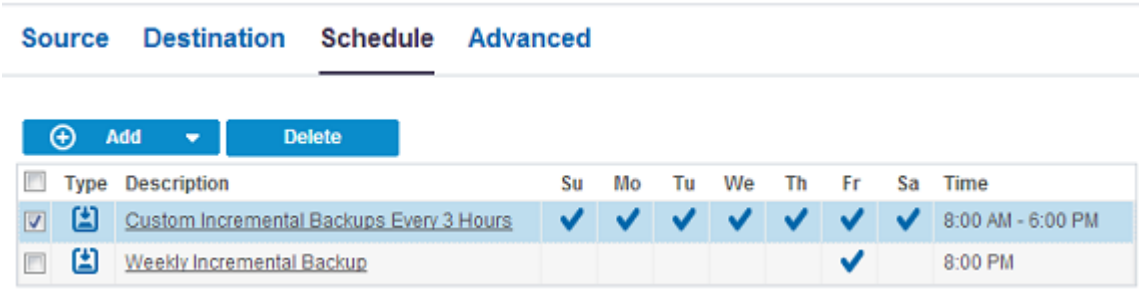
Arcserve UDP esegue il backup incrementale dei blocchi modificati dopo l'ultimo backup, in base alla pianificazione specificata. I backup incrementali presentano il vantaggio di essere particolarmente rapidi e di generare immagini di backup con dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

d. Specificare l'ora di inizio del backup.

e. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina **Pianificazione**.



Aggiunta di una pianificazione di unione

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione di unione**.

La finestra di dialogo **Aggiungi nuova pianificazione di unione** viene chiusa.

b. Specificare l'ora di inizio per il processo di unione.

c. Specificare **Fino a** per fornire un'ora di fine per il processo di unione.

d. Fare clic su **Salva**.

La pianificazione di unione specificata viene visualizzata nella pagina **Pianificazione**.

Aggiungi pianificazione del limite delle risorse

a. Fare clic su **Aggiungi** e selezionare **Aggiungi pianificazione del limite delle risorse**.

Viene visualizzata la finestra di dialogo **Aggiungi nuova pianificazione del limite delle risorse**.

b. Specificare il limite di velocità effettiva in MB per unità di minuti.

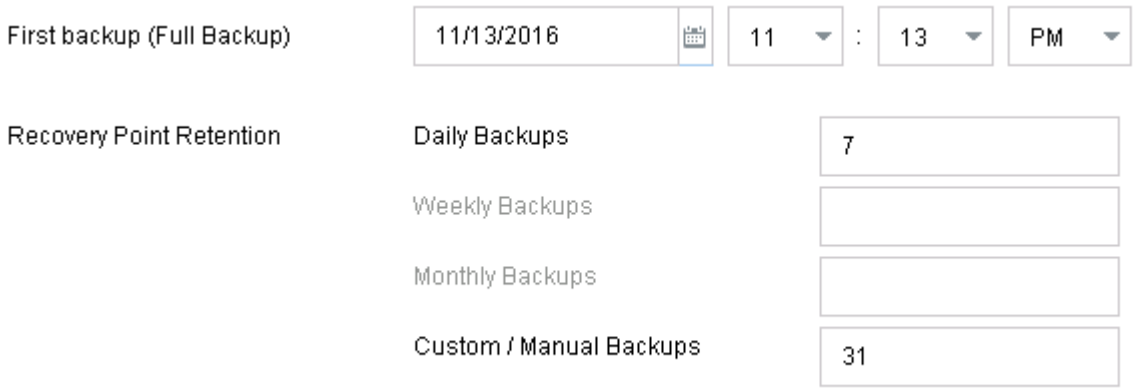
c. Specificare l'ora di inizio per il processo del limite di velocità effettiva del backup.

d. Specificare **Fino a** per fornire un'ora di fine per il processo del limite di velocità effettiva.

e. Fare clic su **Salva**.

La pianificazione del limite delle risorse specificata viene visualizzata nella pagina **Pianificazione**.

2. Specificare l'ora di inizio per il backup pianificato.



3. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

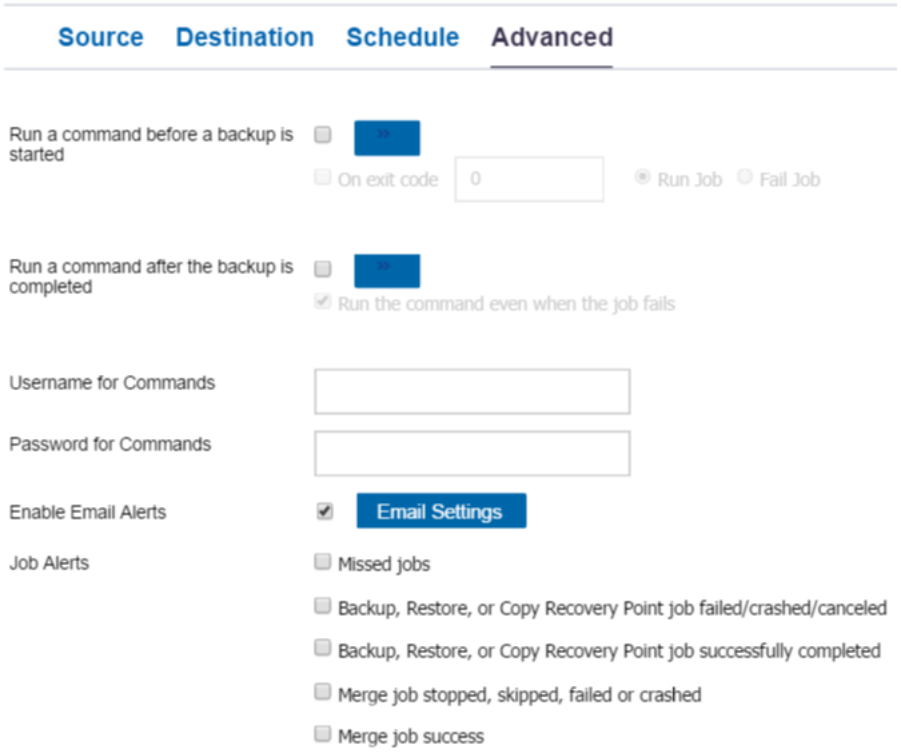
   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo **Pianificazione di backup**.

   Viene specificata la pianificazione.

Definizione delle impostazioni avanzate

La scheda **Avanzate** consente di specificare alcune impostazioni avanzate per il processo di backup. Le impostazioni avanzate includono l'indicazione dei percorsi relativi agli script e le impostazioni di posta elettronica.

La seguente immagine mostra la scheda **Avanzate:**



Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

Esegui un comando prima dell'avvio di un backup

Consente di eseguire uno script prima dell'avvio del processo di backup. Specificare il percorso di archiviazione dello script all'interno del nodo proxy. Fare clic su **Sul codice di uscita** e specificare il codice di uscita per **Esegui processo** o **Interrompi processo**. **Processo con errore** indica che il processo di backup continua quando lo script restituisce il codice di uscita. **Interrompi processo** indica che il processo di backup si interrompe quando lo script restituisce il codice di uscita.

Esegui un comando al completamento di un backup

Consente di eseguire uno script al completamento del processo di backup. Specificare il percorso completo di archiviazione dello script.

Esegui un comando anche quando il processo non riesce

Se questa casella di controllo è selezionata, lo script specificato in **Esegui comando al completamento del backup** viene eseguito anche quando il processo di backup produce un errore. In caso contrario, lo script viene eseguito solo quando il processo di backup viene completato correttamente.

Nome utente comandi

Consente di specificare il nome utente per eseguire i comandi.

Password comandi

Consente di specificare la password per eseguire i comandi.

Abilitazione degli avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere in un messaggio di posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica. Fare clic su **Impostazioni di posta elettronica** e configurare i dettagli del server di posta elettronica e del server proxy. Per ulteriori informazioni sulla configurazione delle impostazioni di posta elettronica, consultare la sezione Configurazione di posta elettronica e avvisi.

Avvisi di processo

Consente di selezionare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

2. Fare clic su **Salva**.

Nota: Quando si seleziona un nodo come origine di backup o proxy di backup, Arcserve UDP controlla se l'agente è installato sul nodo proxy e se si tratta dell'ultima versione. Arcserve UDP quindi mostra una finestra di dialogo di verifica in cui sono elencati tutti i nodi con una versione obsoleta dell'agente o senza agente installato. Per installare/aggiornare l'agente su questi nodi, selezionare il metodo di installazione e fare clic su **Salva.**

Le modifiche vengono salvate e accanto al nome dell'attività viene visualizzato un segno di spunta verde. La pagina del piano viene chiusa.

Nota: se si deve aggiungere un'altra attività, è necessario selezionare il piano dalla scheda **Risorse** e modificare il piano. Per modificare il piano, fare clic sul piano dal riquadro centrale. Verrà visualizzato il piano e sarà possibile modificarlo. È possibile aggiungere le attività **Copia punto di ripristino**, **Copia su nastro**, **Replica**, e **Replica da RPS remoto** come attività di completamento.

Il piano viene distribuito automaticamente sul nodo del server proxy.

Viene creato il piano di backup di SharePoint Online per il server proxy. Il backup viene eseguito in base alla pianificazione configurata nella scheda **Pianificazione.** È possibile eseguire anche un backup manuale in qualsiasi momento.

(Facoltativo) Esecuzione di un backup manuale

In genere, in base alle impostazioni di pianificazione applicate, i backup vengono eseguiti automaticamente. In aggiunta al backup pianificato, un backup manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze. Se ad esempio si dispone di una pianificazione di ripetizione per backup completi e incrementali e si desidera apportare modifiche sostanziali al computer, è possibile eseguire un backup manuale immediato senza attendere l'esecuzione del backup pianificato successivo.

Per eseguire un backup manuale dei nodi SharePoint Online, procedere come segue:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   I nodi SharePoint Online vengono mostrati nel riquadro centrale.
3. Selezionare i nodi SharePoint Online (ad esempio, Mailbox@<organizationname.com>) di cui si desidera eseguire il backup e accertarsi che sia stato assegnato un piano. Il nome del nodo corrisponde all'account utilizzato durante l'aggiunta del nodo SharePoint Online e alla sua connessione.
4. Fare clic con il pulsante destro del mouse sul nodo, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
5. Selezionare il tipo di backup che si desidera eseguire, quindi fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.
6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.
7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Il backup manuale è stato eseguito correttamente.

Per eseguire un backup manuale di un piano SharePoint Online, procedere come segue:

1. Dalla Console, fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Piani**, quindi fare clic su **Tutti i piani**.

   I piani di backup di SharePoint Online vengono visualizzati nel riquadro centrale.
3. Selezionare il piano di cui si desidera eseguire il backup e ai quali è stato assegnato un piano.

4. Fare clic con il pulsante destro del mouse sul piano, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.

5. Selezionare il tipo di backup che si desidera eseguire, quindi fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.

6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.
7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Il backup manuale è stato eseguito correttamente.

Verifica del backup

Per verificare il processo di backup, confermare di avere creato correttamente il piano di backup. Dopo avere verificato che il piano è stato creato correttamente, confermare se il processo di backup è in esecuzione secondo quanto pianificato. È possibile verificare lo stato dei processi di backup dalla scheda **Processi**.

Per la verifica dei piani, attenersi alla seguente procedura:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i nodi.
3. Verificare che sia stato eseguito il mapping dei piani con i nodi.

Attenersi a uno dei seguenti metodi per verificare i processi di backup:

Metodo 1

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Tutti i processi completati**.

   Lo stato di ciascun processo viene elencato nel riquadro centrale.
3. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Metodo 2

1. Fare clic sulla scheda **Processi**.
2. Dal riquadro sinistro, fare clic su **Processi completati correttamente**.

   L'elenco dei processi di backup completati viene visualizzato nel riquadro centrale.
3. Fare clic sul processo che si desidera verificare.

   Il riquadro destro viene aggiornato.
4. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
5. Verificare che il processo di backup sia stato eseguito correttamente.

   Il processo di backup viene verificato.

Ripristino dei dati di una raccolta siti di SharePoint Online

È possibile ripristinare l'elenco/libreria di SharePoint Online o l'elemento dell'elenco nel sito. La raccolta siti e il sito non sono ancora supportati in Arcserve UDP 8.0. È possibile ripristinare i dati in un sito originale con un nuovo nome, ripristinare i dati nella posizione originale ed esportarli su disco dai punti di ripristino.

Per ripristinare l'elemento dell'elenco di SharePoint Online, procedere come segue:

1. Selezione degli elementi nell'elenco del sito di SharePoint Online da ripristinare
2. Definizione delle opzioni di ripristino
3. Verifica del corretto ripristino del contenuto

Selezione degli elementi nell’elenco del sito di SharePoint Online da ripristinare

È possibile ripristinare i dati degli elementi nell'elenco di SharePoint Online da un punto di ripristino. Quando si seleziona una data di ripristino e poi l'ora, vengono visualizzati tutti i punti di ripristino associati per tale durata. È possibile individuare e selezionare i contenuti di backup (applicazioni incluse) da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere ad Arcserve UDP.
2. Fare clic sulla scheda **Risorse**.
3. Selezionare **Tutti i nodi** nel riquadro sinistro.

   Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   Oppure

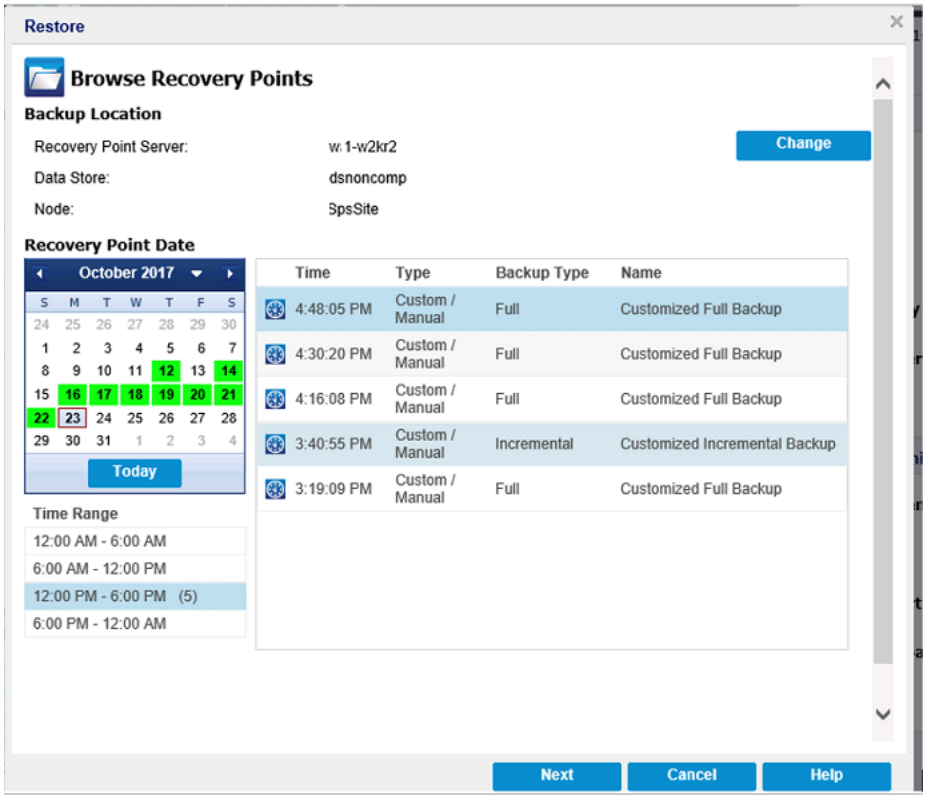
   Selezionare il gruppo **Nodi SharePoint Online**.

   Tutti i nodi SharePoint Online aggiunti vengono visualizzati nel riquadro centrale.
4. Nel riquadro centrale, selezionare il nodo SharePoint Online e fare clic su **Azioni**.
5. Fare clic su **Ripristina** dal menu a discesa Azioni.

   Verrà visualizzata la finestra di dialogo di ripristino della posta di SharePoint.

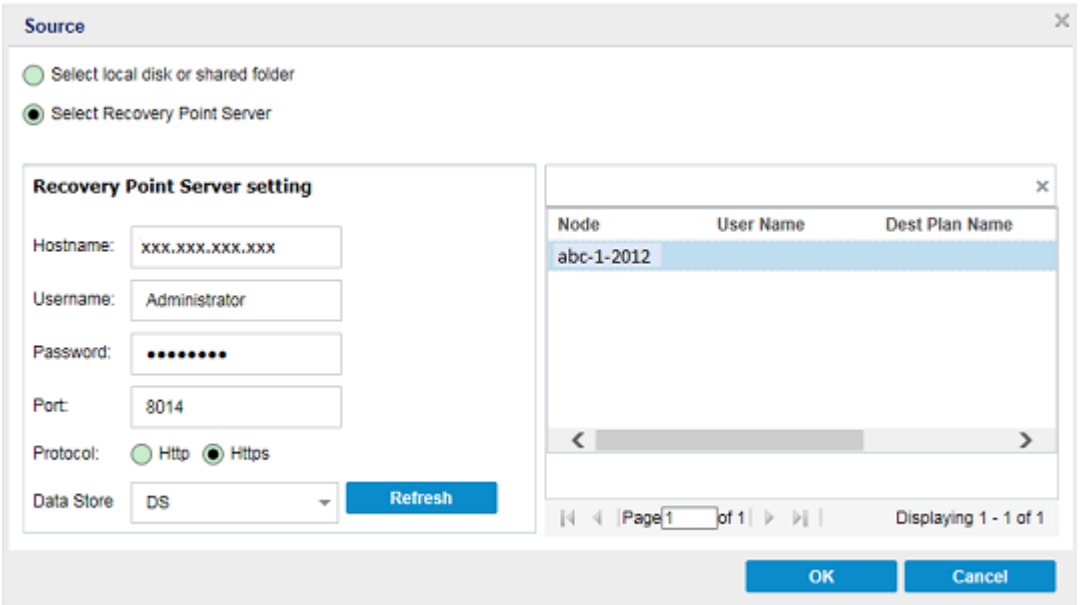
   Nota: L'utente viene connesso automaticamente al nodo dell'agente e viene aperta la finestra di dialogo Ripristina elemento SharePoint.

   La posizione di backup mostra i dettagli del Recovery Point Server.



6. (Facoltativo) Fare clic su **Cambia** per modificare la posizione di backup.

   Viene visualizzata la finestra di dialogo Origine. È possibile selezionare la posizione di backup in questa finestra di dialogo.



Nota: quando si aggiunge un'attività di copia su nastro al piano e si desidera ripristinare il punto di ripristino del backup di copia su nastro, selezionare il punto di

ripristino dal backup di copia su nastro. Per ulteriori informazioni, consultare la sezione Ricerca del punto di ripristino di copia su nastro per il ripristino.

7. Per specificare l'origine, selezionare una delle seguenti opzioni, quindi fare clic su **OK**:

   Selezione di un disco locale o una cartella condivisa

   Nota: in Arcserve UDP, si consiglia di non selezionare l'opzione **Seleziona un disco locale o una cartella condivisa**.

   Selezione di un Recovery Point Server

   a. Specificare i dettagli dell'impostazione Recovery Point Server e fare clic su **Aggiorna**.

      Tutti gli agenti vengono elencati nella colonna Data Protection Agent (Agente di protezione dati) nella finestra di dialogo Origine.

   b. Selezionare l'agente dall'elenco o la libreria visualizzati, quindi fare clic su **OK**.

      I punti di ripristino vengono elencati nella finestra di dialogo di ripristino dell'elemento di SharePoint.

8. Selezionare la data nel calendario per l'immagine di backup che si desidera ripristinare, quindi fare clic su **Avanti**.

   Tutte le date contenenti punti di ripristino per l'origine di backup specificata sono evidenziate in verde.

   Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito (completo, incrementale) e al nome del backup.

9. Dalla finestra di dialogo di ripristino degli elementi di SharePoint Online, espandere la raccolta siti.

   Vengono visualizzati tutti gli elenchi/librerie e un elenco.

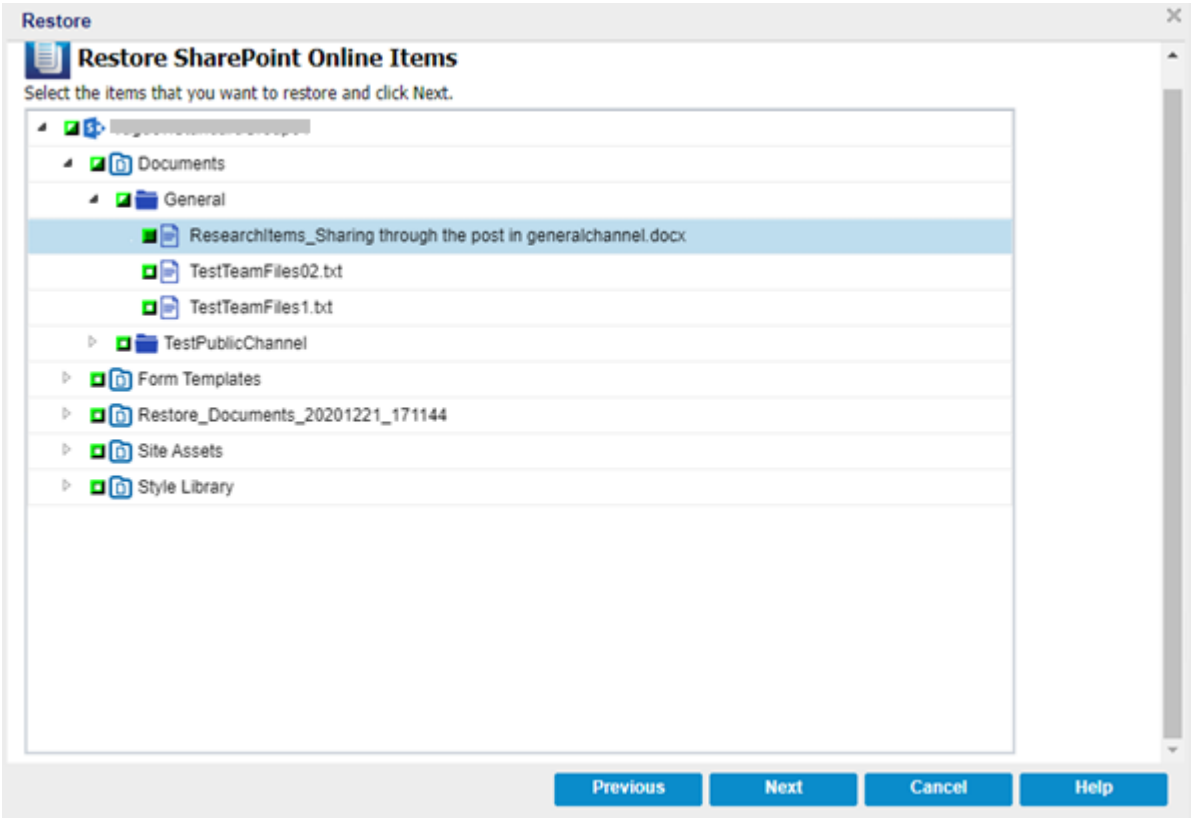
10. Selezionare il sito o il canale specifici disponibili nella raccolta siti di cui si desidera eseguire il ripristino della raccolta siti SharePoint e fare clic su **Avanti**.

    Note:

    - È possibile selezionare l'intero contenuto oppure parte del contenuto dell'oggetto di SharePoint da ripristinare. Per selezionare parte del contenuto, espandere l'oggetto e fare clic sulla casella di controllo del contenuto corrispondente.

- È possibile selezionare più elenchi/librerie o l'elenco degli elementi di SharePoint da ripristinare.

Verrà visualizzata la finestra di dialogo Opzioni di ripristino.



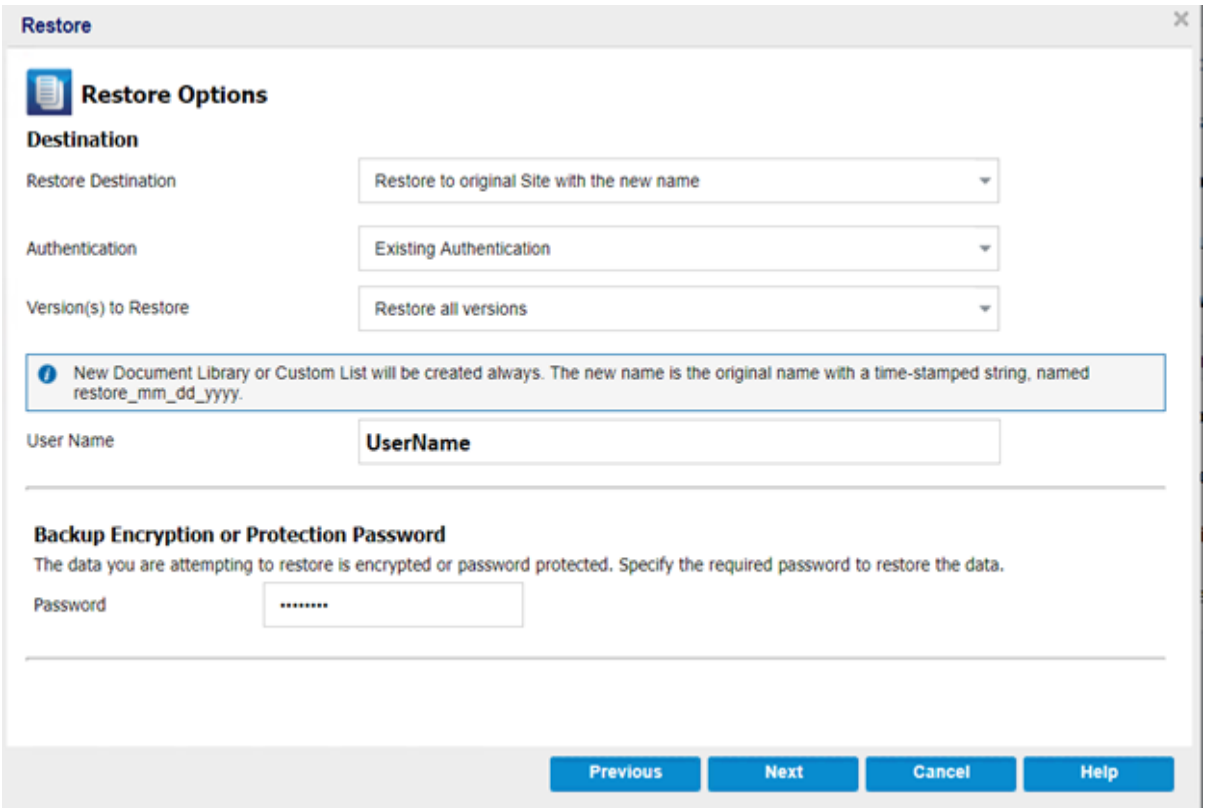
Gli elenchi/librerie o gli elementi dell'elenco di SharePoint Online da ripristinare vengono selezionati. A questo punto, è possibile definire le opzioni di ripristino.

Definizione delle opzioni di ripristino

Dopo avere specificato le informazioni di SharePoint Online da ripristinare, definire le opzioni di ripristino per il contenuto selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo Opzioni di ripristino, selezionare la destinazione di ripristino.



Le opzioni di destinazione disponibili sono:

Ripristina il sito originale con il nuovo nome

Ripristina l'elenco/libreria e i dati degli elementi nell'elenco nello stesso sito con il nome del nuovo elenco da cui è stato eseguito un backup.

Ripristino nella posizione originale

Consente di ripristinare l'elenco/libreria e i dati degli elementi nella stessa posizione da cui è stato eseguito un backup.

2. Specificare una delle opzioni seguenti dall'elenco a discesa Se l'elemento esiste già nella destinazione:

Se il controllo delle versioni è abilitato, aggiungere come nuova versione

Questa opzione funziona quando è abilitata l'impostazione della versione dall'impostazione libreria nel sito di SharePoint. Quando si seleziona questa opzione, se sono presenti gli elementi dell'elenco per le versioni correnti, viene aggiunta la nuova versione alle versioni correnti degli elementi dell'elenco.

Ignora elemento e non ripristinare

Consente di ignorare gli elementi senza eseguire il ripristino.

Sovrascrivi elemento nella destinazione

Sovrascrive l'elemento nella destinazione.

Esporta su disco

Consente di ripristinare gli elenchi/librerie o gli elementi nell'elenco della raccolta siti in una cartella o in una cartella condivisa nel disco.

Nota: Per il ripristino degli elenchi quando si seleziona l'opzione di ripristino dell'esportazione su disco, esportare su disco solamente gli allegati dell'elenco.

Autenticazione

Convalida e identifica l'account utente. Selezionare una delle seguenti opzioni:

- **Autenticazione esistente**

  Quando si seleziona l'autenticazione esistente, viene utilizzato il tipo di autenticazione selezionato durante la creazione del nodo.

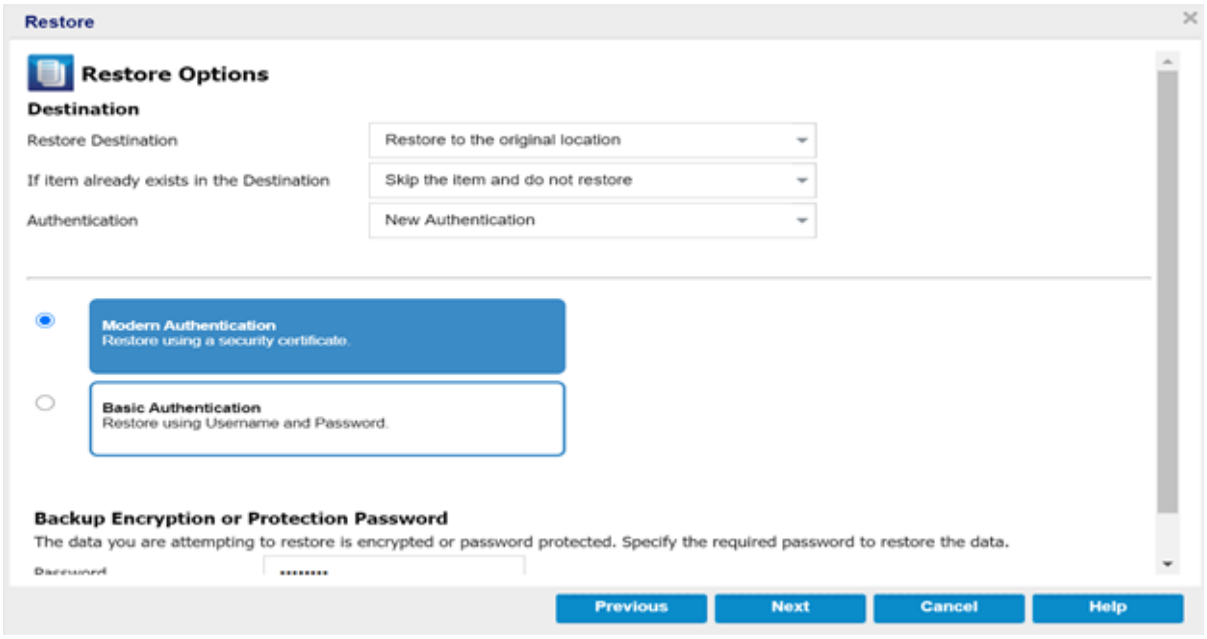
  - Se l'autenticazione del nodo è di base, i parametri quali Nome utente, Password e Crittografia di backup o Password di protezione [se crittografata] vengono caricati automaticamente per procedere con il ripristino.
  - Se l'autenticazione del nodo è moderna, vengono caricati automaticamente parametri quali Nome utente, Crittografia di backup o Password di protezione [se crittografata] per procedere con il ripristino.

- **Nuova autenticazione**

  Durante il ripristino, è possibile selezionare una delle seguenti opzioni per modificare il tipo di autenticazione:

  - Autenticazione moderna

- Autenticazione di base



3. Per applicare l'autenticazione, eseguire una delle seguenti operazioni:

Autenticazione moderna

Per l'autenticazione moderna, è possibile eseguire un ripristino utilizzando un certificato di sicurezza.

Usa certificato di sicurezza

Nota: per impostazione predefinita, il piano di backup seleziona l'opzione **Usa certificato di sicurezza** per l'autenticazione moderna.

Effettuare le operazioni seguenti:

a. Per eseguire l'autenticazione utilizzando un certificato autofirmato, consultare la sezione Download del certificato da UDP e caricamento in Azure.

b. Immettere l'ID applicazione e il nome utente.

c. Per applicare i ruoli e le autorizzazioni richiesti, selezionare la casella di controllo **Consentire ad Arcserve UDP di impostare i ruoli e le autorizzazioni di Azure richiesti per questa applicazione**, quindi fare clic su **Avanti**.

Autenticazione di base

Per l'autenticazione di base, immettere il nome utente e la password per procedere con il ripristino.

Nota: questa opzione non riesce se l'autenticazione moderna è abilitata sul tenant o sull'account.

4. Specificare le versioni dell'elemento nell'elenco che si desidera ripristinare quando è abilitata l'impostazione della versione dall'impostazione libreria nel sito di SharePoint.

   Ripristina tutte le versioni

   Consente di ripristinare tutte le versioni del backup.

   Ripristina solo la versione più recente

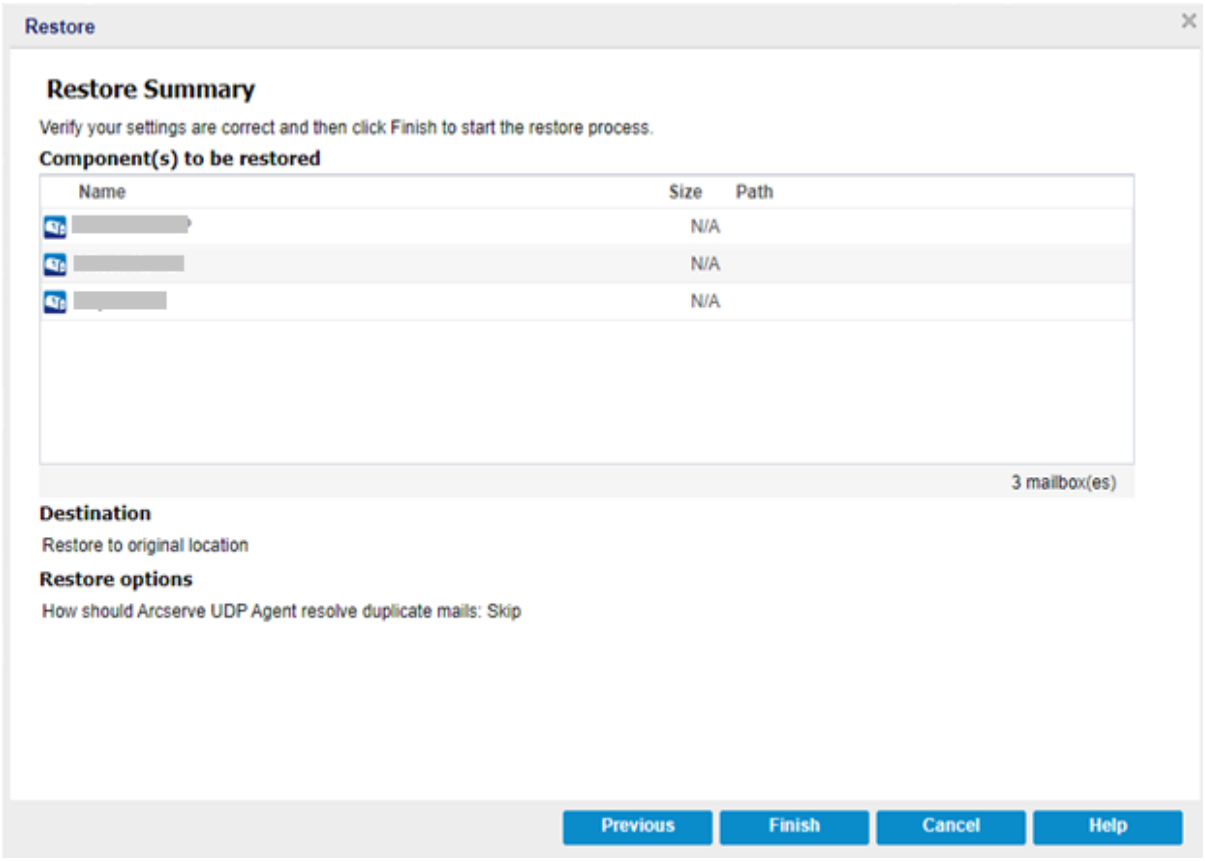
   Consente di ripristinare solo l'ultima versione del backup.

   Ripristina solo la versione principale più recente

   Consente di ripristinare solo la versione principale più recente del backup.

5. Specificare la password della sessione se necessario.
6. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo Riepilogo ripristino.



È possibile verificare le informazioni di ripristino nella finestra di dialogo Riepilogo ripristino.

7. Fare clic su **Fine** per inviare il processo ripristinato.

   Le opzioni di ripristino vengono definite per ripristinare le informazioni di SharePoint Online.

Verifica del corretto ripristino del contenuto

Una volta completato il processo di ripristino, verificare il ripristino del contenuto nella destinazione specificata.

Effettuare le operazioni seguenti:

1. Accedere alla raccolta siti di SharePoint.
2. Verificare l'elenco/libreria e gli elementi dell'elenco.
3. Verificare che il contenuto sia stato ripristinato.

Il contenuto ripristinato è stato verificato correttamente.

Mappa di protezione dei dati per Microsoft Teams

Importante: I dati di Teams per un'intera organizzazione vengono protetti automaticamente se i processi di Exchange, SharePoint e OneDrive sono impostati per utilizzare l'opzione di *protezione di tutti* gli account e i siti.

La tabella seguente descrive la mappa di protezione dei dati per Microsoft Teams:

Elemento Teams	Elementi di cui eseguire il backup in UDP	Da dove eseguire il ripristino
Registrazioni di riunioni pianificate	Account OneDrive dell'utente che esegue le registrazioni	Interfaccia utente dell'agente per l'account OneDrive dell'utente
Chat /Post/Conversazioni 1-1 private	Casella di posta di Exchange dell'utente	Interfaccia utente dell'agente per Exchange
File inviati tramite chat 1-1	Casella di posta Exchange/account OneDrive dell'utente	Interfaccia utente dell'agente per Exchange e account OneDrive dell'utente
Elementi nel canale Teams Standard		
Chat/Post/Conversazioni	Casella di posta di gruppo del canale standard	Interfaccia utente dell'agente per la casella di posta del gruppo
Calendario di Teams per il canale	Casella di posta di gruppo del canale standard	Interfaccia utente dell'agente per la casella di posta del gruppo

File inviati tramite conversazioni chat	Selezionare il sito SharePoint del canale/*Proteggi tutti* i siti o la casella di posta del gruppo del canale	Interfaccia utente dell'agente SharePoint > Sito per canale standard> Raccolta documenti OPPURE Interfaccia utente dell'agente Exchange > Casella di posta di gruppo
File/cartelle caricati utilizzando la scheda File	Selezionare il sito Sharepoint del canale/*Proteggi tutti* i siti	Interfaccia utente dell'agente Sharepoint > Sito per canale standard > Raccolta documenti
Elementi nel canale privato di Teams		
Chat/Post/Conversazioni	Casella di posta di Exchange dell'utente	Interfaccia utente dell'agente per la casella di posta dell'utente
File inviati tramite conversazioni chat	Selezione del sito SharePoint del canale/*Proteggi tutti* i siti o la casella di posta dell'utente	Interfaccia utente dell'agente SharePoint > Sito per canale standard > Raccolta documenti OPPURE Interfaccia utente dell'agente Exchange > Casella di posta dell'utente
File/cartelle caricati utilizzando la scheda File	Selezionare il sito Sharepoint del canale/*Proteggi tutti* i siti	Interfaccia utente dell'agente Sharepoint > Sito per canale standard > Raccolta documenti

Creazione e configurazione di computer virtuali istantanei simultanei su più hypervisor

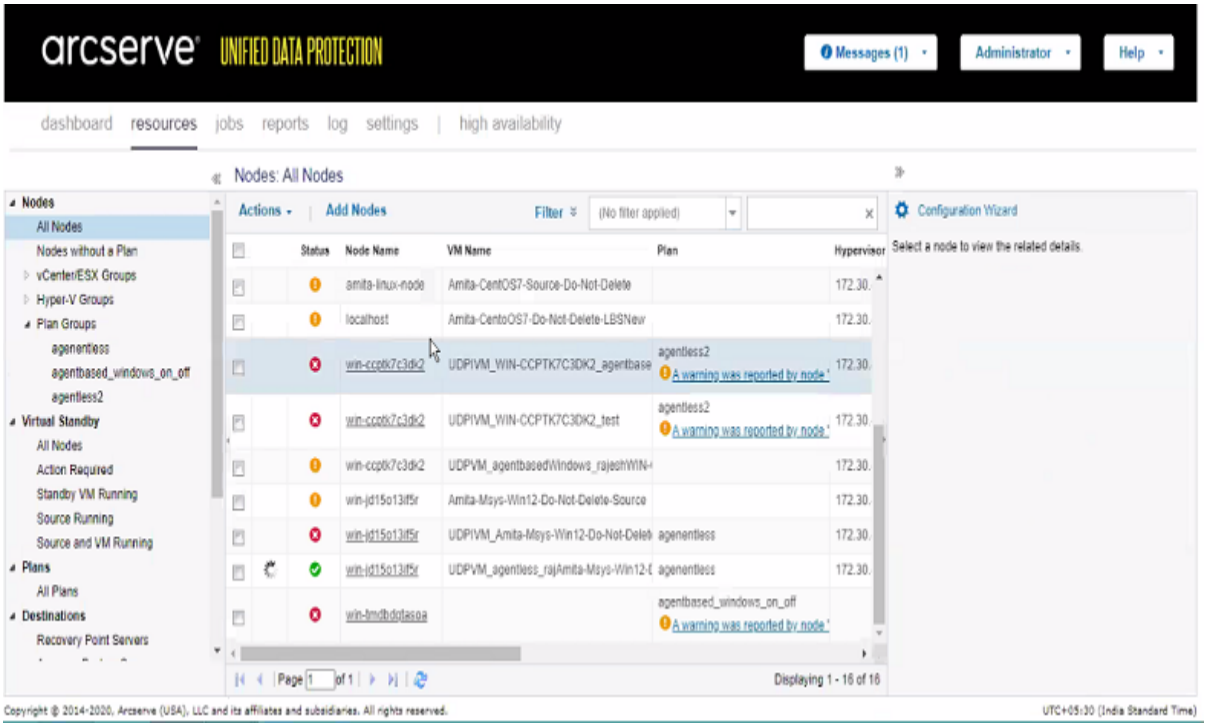
In questa sezione vengono fornite informazioni su come creare e configurare computer virtuali istantanei simultanei su più hypervisor, quali Hyper-V, VMware, Nutanix AHV, Amazon EC2 e Microsoft Azure.

È possibile creare computer virtuali istantanei simultanei dalla console Arcserve UDP utilizzando la procedura guidata Crea computer virtuale istantaneo.

Per aprire la procedura guidata Crea computer virtuale istantaneo, procedere come segue:

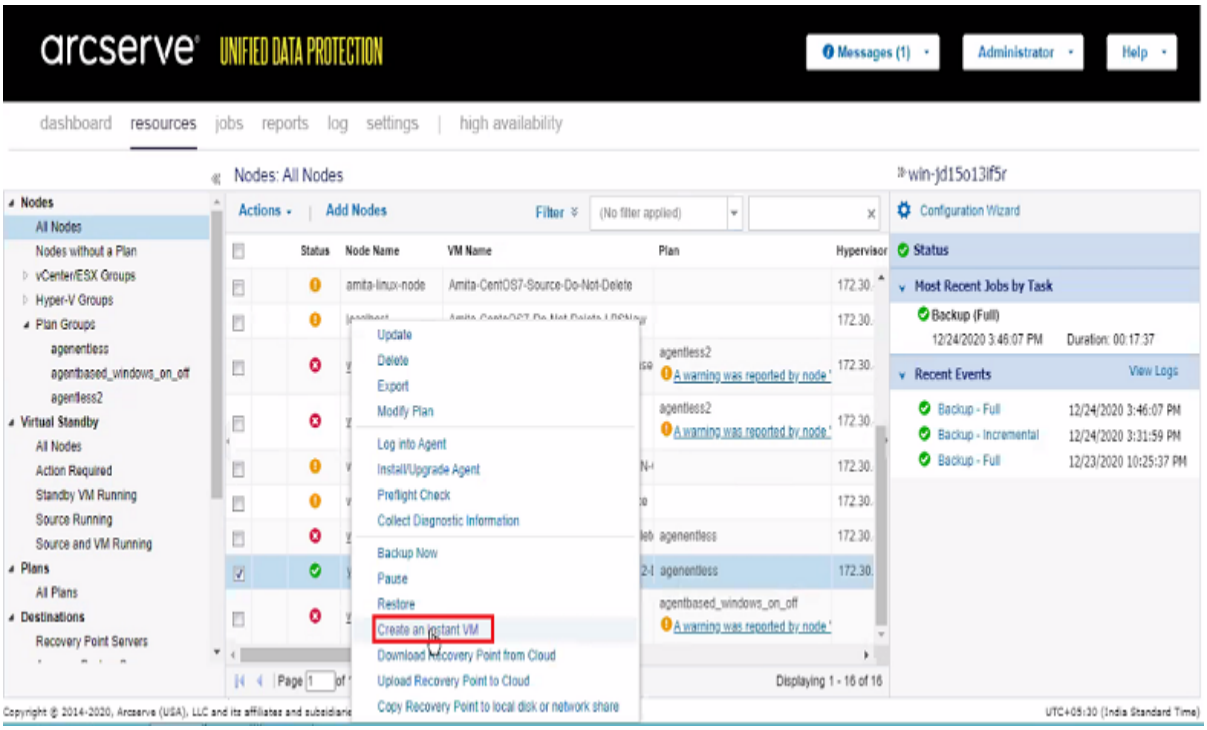
1. Accedere all'account della console UDP.
2. Dalla pagina della console UDP, fare clic sulla scheda **Risorse.**
3. Dal riquadro sinistro, accedere a **Nodi** > **Tutti i nodi**.

   L'elenco dei nodi esistenti viene visualizzato nel riquadro centrale.



4. Selezionare uno o più nodi già associati a un piano.

   Nota: se un nodo non è associato ad alcun piano, l'opzione di creazione di un computer virtuale istantaneo non viene visualizzata.



5. Fare clic con il tasto destro del mouse sui nodi selezionati, quindi selezionare l'opzione **Crea computer virtuale istantaneo**.

Viene visualizzata la procedura guidata Crea un computer virtuale istantaneo. Dalla procedura guidata, è possibile configurare i computer virtuali istantanei simultanei.

Per configurare i computer virtuali istantanei simultanei, procedere come segue:

1. Selezione di un Recovery Point Server di origine
2. Selezione della posizione dei computer virtuali
3. Selezione dei server di ripristino
4. Configurazione delle impostazioni dei computer virtuali
5. Verifica di riepilogo

Selezione di un Recovery point server di origine

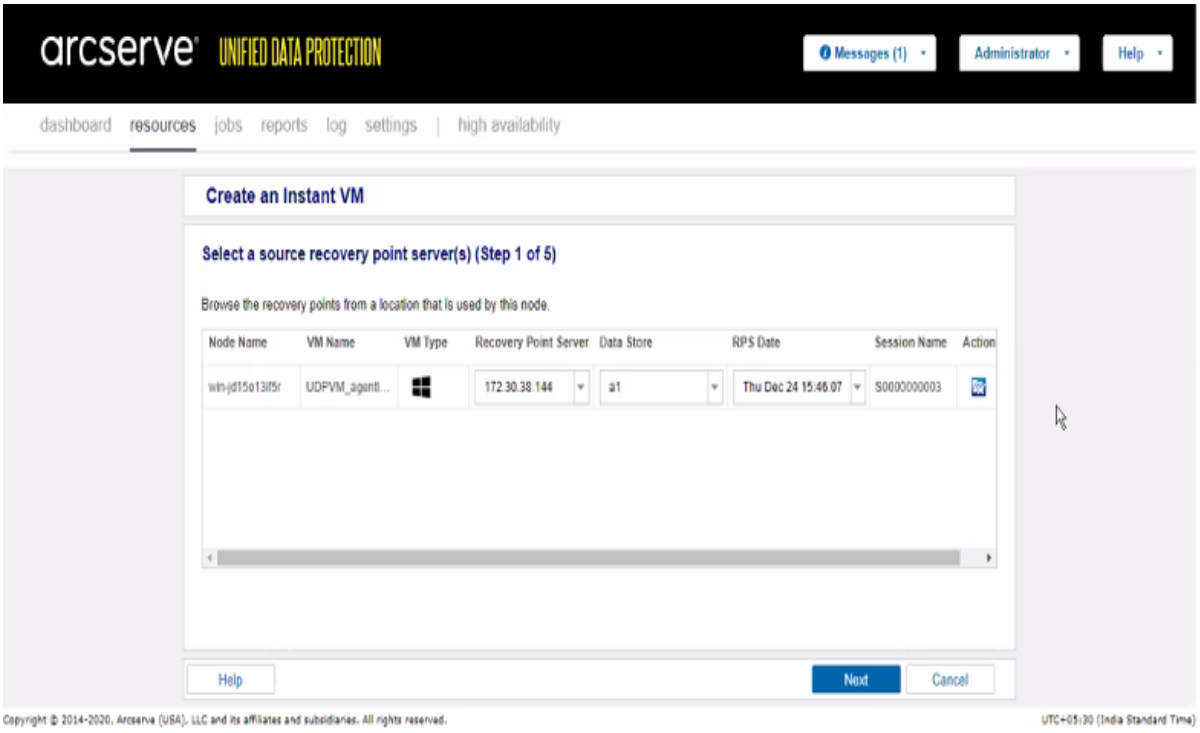
In questa sezione vengono fornite informazioni su come eseguire il primo passaggio di selezione di un Recovery point server di origine.

Viene visualizzata la schermata Selezionare uno o più Recovery Point Server di origine contenente l'elenco dei nodi selezionati con i relativi dettagli quali Nome nodo, Nome computer virtuale, Tipo di computer virtuale, Recovery Point Server, Archivio dati, Data RPS, Nome sessione e Azione. Per ciascun nodo dell'elenco, la console seleziona automaticamente i dettagli relativi al Recovery Point Server,

all'archivio dati e alla data RPS. È inoltre possibile modificare questi dettagli se su ciascun nodo sono disponibili più Recovery Point Server.

Effettuare le operazioni seguenti:

1. Dalla schermata Selezionare uno o più Recovery Point Server di origine, eseguire le seguenti operazioni su ciascun nodo:



   - Per Recovery Point Server, selezionare il Recovery Point Server richiesto dall'elenco a discesa.
   - Per l'archivio dati, selezionare l'archivio dati richiesto dall'elenco a discesa.
   - Per Data RPS, selezionare la data RPS richiesta dall'elenco a discesa.
2. Fare clic su **Avanti**.
3. (Facoltativo) Se la sessione di backup è crittografata per uno dei nodi selezionati, digitare la password.

   Viene visualizzata la schermata Posizione computer virtuale.

Completare il passaggio successivo: Selezione della posizione dei computer virtuali

Selezione della posizione dei computer virtuali

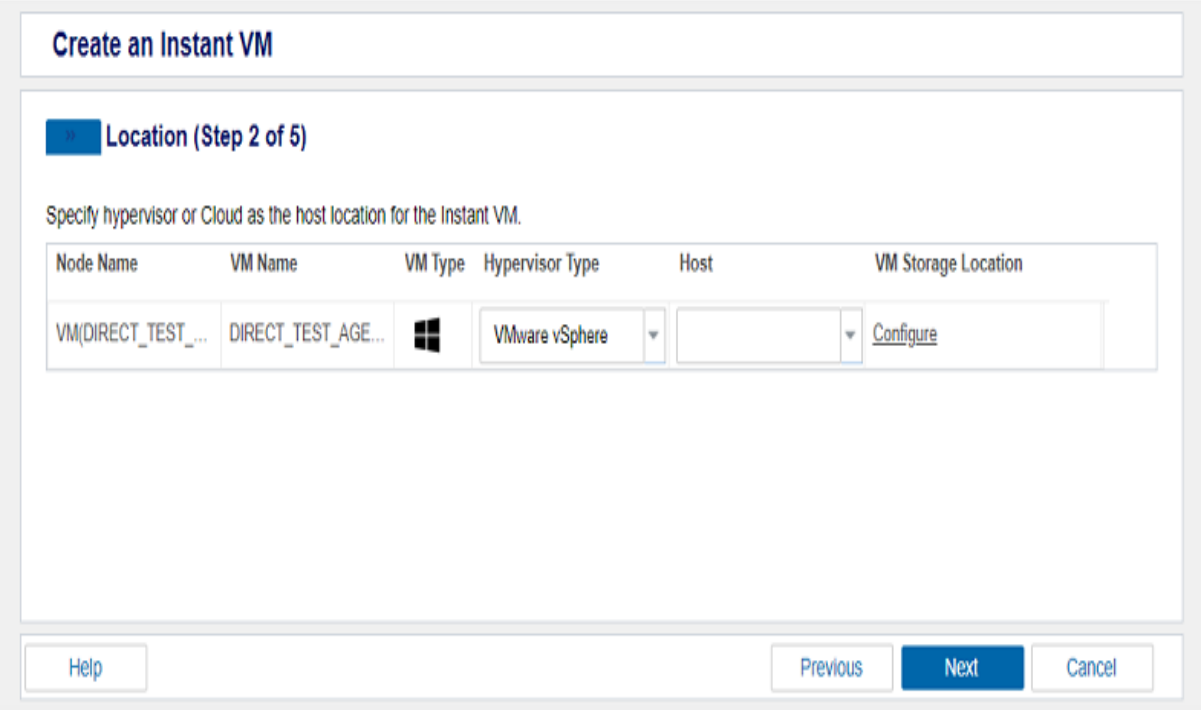
In questa sezione vengono fornite informazioni su come eseguire il secondo passaggio della selezione di una posizione del computer virtuale per l'hosting del

computer virtuale istantaneo.

La schermata Posizione computer virtuale visualizza l'elenco dei nodi selezionati e i relativi dettagli quali il nome del computer virtuale, il tipo di computer virtuale, il tipo di hypervisor e l'host. Per ciascun nodo nell'elenco, è possibile selezionare il tipo di hypervisor e la posizione del computer virtuale per l'hosting del computer virtuale istantaneo.

Effettuare le operazioni seguenti:

1. Dalla schermata Posizione computer virtuale, eseguire le seguenti operazioni su ciascun nodo:



Nodo Windows

- Per Tipo di hypervisor, selezionare il tipo di hypervisor dall'elenco a discesa.

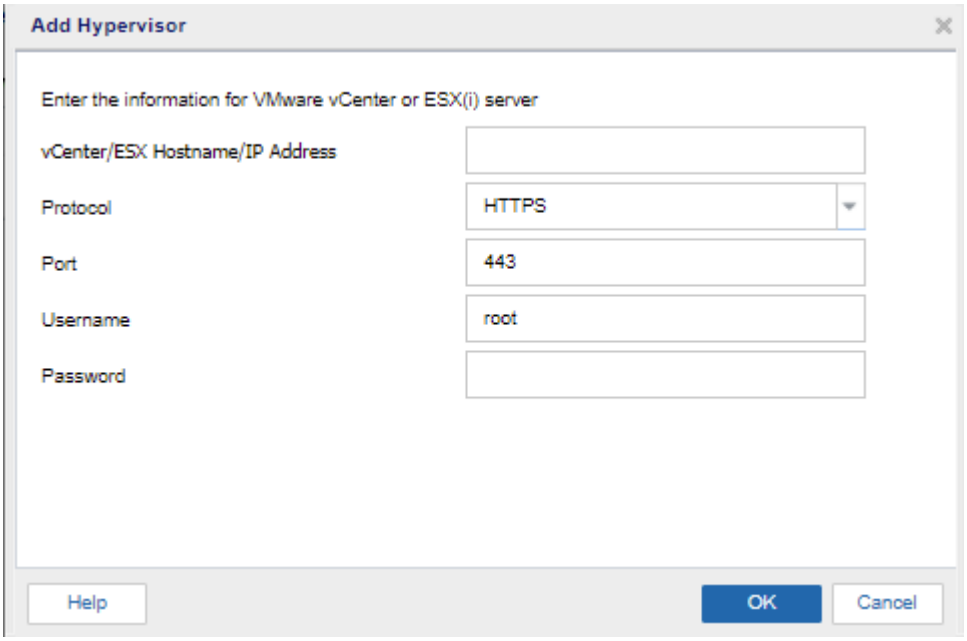
  Nota: Arcserve UDP supporta VMware e Hyper-V per l'hosting dei nodi del computer virtuale istantaneo per Windows.

- Per Host, selezionare l'hypervisor esistente dall'elenco a discesa o aggiungerne uno nuovo.

  Per aggiungere un nuovo hypervisor, procedere come segue:

  a. Dall'elenco a discesa Host, fare clic su **+Aggiungi nuovo hypervisor**.

Viene visualizzata la finestra di dialogo Aggiungi hypervisor.



b. Nella finestra di dialogo Aggiungi hypervisor, fornire i seguenti dettagli, se necessario:

- **Nome host vCenter/ESX/Indirizzo IP**: immettere il nome host o l'indirizzo IP di vCenter.
- **Protocollo**: selezionare il protocollo, ad esempio HTTP o HTTPS.
- **Porta**: immettere il numero di porta.
- **Nome utente**: immettere il nome utente.
- **Password**: immettere la password.

c. Fare clic su **OK**.

Il nuovo hypervisor viene aggiunto.

- Per la posizione di archiviazione del computer virtuale, per configurare la selezione della posizione di archiviazione VMware, fare clic su **Configurato**.

Nodo Linux

- Per Tipo di hypervisor, selezionare il tipo di hypervisor dall'elenco a discesa.

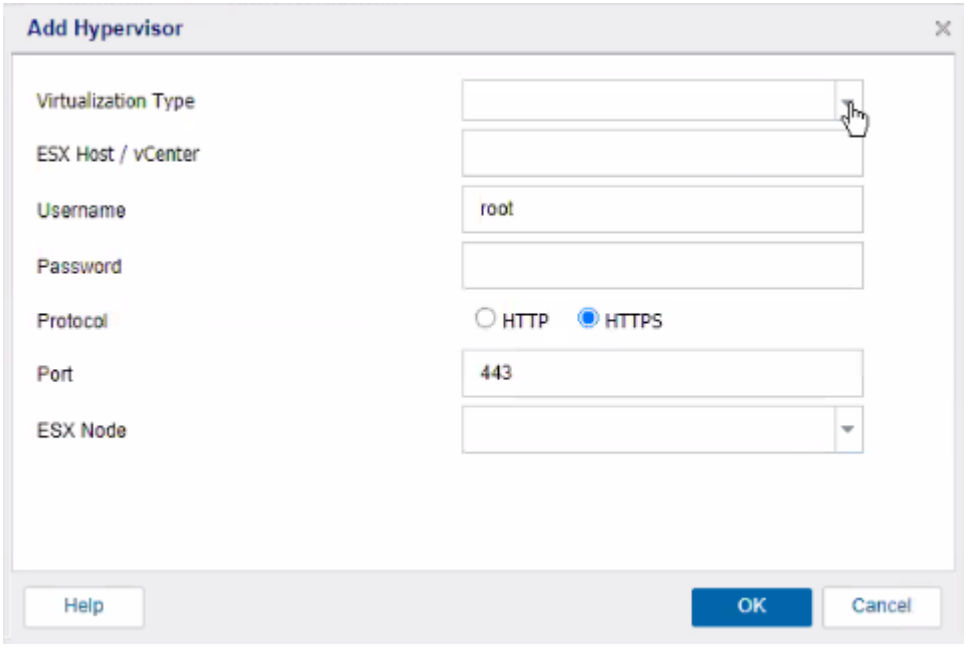
Nota: Arcserve UDP supporta VMware, Hyper-V, Nutanix AHV, Amazon EC2 e Microsoft Azure per l'hosting del computer virtuale istantaneo per i nodi Linux.

- Per Host, selezionare l'hypervisor esistente dall'elenco a discesa o aggiungerne uno nuovo.

  Per aggiungere un nuovo hypervisor, procedere come segue:

  a. Dall'elenco a discesa Host, fare clic su **+Aggiungi nuovo hypervisor**.

     Viene visualizzata la finestra di dialogo Aggiungi hypervisor.



  b. Nella finestra di dialogo Aggiungi hypervisor, dall'elenco a discesa Tipo di virtualizzazione, selezionare una delle seguenti opzioni:

     VMware

     Fornire i seguenti dettagli, se necessario:

     - **Host ESX/vCenter**: immettere il nome host o l'indirizzo IP di vCenter.
     - **Nome utente**: immettere il nome utente.
     - **Password**: immettere la password.

- **Protocollo**: selezionare il protocollo, ad esempio HTTP o HTTPS.
- **Porta**: immettere il numero di porta.
- **Nodo ESX**: dal menu a discesa, selezionare uno dei nodi disponibili.

Hyper-V

Fornire i seguenti dettagli, se necessario:

- **Nome host Hyper-V**: immettere il nome host per l'hypervisor Hyper-V.
- **Nome utente**: immettere il nome utente.
- **Password**: immettere la password.

Nutanix AHV

Fornire i seguenti dettagli, se necessario:

- **Indirizzo IP virtuale del cluster Nutanix AHV**: immettere l'indirizzo IP.
- **Nome utente**: immettere il nome utente.
- **Password**: immettere la password.
- **Porta**: immettere il numero di porta.

EC2

Fornire i seguenti dettagli, se necessario:

- **Nome account**: immettere il nome dell'account cloud. Se l'account cloud non viene aggiunto, fare clic su Aggiungi. Per ulteriori informazioni, consultare la sezione Aggiunta di un account cloud.
- **Area**: dal menu a discesa, selezionare l'area disponibile.

Azure

Fornire i seguenti dettagli, se necessario:

- **Nome account**: immettere il nome dell'account cloud. Se l'account cloud non viene aggiunto, fare clic su Aggiungi. Per ulteriori informazioni, consultare la sezione

Aggiunta di un account cloud.

- **Gruppo di risorse**: dall'elenco a discesa, selezionare il gruppo di risorse disponibile.
- **Area**: dal menu a discesa, selezionare l'area disponibile.

c. Fare clic su **OK**.

Il nuovo hypervisor viene aggiunto.

- Per la posizione di archiviazione del computer virtuale, per configurare la selezione della posizione di archiviazione VMware, fare clic su **Configurato**.

2. Fare clic su **Avanti**.

Viene visualizzata la schermata Server di ripristino.

Completare il passaggio successivo: Selezione dei server di ripristino

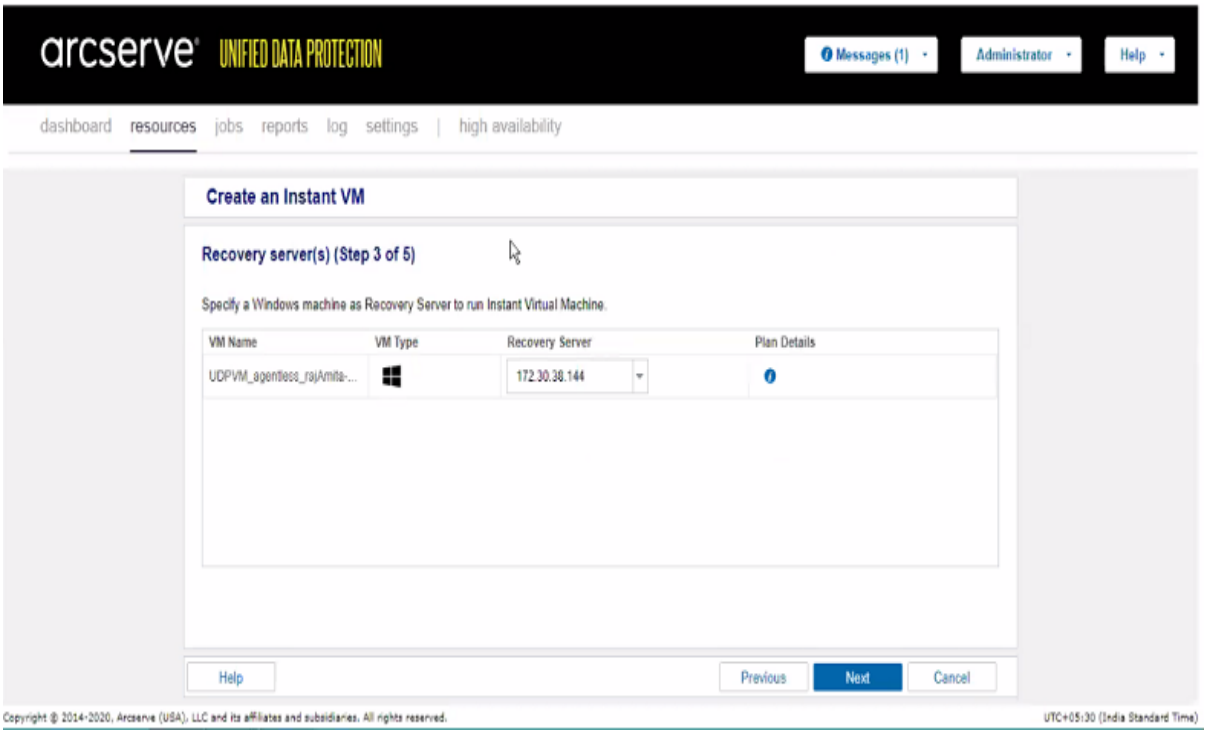
Selezione dei server di ripristino

In questa sezione vengono fornite informazioni su come eseguire il terzo passaggio della selezione di un server di ripristino per l'esecuzione del computer virtuale istantaneo.

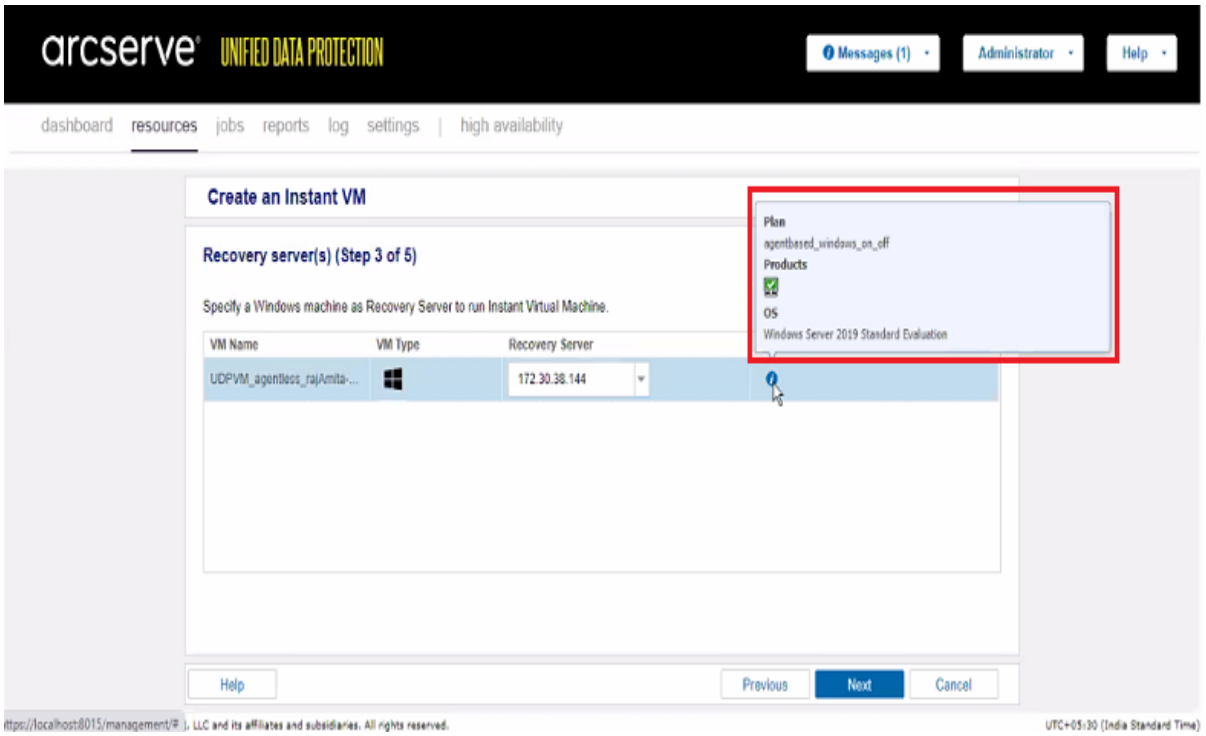
Nella schermata Server di ripristino viene visualizzato l'elenco dei nodi selezionati e i relativi dettagli quali il nome del computer virtuale, il tipo di computer virtuale, il server di ripristino e i dettagli del piano. Per ciascun nodo nell'elenco, è possibile selezionare il server di ripristino per eseguire il computer virtuale istantaneo.

Effettuare le operazioni seguenti:

1. Dalla schermata Server di ripristino, eseguire le seguenti operazioni su ciascun nodo:



- Per il server di ripristino, dall'elenco a discesa selezionare il server di ripristino richiesto.
- Per i dettagli del piano, posizionare il mouse sull'icona delle informazioni per verificare i dettagli del piano.



Note:

- Per le sessioni di backup di Linux, il server di ripristino è un server di backup di Linux.
- Quando l'hypervisor è VMware vSphere, il ruolo Network File System (NFS) di Windows deve essere installato sul Recovery Point Server. Viene installato automaticamente durante il processo del computer virtuale istantaneo. Per installare manualmente il servizio NFS, consultare la sezione Installazione manuale di NFS su un server Windows.

2. Fare clic su **Avanti**.

   Viene visualizzata la schermata Impostazioni computer virtuali.

Completare il passaggio successivo: Configurazione delle impostazioni dei computer virtuali

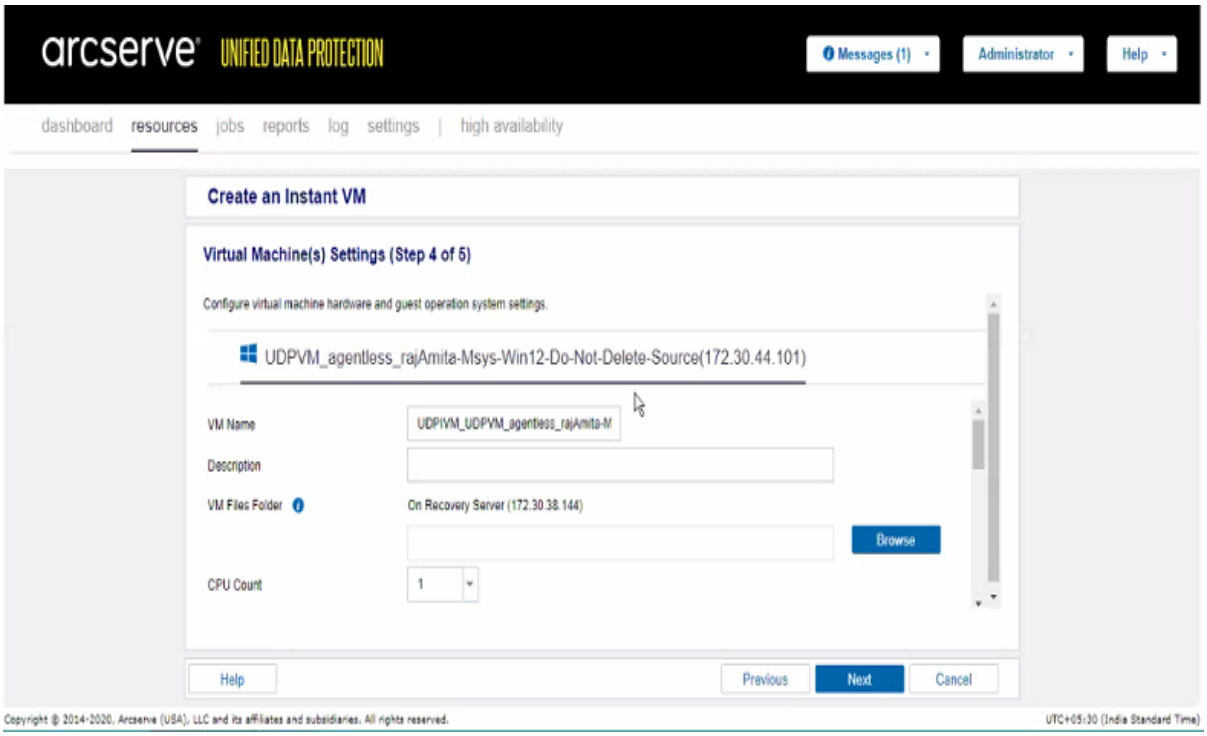
Configurazione delle impostazioni dei computer virtuali

In questa sezione vengono fornite informazioni su come configurare le impostazioni dei computer virtuali per la creazione di un computer virtuale istantaneo.

La schermata Impostazioni computer virtuale visualizza singole sezioni per ciascun nodo selezionato con i relativi dettagli di configurazione. In ciascuna sezione è possibile fornire i dettagli necessari per creare il computer virtuale istantaneo.

Effettuare le operazioni seguenti:

1. Dalla schermata Impostazioni computer virtuale, fare clic sul nodo del computer virtuale che si desidera configurare.



2. Sul nodo del computer virtuale selezionato, eseguire le seguenti operazioni:
   - Per il nome del computer virtuale, digitare il nome del computer virtuale istantaneo. Il nome del nodo di origine con prefisso diventa il nome predefinito del computer virtuale istantaneo.
   - (Facoltativo) Per Descrizione, immettere la descrizione necessaria per il computer virtuale istantaneo.
   - Per la cartella File computer virtuale, fare clic sul pulsante **Sfoglia** per selezionare la posizione della cartella sul server di ripristino per il computer virtuale istantaneo. È inoltre possibile creare una nuova cartella dalla finestra di dialogo Cartella file computer virtuale.

     Nota: l'opzione Cartella file computer virtuale è disponibile solo per i nodi del computer virtuale di Windows. Per il nodo del computer virtuale di Linux, è possibile selezionare l'archivio dati disponibile dall'elenco a discesa Archivio dati file del computer virtuale.
   - Per Numero CPU, selezionare il numero di CPU per il computer virtuale istantaneo.
   - Per Dimensione memoria, immettere la dimensione della memoria per il computer virtuale istantaneo.

Nota: è inoltre possibile utilizzare il dispositivo di scorrimento per specificare la dimensione della memoria per il computer virtuale istantaneo.

- Per le schede di rete, procedere come segue:

  Aggiungere una scheda di rete

  È possibile aggiungere più schede di rete. Una volta aggiunta la scheda di rete, è possibile modificarla ed eliminarla dalla colonna Azioni.

  Nota: per un computer virtuale istantaneo di Linux, è possibile utilizzare almeno una scheda NIC virtuale per stabilire la connessione al server di backup di Linux.

  Per aggiungere una scheda di rete, procedere come segue:

  a. Nella sezione Scheda di rete, fare clic su **Aggiungi una scheda di rete**.

     Viene visualizzata la finestra di dialogo Aggiungi scheda di rete.

  b. Nella finestra di dialogo Aggiungi scheda di rete, immettere i dettagli seguenti, quindi fare clic su **OK**.

     - **Rete virtuale**: dall'elenco a discesa Rete virtuale, selezionare la rete virtuale richiesta.
     - **Tipo di scheda di rete**: dall'elenco a discesa Tipo di scheda di rete, selezionare il tipo di scheda.
     - **Impostazioni TCP/IP**: dall'elenco a discesa Impostazioni TCP/IP, selezionare **Origine (Automatico)** o **Impostazioni IP/Gateway/DNS/WINS personalizzate** in base alle proprie esigenze.

       Nota: se si seleziona l'opzione Impostazioni IP/Gateway/DNS/WINS personalizzate, fare clic su Aggiungi indirizzo per fornire manualmente i dettagli TCP/IP.

  La scheda di rete è stata aggiunta.

  Aggiornare il DNS

  Se sono già stati forniti un indirizzo IP e un indirizzo DNS nella scheda di rete e nel computer di origine di un dominio, è possibile aggiornare il DNS procedendo come segue:

Nota: questa funzionalità è disponibile solo per i computer virtuali istantanei di Windows.

a. Nella sezione Scheda di rete, fare clic su **Aggiorna DNS**.

b. Per aggiungere un record di aggiornamento DNS, fare clic su **Aggiungi indirizzo DNS**.

Note:

- È possibile rimuovere il record di aggiornamento DNS. Per rimuoverlo, fare clic su **Rimuovi**.
- Per regolare la sequenza dei record, fare clic sui pulsanti Su e Giù.

c. Selezionare un indirizzo DNS e un indirizzo IP dall'elenco a discesa, quindi fare clic su **OK**.

d. Specificare la durata (TTL).

e. Specificare l'autenticazione DNS.

Per i server DNS di Microsoft, immettere nome utente e password. Per i server Bind, è necessario specificare il percorso completo, compreso il nome del file di chiave sul server di ripristino.

- Per le impostazioni avanzate, procedere come segue:
  - Verificare lo spazio libero su disco della capacità della cartella del file del computer virtuale.

    Nota: La casella di controllo **Monitora spazio libero su disco per la capacità della cartella di file del computer virtuale** è selezionata per impostazione predefinita. La barra di capacità viene visualizzata in giallo nella pagina Computer virtuale istantaneo se lo spazio disponibile della capacità della cartella del file del computer virtuale è minore del valore di soglia. Il valore di soglia predefinito è 3%. È possibile modificare il valore in base alle proprie esigenze.
  - Selezionare la casella di controllo **Specificare il tipo di controller disco per il computer virtuale**, quindi selezionare il tipo di controller del disco dall'elenco a discesa per il computer virtuale.

    Nota: La casella di controllo **Specificare il tipo di controller disco per il computer virtuale** è disponibile se è stato

selezionato **VMware vSphere** come posizione del computer virtuale. Il computer virtuale istantaneo viene creato mediante l'applicazione del controller del disco specificato in VMware.

- Per reindirizzare gli aggiornamenti del disco virtuale all'archivio dati di VMware, procedere come segue:

  a. Selezionare la casella di controllo **Reindirizza aggiornamenti del disco virtuale all'archivio dati VMware**.

     Nota: la casella di controllo **Reindirizza aggiornamenti del disco virtuale all'archivio dati VMware** è disponibile solo se è stato selezionato VMware vSphere come posizione del computer virtuale.

  b. Dal menu a discesa, selezionare l'archivio dati VMware richiesto.

  Gli aggiornamenti del disco virtuale vengano reindirizzati all'archivio dati VMware selezionato.

- Per modificare il nome host del computer virtuale istantaneo, procedere come segue:

  a. Fare clic sulla casella di controllo **Modifica nome host**.

     La schermata viene aggiornata con i nuovi campi.

  b. Nel campo Nuovo nome host, immettere il nuovo nome host.

  c. Se il computer di origine si trova in un dominio, fornire i seguenti dettagli, se necessario:

     - **Account utente**: immettere l'account utente.
     - **Password**: immettere la password.
     - **Conferma password**: digitare nuovamente la password per confermarla.

     Nota: se il computer di origine è compreso in un dominio, l'account deve disporre delle autorizzazioni necessarie per la modifica del nome host nel dominio.

- (Facoltativo) Per il computer virtuale istantaneo di Linux, selezionare la casella di controllo **Ripristina i dati automaticamente dopo l'avvio del computer virtuale istantaneo** per abilitare il ripristino automatico dei dati con l'avvio del computer virtuale istantaneo di destinazione.

Il comportamento predefinito del computer virtuale istantaneo di Linux deve innanzitutto eseguire il ripristino dei dati necessari e avviare il computer virtuale. Se l'opzione non è selezionata, quando il computer virtuale viene avviato, i dati restanti non vengono ripristinati, anche nel caso in cui vengano utilizzati come computer virtuale normale. Se l'opzione è attivata, i dati rimanenti vengono ripristinati sul backend durante l'utilizzo del computer virtuale. È inoltre possibile salvare la destinazione del computer virtuale istantaneo in modo permanente una volta completato il ripristino dei dati.

Nota: quando lo stato del computer virtuale istantaneo di Linux di destinazione non è attivato, il processo del computer virtuale non riesce. Se tale punto di ripristino viene unito, il computer virtuale istantaneo di Linux non viene attivato.

3. Fare clic su **Avanti**.

   Verrà visualizzata la schermata Riepilogo.

Completare il passaggio finale: Verifica di riepilogo

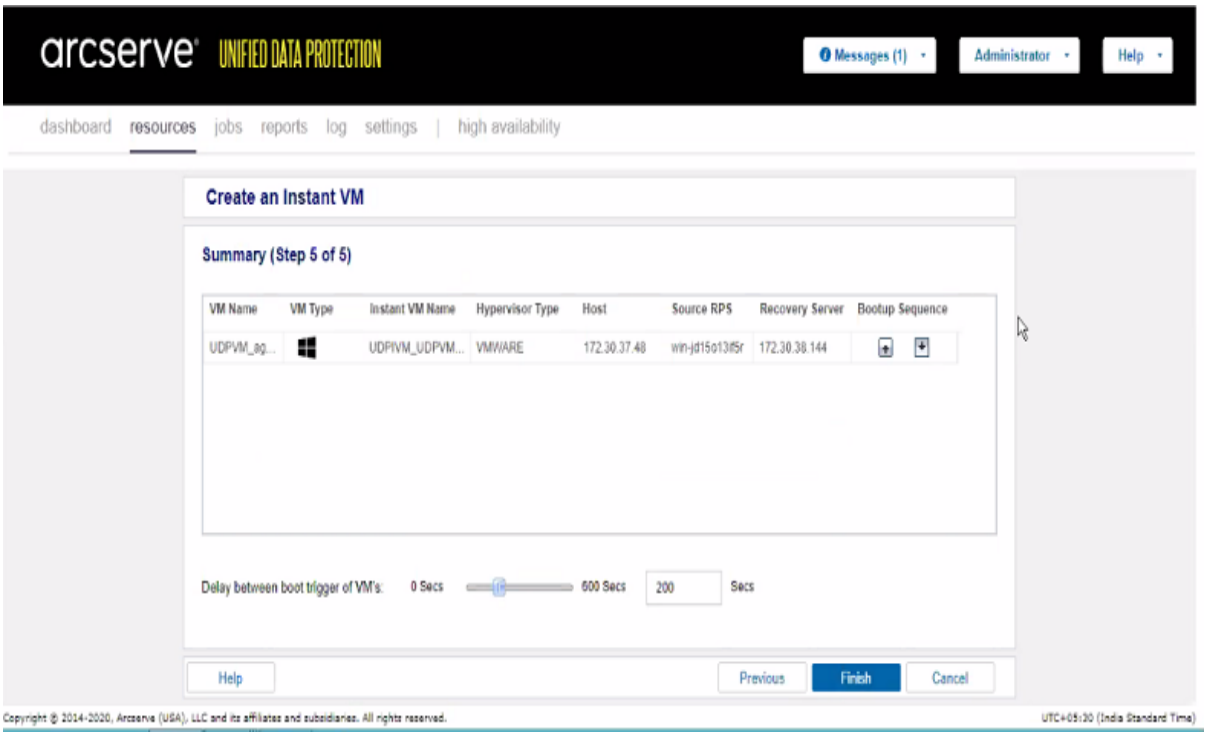
Verifica di riepilogo

Si tratta del passaggio finale per la creazione di computer virtuali istantanei simultanei. In questa sezione vengono fornite informazioni su come verificare il riepilogo, regolare la sequenza di avvio e stabilire il ritardo tra l'attivazione dei computer virtuali.

La schermata Riepilogo visualizza l'elenco dei nodi selezionati con dettagli quali il nome del computer virtuale, il tipo di computer virtuale, il nome del computer virtuale istantaneo, il tipo di hypervisor, l'host, il server RPS di origine, il server di ripristino e la sequenza di avvio. È possibile verificare i dettagli e assegnare priorità ai computer virtuali nell'ordine in cui si desidera avviarli.

Effettuare le operazioni seguenti:

1. Dalla schermata Riepilogo, eseguire le seguenti operazioni:



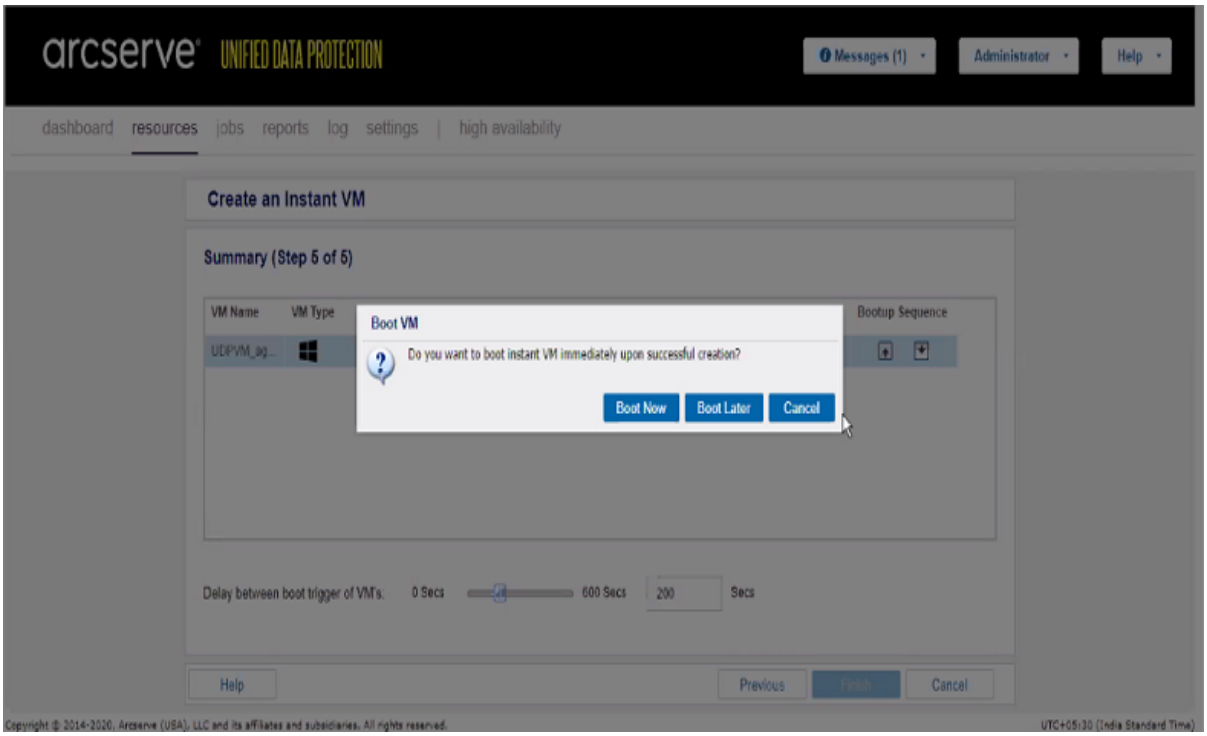
   - Dall'elenco dei nodi, in Sequenza di avvio di ciascun nodo, fare clic sul pulsante Su o Giù per assegnare la priorità alla sequenza di avvio del computer virtuale.
   - Per Ritardo tra i trigger di avvio dei computer virtuali, immettere un intervallo di tempo compreso tra 0 e 600 secondi.

     Nota: è inoltre possibile utilizzare il dispositivo di scorrimento per impostare il ritardo.

2. Fare clic su **Fine**.

   Viene visualizzata la finestra di dialogo Avvia computer virtuale.

3. Nella finestra di dialogo Computer virtuale, selezionare una delle seguenti voci:



- **Avvia ora**: crea computer virtuali istantanei simultanei. Dopo aver creato i computer virtuali istantanei simultanei, la console avvia automaticamente i computer virtuali.
- **Avvia più tardi**: crea computer virtuali istantanei simultanei. Dopo aver creato i computer virtuali istantanei simultanei, è possibile avviare manualmente i computer virtuali.
- **Annulla**: si torna alla pagina Crea nuovi computer virtuali istantanei senza che vengano computer virtuali istantanei simultanei.

Vengono creati computer virtuali istantanei simultanei.

Configurazione di computer Virtual Standby simultanei

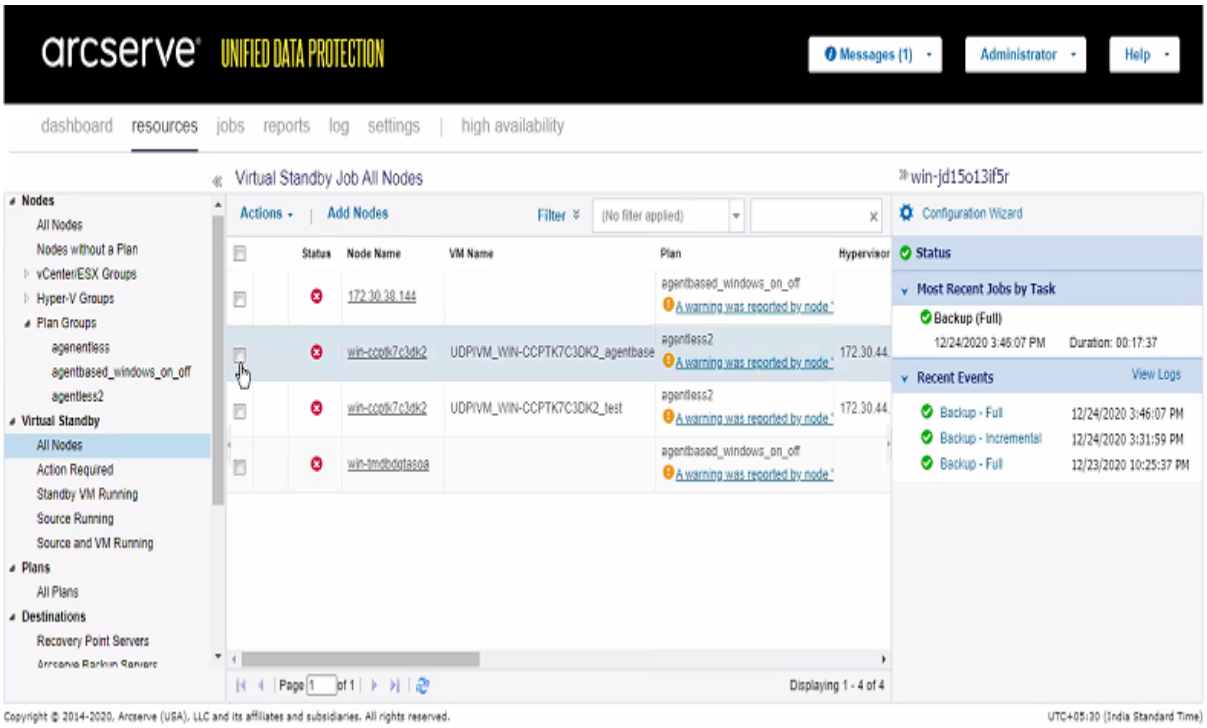
In questa sezione vengono fornite informazioni sulla configurazione dei computer Virtual Standby simultanei.

È possibile configurare computer Virtual Standby simultanei dalla console Arcserve UDP utilizzando la finestra di dialogo Computer virtuale di standby.

Effettuare le operazioni seguenti:

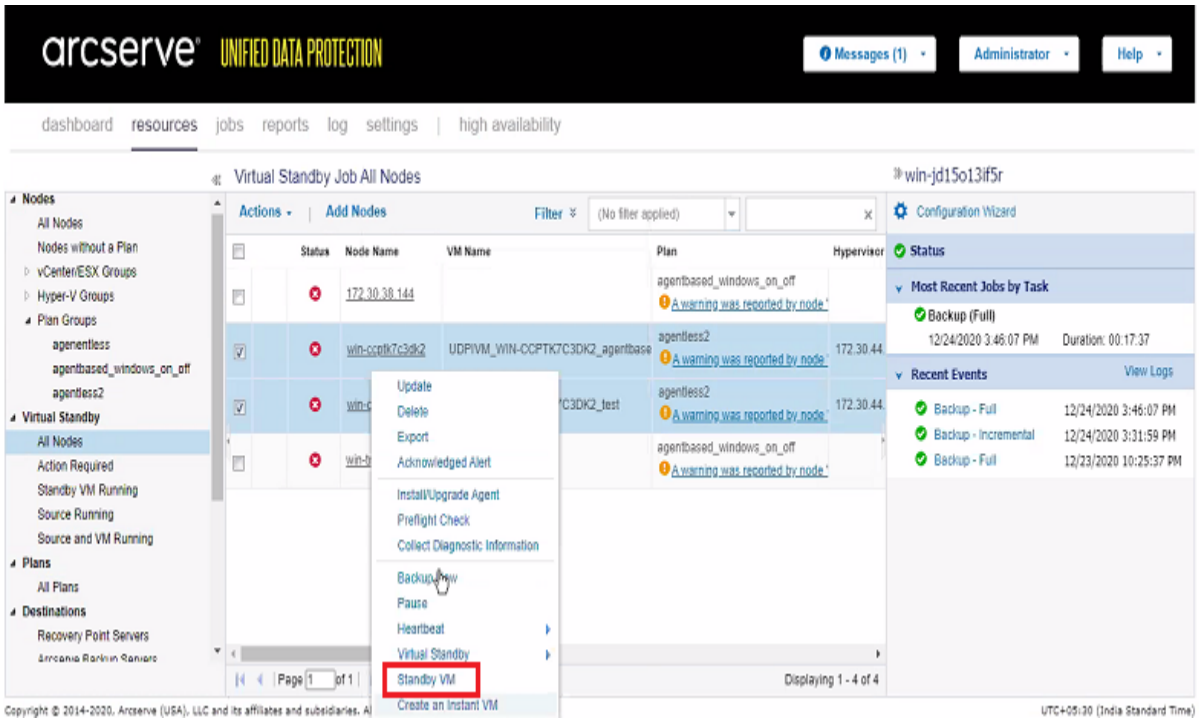
1. Accedere alla console Arcserve UDP.
2. Dalla pagina della console UDP, fare clic sulla scheda **Risorse.**
3. Dal riquadro sinistro, accedere a **Nodi** > **Tutti i nodi**.

   L'elenco dei nodi esistenti viene visualizzato nel riquadro centrale.



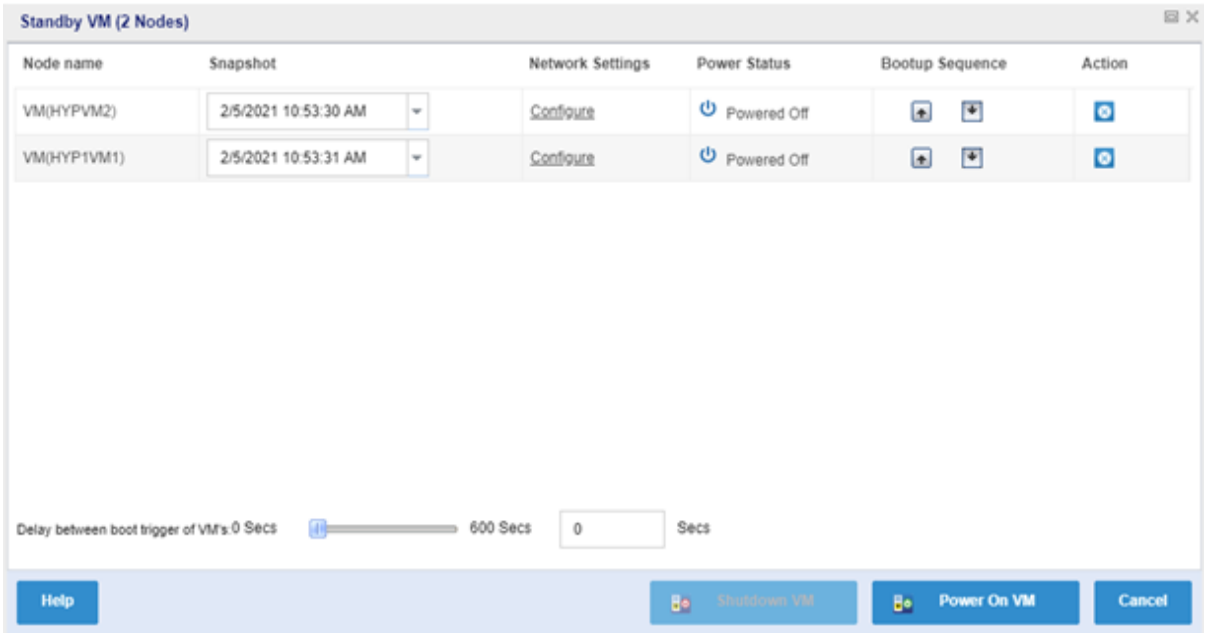
4. Selezionare uno o più nodi già associati a un piano.

   Nota: se un nodo non è associato ad alcun piano, l'opzione Computer virtuale di standby non viene visualizzata.



5. Fare clic con il tasto destro del mouse sui nodi selezionati, quindi selezionare l'opzione **Computer virtuale di standby**.

   Viene visualizzata la finestra di dialogo Computer virtuale di standby con l'elenco dei nodi selezionati.



6. Nella finestra di dialogo Computer virtuale di standby, completare le informazioni seguenti:

- **Attiva computer virtuale**

  Nota: questa opzione è abilitata solo per i computer Virtual Standby disattivati.

  Per attivare i computer virtuali contemporaneamente, procedere come segue:

  a. Dall'elenco dei nodi selezionati, eseguire le seguenti operazioni per ciascun nodo:

     - Per Snapshot, selezionare la data e l'ora della snapshot del punto di ripristino dall'elenco a discesa.

       Nota: i dettagli della snapshot vengono visualizzati solo quando il processo VSB viene completato correttamente.

     - Per le impostazioni di rete, selezionare il collegamento Configura. Per ulteriori informazioni, consultare la sezione Configurazione della rete del computer virtuale di standby.

     - Per Sequenza di avvio, fare clic sul pulsante Su o Giù per assegnare la priorità alla sequenza di avvio del computer virtuale di standby.

     - In Azione, fare clic sull'icona a forma di croce blu per rimuovere il nodo.

  b. (Facoltativo) Per Ritardo tra i trigger di avvio dei computer virtuali, immettere un intervallo di tempo compreso tra 0 e 600 secondi.

     Nota: è inoltre possibile utilizzare il dispositivo di scorrimento per impostare il ritardo.

  c. Fare clic su **Attiva computer virtuale**.

     Il computer virtuale di standby viene attivato utilizzando simultaneamente i dati contenuti nella snapshot del punto di ripristino.

- **Arresta computer virtuale**

  Per arrestare i computer Virtual Standby contemporaneamente, fare clic su **Arresta computer virtuale**.

  Nota: questa opzione è abilitata solo per i computer Virtual Standby attivati.

Chapter 12: Utilizzo di una snapshot hardware per il backup

La presente sezione descrive i seguenti argomenti:

Utilizzo di una snapshot hardware per il backup

Arcserve UDP ha la possibilità di utilizzare le snapshot di archiviazione hardware per il backup. È possibile specificare se si desidera utilizzare la snapshot hardware durante la creazione di un'attività di backup. Se si seleziona la snapshot hardware, Arcserve UDP prova innanzitutto a creare una snapshot hardware. In caso di errore della snapshot hardware, Arcserve UDP torna automaticamente alla snapshot software senza interrompere il processo di backup.

È possibile utilizzare la snapshot hardware per un backup basato sull'agente (computer fisici Windows) e un backup senza agente basato su host (VMware e Hyper-V).

Array di archiviazione supportati:

- **Array di archiviazione NetApp:** NetApp Arcserve UDP supporta snapshot hardware per il backup basato sull'agente (computer fisici Windows) e per il backup senza agente basato sull'host (VMware e Hyper-V).
- **Array di archiviazione Nimble:** Arcserve UDP supporta snapshot hardware per il backup basato sull'agente (computer fisici Windows) e per il backup senza agente basato sull'host (VMware e Hyper-V).
- **Array HPE 3PAR StoreServ:** Arcserve UDP supporta snapshot hardware per il backup basato sull'agente (computer fisici Windows) e per il backup senza agente basato sull'host (VMware e Hyper-V).
- **Array di archiviazione VSA Dell EMC Unity:** NetApp Arcserve UDP supporta snapshot hardware per il backup basato sull'agente (computer fisici Windows) e per il backup senza agente basato sull'host (Hyper-V).

Come procedere

- Utilizzo della snapshot hardware per il backup senza agente VMware
- Utilizzo della snapshot hardware per il backup senza agente Hyper-V
- Utilizzo di una snapshot hardware per il backup basato sull'agente
- Verifica dell'utilizzo di una snapshot hardware da parte del backup

Utilizzo della snapshot hardware per il backup senza agente VMware

Effettuare le operazioni seguenti:

1. Verificare che siano soddisfatti i prerequisiti seguenti:

   Snapshot NetApp

   - Arcserve UDP supporta i LUN NetApp iSCSI//FC e le esportazioni di volumi NetApp NFS configurate come archivi dati. iSCSI, FC ed NFS devono soddisfare determinate condizioni per l'utilizzo delle snapshot hardware.

     Considerazioni sul supporto NetApp iSCSI/FC per VMware

     Considerazioni sul supporto NFS per VMware

   - Per creare una snapshot hardware per VMware, aggiungere l'array di archiviazione alla console. Per ulteriori informazioni sull'aggiunta di un array di archiviazione, consultare la sezione Aggiunta di un array di archiviazione.
   - Per utilizzare la snapshot hardware, è consigliata la licenza FlexClone per gli array di archiviazione NetApp in esecuzione con Data ONTAP in modalità 7-Mode e Cluster.

   Note: per ulteriori informazioni sulla configurazione di NetApp, consultare la relativa documentazione o contattare il team del supporto tecnico di NetApp.

   Snapshot hardware HPE 3PAR:

   - Per supportare la snapshot hardware del computer virtuale VMware, HP RMC deve gestire l'array di archiviazione 3PAR HPE.
   - L'array di archiviazione deve disporre della licenza di copia virtuale.

     Protocolli supportati per le snapshot hardware di VMware: FC e iSCSI
   - Per creare una snapshot hardware per VMware, aggiungere l'array di archiviazione alla console. Per ulteriori informazioni sull'aggiunta di un array di archiviazione, consultare la sezione Aggiunta di un array di archiviazione.

   Snapshot hardware Nimble:

   - Protocolli supportati per le snapshot hardware di VMware: FC e iSCSI
   - Per creare una snapshot hardware per VMware, aggiungere l'array di archiviazione alla console. Per ulteriori informazioni sull'aggiunta di un array di archiviazione, consultare la sezione Aggiunta di un array di archiviazione

Considerazioni sull'archiviazione Nimble quando è abilitata l'autenticazione CHAP

2. Accedere alla console e creare un piano di backup.

   Nota: per ulteriori informazioni sulla creazione di un piano di backup senza agente, consultare la sezione Creazione di un piano di backup senza agente basato su host.

3. Verificare che sia selezionata l'opzione **Utilizza snapshot hardware se possibile** nella scheda **Avanzate**.

   Nota: per eseguire il backup solo da una snapshot hardware (non da una snapshot software), Arcserve UDP fornisce la seguente chiave del Registro di sistema: *FallbackToSWSnapshot =0(dword)*

   È possibile applicare tale chiave del Registro di sistema sia a un nodo specifico, sia a tutti i nodi.

   - Per applicarla a un nodo specifico, creare la chiave in HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\(Nodeid)

     Nota: (Nodeid) viene creato solo dopo che è stato eseguito un backup.

   - Per applicarla a tutti i nodi, creare la chiave in HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Importante: Se la sottochiave *AFBackupDll* non è disponibile, aggiungerla manualmente sotto Engine, come Engine\AFBackupDll\, quindi aggiungere *DWORD FallbackToSWSnapshot* sotto *AFBackupDll*.

4. **Salvare il piano e inviare il processo di backup.**

   Il processo di backup viene eseguito mediante la snapshot hardware.

Considerazioni sul supporto NetApp iSCSI/FC per VMware

Arcserve UDP supporta le snapshot hardware per i computer virtuali VMware solo se l'array di archiviazione sottostante è NetApp.

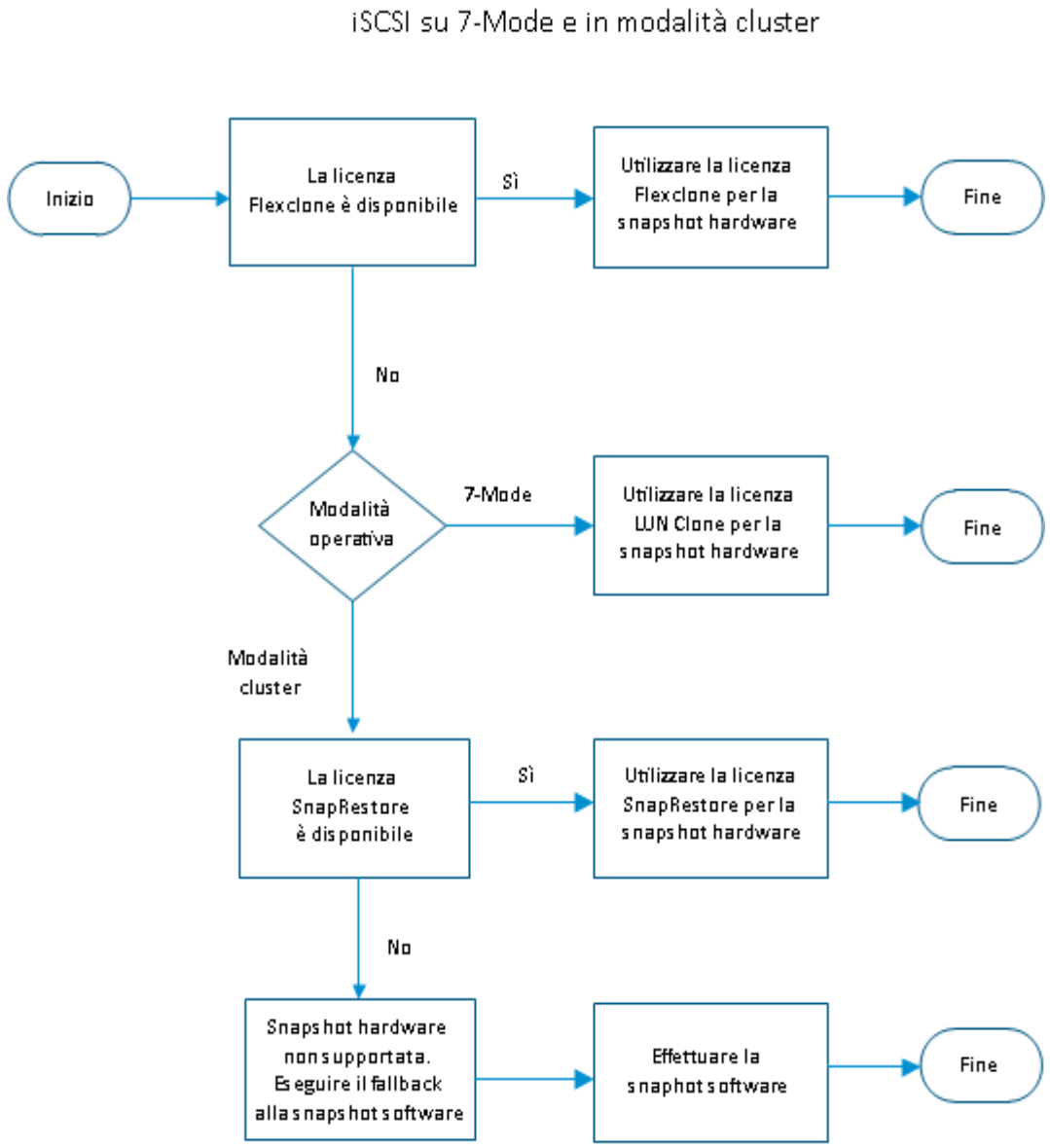
NetApp in modalità 7-mode

Se il sistema di archiviazione NetApp funziona in modalità 7-mode, non è necessario installare ulteriori licenze per l'utilizzo delle snapshot hardware. Tuttavia, è consigliabile che sia installata la licenza FlexClone.

NetApp in modalità Cluster

Se il sistema di archiviazione NetApp funziona in modalità Cluster (C-mode), è necessario disporre di una licenza FlexClone o SnapRestore per l'utilizzo delle snapshot hardware.

Il diagramma seguente illustra le condizioni applicate alla snapshot hardware per VMware NetApp iSCSI/FC:



Limitazione di un clone LUN

In un clone LUN tradizionale, a volte non è possibile eliminare la snapshot di backup durante le operazioni di pulitura. In genere, un LUN è presente come file nel file system. La snapshot permette di acquisire il file. Quando si crea un clone LUN, viene creato un altro file nel file system. Pertanto, la snapshot successiva acquisirà il file originale e il duplicato. In caso di più snapshot, il clone LUN rientra nella catena di snapshot. A questo punto, se si elimina una snapshot, questa non viene eliminata perché fa riferimento a un clone LUN che, a sua volta, si basa su un'altra snapshot. In questi casi, non è possibile eliminare una snapshot se prima non si eliminano il clone LUN e tutte le snapshot che fanno riferimento a tale clone LUN. Di conseguenza, il criterio di memorizzazione per le snapshot pianificate potrebbe essere danneggiato.

Per evitare questa situazione, installare la licenza FlexClone sul sistema di archiviazione NetApp in modo che Arcserve UDP utilizzi la tecnologia FlexClone per la clonazione LUN.

Chiavi del Registro di sistema per SnapRestore

Quando si utilizza la licenza SnapRestore, il ripristino LUN richiede molto tempo a seconda delle dimensioni del LUN e dell'ambiente. Ciò avviene perché l'eliminazione di una snapshot richiede più tempo se occupata con il ripristino LUN, che richiede più tempo. Arcserve UDP non dispone di un meccanismo per monitorare l'avanzamento del ripristino LUN. Pertanto, Arcserve UDP esegue vari tentativi per eliminare la snapshot.

Arcserve UDP fornisce due chiavi del Registro di sistema (**DeleteRetryTimeoutInMins** e **DeleteRetryCount**) utilizzabili per migliorare le prestazioni di eliminazione delle snapshot a seconda delle dimensioni del LUN e dell'ambiente. Le chiavi del Registro di sistema sono disponibili al percorso seguente:

SOFTWARE\Arcserve\Unified Data Protection\Engine

DeleteRetryTimeoutInMins

Specifica la durata del timeout (in minuti) per eliminare una snapshot. Se si dispone soltanto della licenza SnapRestore e non di FlexClone, è probabile che l'eliminazione delle snapshot richieda molto tempo. È possibile utilizzare la chiave del Registro di sistema per specificare i valori personalizzati. Tuttavia, è consigliabile utilizzare la licenza FlexClone.

Ad esempio, se la durata del timeout è di due minuti, l'agente UDP attende due minuti perché NetApp elimini la snapshot prima di inviare il comando di eliminazione all'array di archiviazione NetApp nel tentativo successivo. Questa chiave del Registro di sistema viene utilizzata con la chiave **DeleteRetryCount**.

Valore predefinito: 1 (in minuti)

Tipo: REG_SZ

DeleteRetryCount

Specifica il numero di tentativi per eliminare una snapshot.

Ad esempio, se il numero di tentativi è cinque, l'agente UDP tenterà per cinque volte di inviare il comando di eliminazione snapshot all'array di archiviazione NetApp. Esauriti i cinque tentativi per inviare il comando di eliminazione snapshot, se la snapshot è ancora presente, occorre eliminarla manualmente e aumentare il numero di tentativi in modo appropriato per non riscontrare lo stesso problema nel backup successivo. Questa chiave del

Registro di sistema viene utilizzata con la chiave **DeleteRetryTimeoutInMins**.

Valore predefinito: 30

Tipo: REG_SZ

Chiavi di registro per la disattivazione della prenotazione di spazio Lun

Quando viene eseguito il clone Lun durante il backup mediante la snapshot hardware, la prenotazione dello spazio viene ereditata per impostazione predefinita dal Lun di origine. Arcserve UDP fornisce una chiave di registro che consente di disattivare la prenotazione di spazio. La chiave di registro è disponibile nel percorso seguente:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

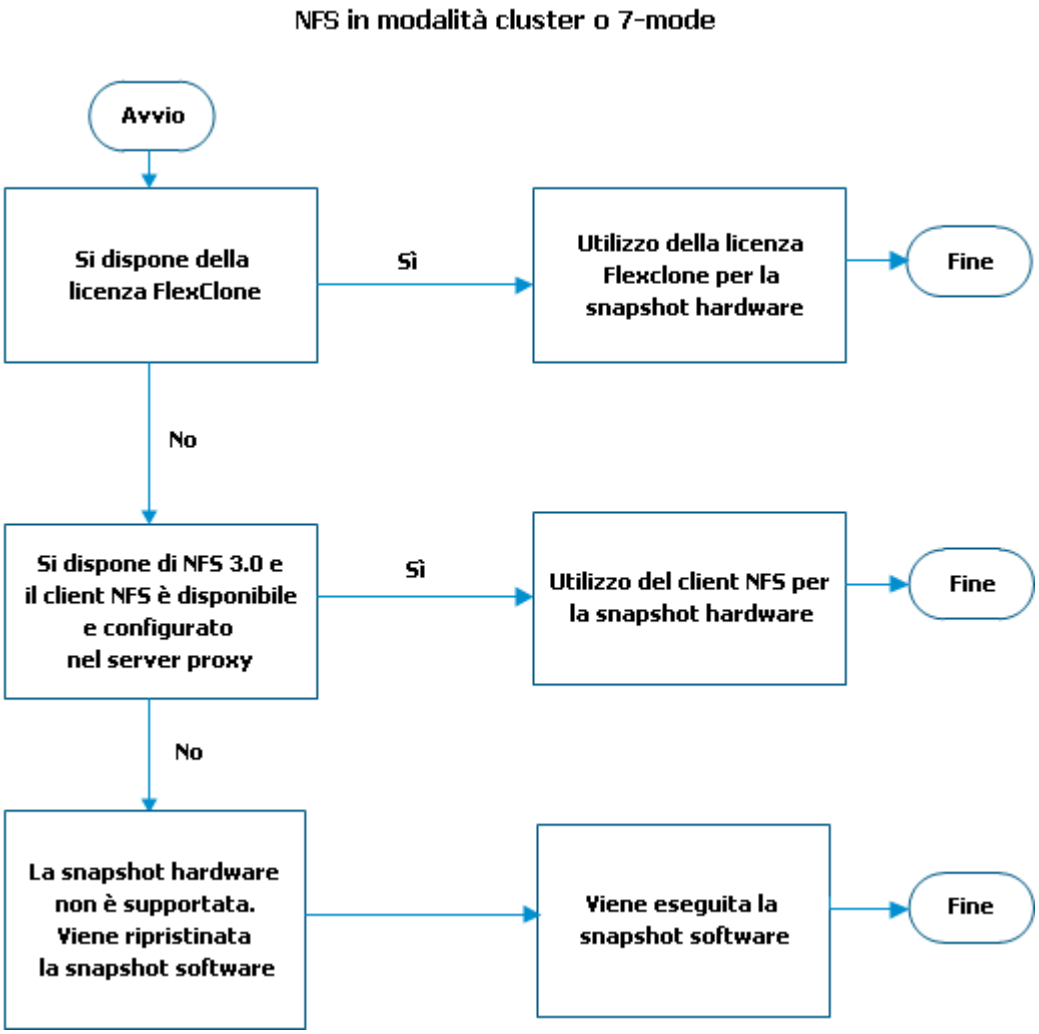
DisableLunSpaceReservation =1

Specifica che le prenotazioni di spazio Lun sono disattivate.

Nota: questa opzione è valida solo quando viene applicata la licenza FlexClone.

Considerazioni sul supporto NFS per VMware

Il diagramma seguente illustra le condizioni applicate alla snapshot hardware per VMware NFS NetApp:



Arcserve UDP supporta la snapshot hardware per gli archivi dati con NFS Versione 3.0. Per utilizzare la snapshot hardware, è necessario che sul proxy di backup sia installato e configurato il client Microsoft NFS.

La tabella seguente mostra le versioni di NFS supportate dal computer virtuale VMware e da Arcserve UDP. Accertarsi di disporre della versione di NFS corretta con la versione di VMware corrispondente.

Versioni VMware	Versioni di NFS supportate da VMware	Versioni di NFS supportate da Arcserve UDP per la snapshot hardware per FlexClone	Versioni di NFS supportate da Arcserve UDP per la snapshot hardware per il client Windows NFS
VMware 6.0 e	Supporta NFS	Supporta NFS 3.0 e 4.1	Supporta solo NFS 3.0 e deve

versioni successive	3.0 e 4.1		soddisfare i prerequisiti
Versioni di VMware precedenti alla 6.0	Supporta solo NFS 3.0	Supporta NFS 3.0	Supporta solo NFS 3.0 e deve soddisfare i prerequisiti

Prerequisito per NFS 3.0

- Se la licenza FlexClone non è presente, per il supporto della snapshot hardware dei file VMDK ospitati su un archivio dati con NFS 3.0, è necessario che sul dispositivo NetApp siano installate le seguenti versioni di OnTAP:
  - Sono supportati tutti i sistemi 7-Mode di Data ONTAP.
  - Sono supportate le release in cluster di Data ONTAP 8.2 a partire dalla release 8.2.3. Inoltre, sono supportate le release in cluster di Data ONTAP 8.3 a partire dalla release 8.3.1
  - Per impostazione predefinita, il supporto del client Windows NFS v3 è disabilitato. Per abilitarlo sui computer virtuali di archiviazione (SVM), utilizzare il comando seguente:

  vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled

- È necessario che il client Microsoft NFS sia installato e configurato sul proxy di backup che esegue il backup del computer virtuale VMware. Il proxy di backup deve disporre dell'accesso alla condivisione NFS. Per installare manualmente il client NFS sul server, consultare la sezione Installazione manuale del client Microsoft NFS su un server Windows.
- In seguito alla distribuzione del piano di backup senza agente, è necessario riavviare il servizio del client Microsoft NFS sul server proxy. È necessario riavviare soltanto una volta il servizio al primo utilizzo, in quanto la distribuzione del piano attiva sul server proxy alcune modifiche relative al client NFS.

Installazione manuale del client Microsoft NFS su un server Windows

Attenersi alla seguente procedura per installare manualmente il client Microsoft NFS su un server Windows.

1. Accedere al server Windows.
2. Aprire Server Manager e fare clic su Gestisci.
3. Fare clic su Aggiungi ruoli e funzionalità.
4. Nella finestra di dialogo Prima di iniziare, fare clic su Avanti.
5. Nella finestra di dialogo Seleziona tipo di installazione, scegliere Installazione basata su ruoli o basata su funzionalità, quindi fare clic su Avanti.
6. Nella finestra di dialogo Selezione server di destinazione, se l'installazione avviene nel server locale, fare clic su Avanti. Altrimenti, selezionare un server dall'elenco Pool di server.
7. Nella finestra di dialogo Selezione ruoli server, fare clic su Avanti.
8. Nella finestra di dialogo Selezione funzionalità, scorrere l'elenco delle funzionalità disponibili e selezionare la casella di controllo Client per NFS.
9. Fare clic su Avanti.
10. Nella finestra di dialogo Conferma selezioni per l'installazione, rivedere le selezioni e fare clic su Installa.
11. Al termine dell'installazione, controllare i risultati e fare clic su Chiudi.

Considerazioni sull'archiviazione Nimble quando è abilitata l'autenticazione CHAP

È possibile eseguire il backup della snapshot hardware quando è abilitata l'autenticazione CHAP per l'archiviazione Nimble.

Nota: L'autenticazione CHAP non è supportata su ESXi 5.0 poiché la versione di ESXi non dispone di SQLite.

È necessario completare i prerequisiti seguenti:

Prerequisiti

Importante: I prerequisiti si applicano solo se si desidera che il processo di backup senza agente basato su host utilizzi la modalità di trasporto SAN.

- Abilitare SSH su cui archiviazione Nimble è configurato con autenticazione CHAP ESXi.
- Verificare se il computer proxy presenta l'interfaccia della riga di comando iscsicli necessaria per configurare le periferiche di destinazione iSCSI.
- Impostare il criterio di esecuzione RemoteSigned sul computer proxy per eseguire gli script Powershell. Utilizzare il comando seguente:

  Set-ExecutionPolicy RemoteSigned
- Salvare le credenziali ESXi tramite uno script Powershell per cui è configurata l'archiviazione Nimble con autenticazione CHAP.

  Per salvare le credenziali ESXi, attenersi alla procedura seguente:

  - Eseguire lo script Powershell "StoreESXCredentials.ps1" da Powershell sul proxy.

    Viene richiesto di immettere i dettagli su indirizzo IP, nome utente e password.
  - Immettere i tre parametri.

    Le credenziali vengono archiviate nel file CSV "ESXCredentials.csv" e la password viene crittografata.

  Per individuare lo script Powershell, attenersi alla seguente procedura:

  - Accedere al computer proxy e aprire Powershell.
  - Accedere alla directory seguente:

    Nota: Il percorso viene cambiato in base alla directory di installazione.

    C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN

- Eseguire lo script Powershell come indicato di seguito:

  PS C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN> .\StoreESXCredentials.ps1

Utilizzo della snapshot hardware per il backup senza agente Hyper-V

Importante: il backup senza agente di Hyper-V utilizza snapshot hardware solo quando tutti i dischi del computer virtuale si trovano su volumi compatibili con le snapshot hardware. In caso contrario, il backup utilizza snapshot software.

Effettuare le operazioni seguenti:

1. Verificare che siano soddisfatti i prerequisiti seguenti.
   - Installare un provider hardware VSS (ad esempio, NetApp) sui server Hyper-V. Per supportare la snapshot trasportabile, installare il provider hardware VSS sul server proxy di backup. La configurazione tipica di un provider hardware VSS include:
     - Definizione di un server che controlla la LUN
     - Definizione delle credenziali dell'array di dischi per accedere all'array di dischi

     Nota: per ulteriori informazioni sulla configurazione del provider di hardware VSS, contattare il rivenditore del provider hardware.
   - Il server Hyper-V e il server proxy devono disporre di una versione del sistema operativo simile.
   - Se il server Hyper-V è compreso in un cluster, il server proxy non deve far parte del cluster Hyper-V.
2. Accedere alla console e creare un piano di backup.

   Nota: per ulteriori informazioni sulla creazione di un piano di backup senza agente, consultare la sezione Creazione di un piano di backup senza agente basato su host.
3. Verificare che sia selezionata l'opzione **Utilizza snapshot hardware se possibile** nella scheda **Avanzate**.

   Nota: per eseguire il backup solo da una snapshot hardware (non da una snapshot software), Arcserve UDP fornisce la seguente chiave del Registro di sistema: *FallbackToSWSnapshot =0(dword)*

   È possibile applicare tale chiave del Registro di sistema sia a un nodo specifico, sia a tutti i nodi.
   - Per applicarla a un nodo specifico, creare la chiave in HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\(Nodeid)

     Nota: (Nodeid) viene creato solo dopo che è stato eseguito un backup.

- Per applicarla a tutti i nodi, creare la chiave in HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

Importante: Se la sottochiave *AFBackupDll* non è disponibile, aggiungerla manualmente sotto Engine, come Engine\AFBackupDll\, quindi aggiungere *DWORD FallbackToSWSnapshot* sotto *AFBackupDll*.

4. **Salvare** il piano e **inviare** il processo di backup.

   Il processo di backup viene eseguito mediante la snapshot di archiviazione.

Utilizzo della snapshot hardware per il backup basato sull'agente

Effettuare le operazioni seguenti:

1. Verificare che siano soddisfatti i prerequisiti seguenti:
   - Installare un provider hardware VSS in grado di supportare la snapshot hardware sugli agenti Arcserve UDP. La configurazione tipica di un provider hardware VSS include:
     - Definizione di un server che controlla la LUN.
     - Definizione delle credenziali dell'array di dischi per accedere all'array di dischi.

     Nota: Per ulteriori informazioni sulla configurazione del provider di hardware VSS, contattare il rivenditore del provider hardware.
2. Accedere alla console e creare un piano di backup.

   Nota: Per ulteriori informazioni sulla creazione di un piano senza agente per Windows, consultare la sezione Creazione di un piano di backup di Windows.
3. Verificare che sia selezionata l'opzione **Utilizza snapshot hardware se possibile** nella scheda **Avanzate**.
4. Salvare il piano e inviare il processo di backup.

   Il processo di backup viene eseguito mediante la snapshot di archiviazione.

Verifica del backup completato utilizzando la snapshot hardware

Se non vengono soddisfatti i prerequisiti per la snapshot hardware, Arcserve UDP passerà automaticamente a una snapshot software senza interrompere il processo di backup. In caso di errore della snapshot hardware, l'evento viene registrato nei registri delle attività.

Rivedere i messaggi di registro per verificare che il backup abbia utilizzato la snapshot hardware.

Effettuare le operazioni seguenti:

1. Accedere al seguente percorso:

   <Installation folder>\Arcserve\Unified Data Protection\Engine\Logs

2. Aprire il file corrispondente per l'ID di processo corrispondente.

   Ad esempio, se l'ID di processo è JW002, accedere alla cartella **Registri** e aprire il file JW002.

3. Rivedere i messaggi nel file per confermare se il backup ha utilizzato la snapshot di archiviazione.

   La snapshot di archiviazione è stata utilizzata correttamente per il backup.

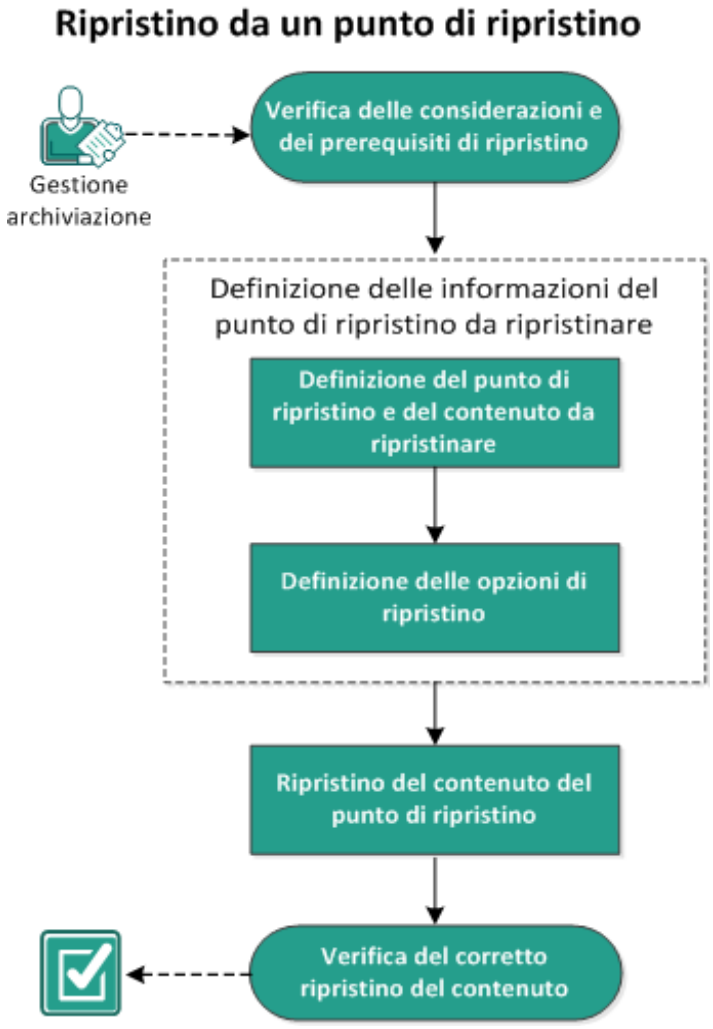
Chapter 13: Ripristino dei dati protetti

La presente sezione descrive i seguenti argomenti:

Ripristino da un punto di ripristino

Ogni volta che un backup di Arcserve UDP viene completato correttamente, viene creata un'immagine snapshot temporizzata del backup (punto di ripristino). L'insieme dei punti di ripristino consente di individuare e specificare esattamente le immagini di backup da ripristinare. Inoltre, se si ritiene che le informazioni di backup sono mancanti, corrotte o non affidabili, è possibile individuare ed eseguire il ripristino da una versione precedente attendibile.

Il diagramma seguente mostra il processo di ripristino da un punto di ripristino:



Per eseguire il ripristino da un punto di ripristino, effettuare le seguenti attività:

1. Verifica delle considerazioni e dei prerequisiti di ripristino
2. Definizione delle informazioni del punto di ripristino da ripristinare
    a. Definizione del punto di ripristino e del contenuto da ripristinare
    b. Definizione delle opzioni di ripristino

3. Ripristino del contenuto del punto di ripristino
4. Verifica del corretto ripristino del contenuto

Verifica delle considerazioni e dei prerequisiti di ripristino

Verificare i seguenti prerequisiti prima di procedere al ripristino:

- È necessario disporre di almeno un punto di ripristino per il ripristino.
- È necessario disporre di una destinazione valida e accessibile da cui eseguire il ripristino del contenuto del punto di ripristino.
- È necessario disporre di una posizione di destinazione valida e accessibile dove eseguire il ripristino del punto di ripristino.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Verificare le seguenti considerazioni sul ripristino:

- Se il ripristino viene eseguito su una destinazione remota e tutte le unità (A - Z) sono occupate, non sarà possibile eseguire il ripristino su posizione remota. L'agente Arcserve UDP (Windows) deve utilizzare una lettera di unità per eseguire il montaggio del percorso di destinazione remoto.
- (Facoltativo) Comprendere il funzionamento del processo di ripristino. Per ulteriori informazioni, consultare la sezione Funzionamento del ripristino a livello di file.
- (Facoltativo) Rivedere i file ignorati durante il ripristino. Per ulteriori informazioni, consultare la sezione File ignorati durante il ripristino.
- Quando si esegue il ripristino di una sessione di backup ottimizzata su un volume non vuoto (ripristino non ottimizzato), il processo di ripristino potrebbe richiedere più tempo del tempo previsto visualizzato nel monitoraggio dei processi. La quantità di dati elaborata e il tempo trascorso potrebbero aumentare in base ai dati ottimizzati sul volume.

Esempio:

La dimensione del volume di backup è 100 GB. In seguito all'ottimizzazione, la dimensione del volume viene ridotta a 50 GB.

Quando si esegue un ripristino non ottimizzato del volume, il monitoraggio del processo di ripristino mostra 100% dopo aver ripristino 50 GB. Sarà tuttavia necessario più tempo per eseguire il ripristino dei 50 GB restanti.

- Il messaggio seguente del Registro attività viene visualizzato quando si ripristinano i file di sistema:

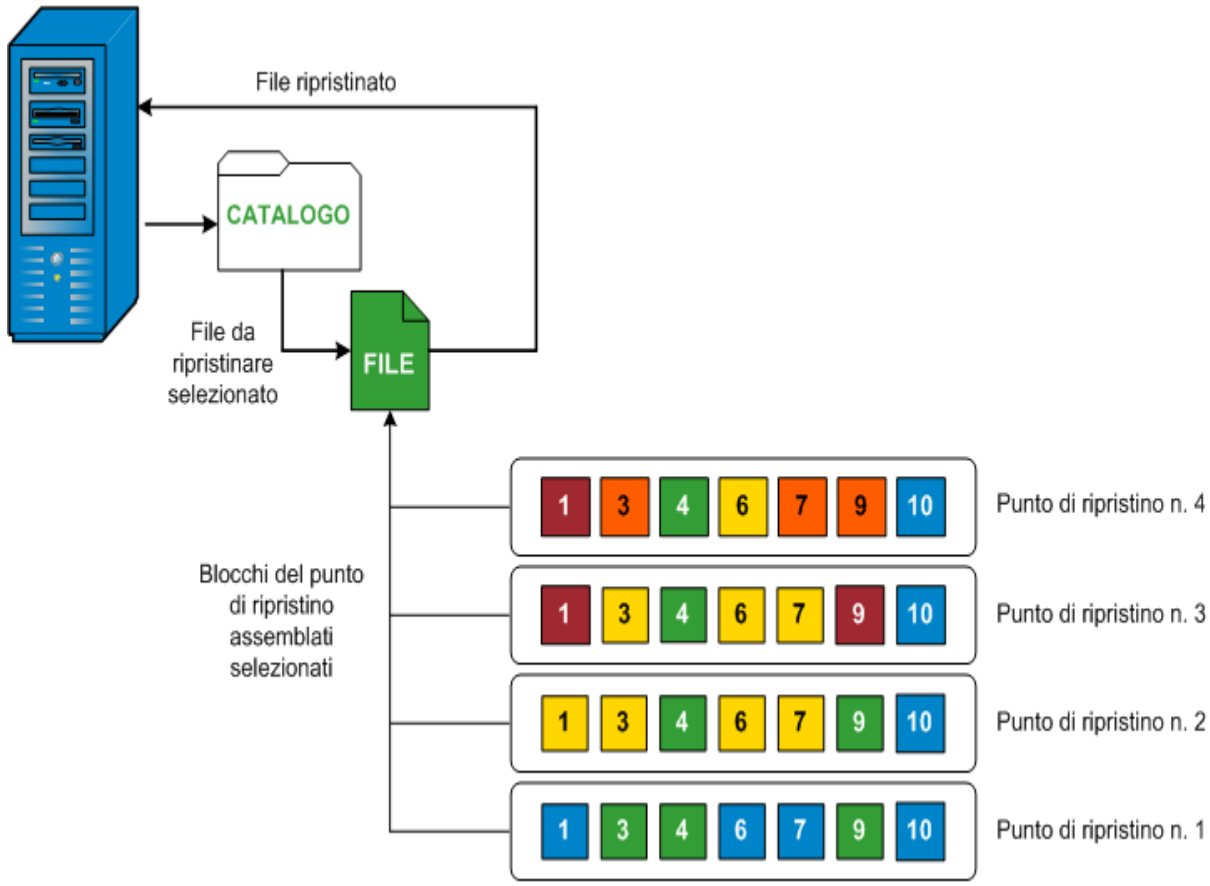
I file di sistema sono stati ignorati. Se necessario, è possibile utilizzare l'opzione di ripristino bare metal per eseguire il ripristino.

Funzionamento del ripristino a livello di file

Durante il processo di backup a livello di blocco, ciascun file di backup include un insieme di blocchi che definiscono tale file. Il file di catalogo creato contiene un elenco dei file di backup, i singoli blocchi utilizzati per ciascun file e i punti di ripristino disponibili per tali file. Nel caso in cui sia necessario ripristinare un file specifico, è possibile individuare il file che si desidera ripristinare e il punto di ripristino che si desidera utilizzare. Arcserve UDP esegue la raccolta della versione dei blocchi utilizzati per il punto di ripristino del file specificato, li riassembla ed esegue il ripristino del file.

Nota: È anche possibile eseguire un ripristino senza un file di catalogo da un punto di ripristino di backup senza catalogo.

Nel seguente diagramma di flusso è possibile visualizzare il processo di ripristino di un file specifico in Arcserve UDP:



File ignorati durante il ripristino

Durante un ripristino con l'agente Arcserve UDP (Windows), è possibile che alcuni file vengano ignorati intenzionalmente.

I file e le cartelle nella tabella seguente vengono ignorati durante il ripristino se si verificano le due condizioni seguenti:

- I file vengono ignorati se esistono prima del ripristino e l'opzione di conflitto è Ignora file esistenti.
- I file e le cartelle elencati nella tabella seguente vengono ignorati poiché non costituiscono un componente importante di Windows o dell'agente Arcserve UDP (Windows).

Sistema operativo	Cartella o posizione	Nome di file o cartella	Note
Tutto	Cartella root di ciascun volume	CAVolTrc.dat	Utilizzato dal driver di rilevamento di Arcserve UDP.
		cavoltrcsnapshot.dat	
		System Volume Information*	Utilizzato per salvare file/cartelle con un sistema Windows, ad esempio file di copia shadow del volume.
		RECYCLER*	Utilizzato solamente su partizioni NTFS. Contiene un cestino per ogni utente che accede al computer, ordinato in base al rispettivo ID di sicurezza (SID).
		$Recycle.Bin*	Quando si elimina un file da Gestione risorse o da Risorse del computer, il file viene archiviato nel cestino finché non si svuota il cestino o si ripristina il file.
	Qualsiasi cartella con file di immagini	Thumbs.db	Archivia le immagini di anteprima per la visualizzazione Anteprima di Esplora risorse.
	Cartella root del volume	PageFile.Sys	File di scambio per la memoria virtuale di Windows.
		Hiberfil.sys	File per l'ibernazione usato per salvare i dati di sistema quando si attiva la modalità di ibernazione.

I file e le cartelle seguenti vengono ignorati soltanto quando si esegue il ripristino nella posizione originale o in una posizione alternativa:

Sistema	Cartella o posizione	Nome di file o cartella	Nota

ope-rativo			
Tutto	Cartella specificata nel record di valore in: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Tutti i file/cartelle (in modo ricorsivo)	La cartella contiene un file .dll memorizzato nella cache che viene utilizzato per il controllo dei file di sistema (SFC). I contenuti della directory di cache dll di sistema vengono ricostruiti mediante SFC.
	%SystemRoot%\SYSTEM32\dllCache		
	Cartella principale di quorum_device	MSCS*	Utilizzato per Microsoft Cluster Server.

	%SystemRoot%\SYSTEM32\	perf?00?.dat	Dati relativi alle prestazioni utilizzati dal contatore delle prestazioni di Windows.

		perf?00?.bak	

		CATROOT*	Utilizzato per le firme digitali dei record Protezione file Windows (WFP) installati nel sistema operativo (ad esempio DLL, EXE, SYS, OCX e così via) per evitare che siano eliminati o sostituiti con versioni precedenti.
	%SystemRoot%\inetsrv\	metabase.bin	File binario metabase delle versioni di IIS precedenti alla 6.0.
	File o cartella specificato nel valore eccetto l'Archivio comune SIS in HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup	Tutti i file/cartelle (in modo ricorsivo)	I file e le cartelle non devono essere sottoposti a backup e ripristino. Per ulte-

			riori informazioni, fare clic sul seguente collegamento.
XP W2003	Volume di sistema	NTLDR	Caricatore di avvio principale.
		BOOT.INI	Contiene la configurazione di avvio (se assente, il valore predefinito NTLDR sarà impostato su \Windows nella prima partizione del primo disco rigido).
		NTDETECT.COM	Richiesto per l'avvio del sistema operativo basato su NT. Rileva le informazioni hardware di base necessarie per il

			corretto avvio.
Vista e sistemi successivi	Cartella root del volume di sistema	boot*	Cartella di avvio per Windows.
		bootmgr	File di Windows Boot Manager.
		EFI\Microsoft\Boot*	Usata per l'avvio EFI.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Archivia i file di traccia ETW (estensione .etl) per le sessioni di traccia degli eventi in tempo reale.
		config\RegBack*	Backup della tabella del registro di sistema attuale.
Win8 e sistemi successivi	Volume di sistema	swapfile.sys	File del controller di sistema, in genere di circa 256 MB. Viene utilizzato da applicazioni come

			Metro che non si adattano alle caratteristiche di paging tradizionali (schema di utilizzo, crescita, spazio riservato) di pagefile.sys.
		BOOTNXT	Utilizzato per l'avvio da un sistema operativo diverso da Windows 8. Creato durante l'abilitazione delle opzioni di avvio e aggiornato da Windows.

Il Registro attività fornisce le seguenti informazioni:

- Informazioni di data e ora: File system jobxxxx ignorati. È possibile utilizzare l'opzione Ripristino bare metal (BMR) per ripristinarli.
- Informazioni di data e ora: File o directory jobxxxx ignorati. L'elenco dei file o delle directory ignorati è disponibile in: C:\Programmi\Arcserve\Unified Data Protection\Engine\Logs\Restore-<YYYYMMDD>-<hhmmss>-<Process ID>-<Job ID>.log.

Definizione delle informazioni del punto di ripristino da ripristinare

Arcserve UDP include un'opzione per il ripristino dei dati da un punto di ripristino. L'obiettivo di un processo di ripristino è quello di identificare rapidamente i dati necessari e di recuperarli dalla posizione di backup appropriata. Per ciascun processo di ripristino è richiesta un'origine e una destinazione.

Il processo per il ripristino da un punto di ripristino è il seguente:

1. Definizione del punto di ripristino e del contenuto da ripristinare
2. Definizione delle opzioni di ripristino

Definizione del punto di ripristino e del contenuto da ripristinare

In questa sezione vengono fornite informazioni su come specificare il punto di ripristino e il contenuto da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere alla finestra di dialogo per la selezione del metodo di ripristino in uno dei modi seguenti:

   Dalla console Arcserve UDP:

   a. Accedere alla console Arcserve UDP.

   b. Accedere a **Risorse** > **Nodo** > **Tutti i nodi**.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   c. Fare clic con il tasto destro del mouse sul nodo, quindi selezionare **Ripristino**.

      L'utente verrà indirizzato automaticamente alla console del nodo dell'agente e verrà visualizzata la finestra di dialogo Ripristino.

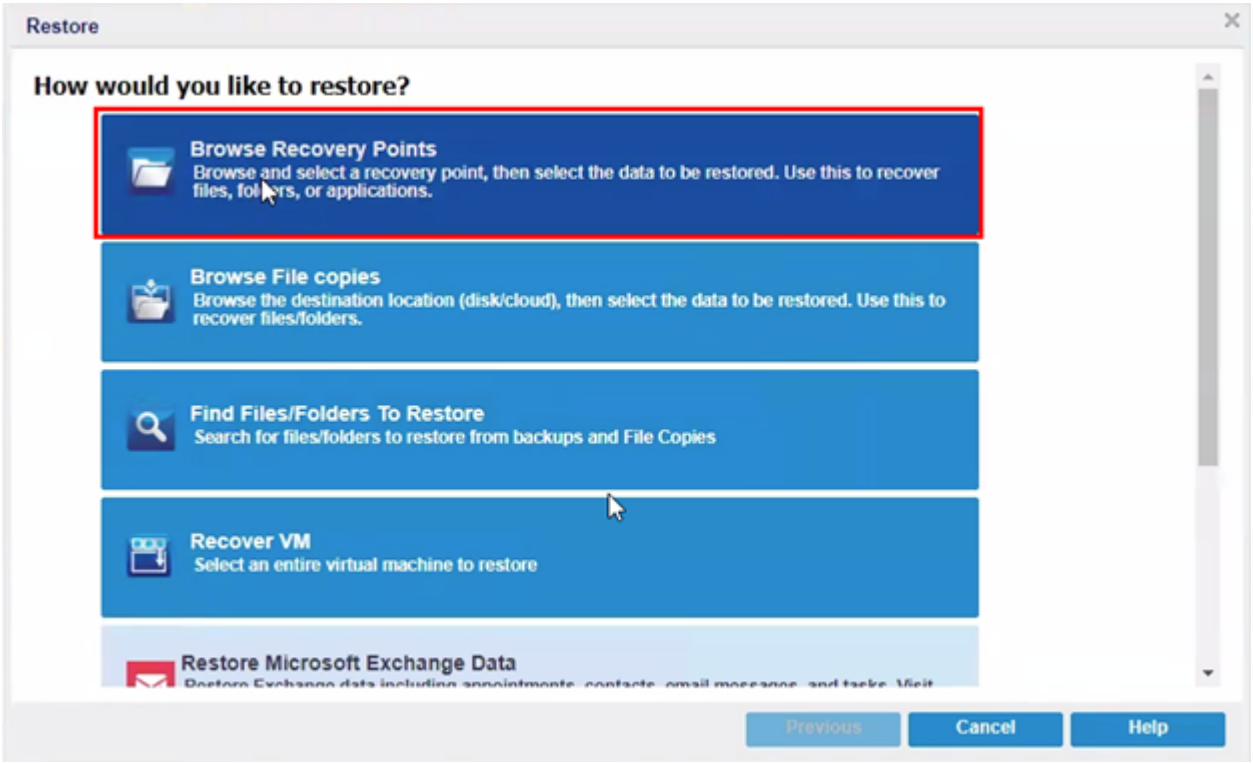
   Dall'agente Arcserve UDP (Windows):

   a. Accedere all'agente Arcserve UDP (Windows).

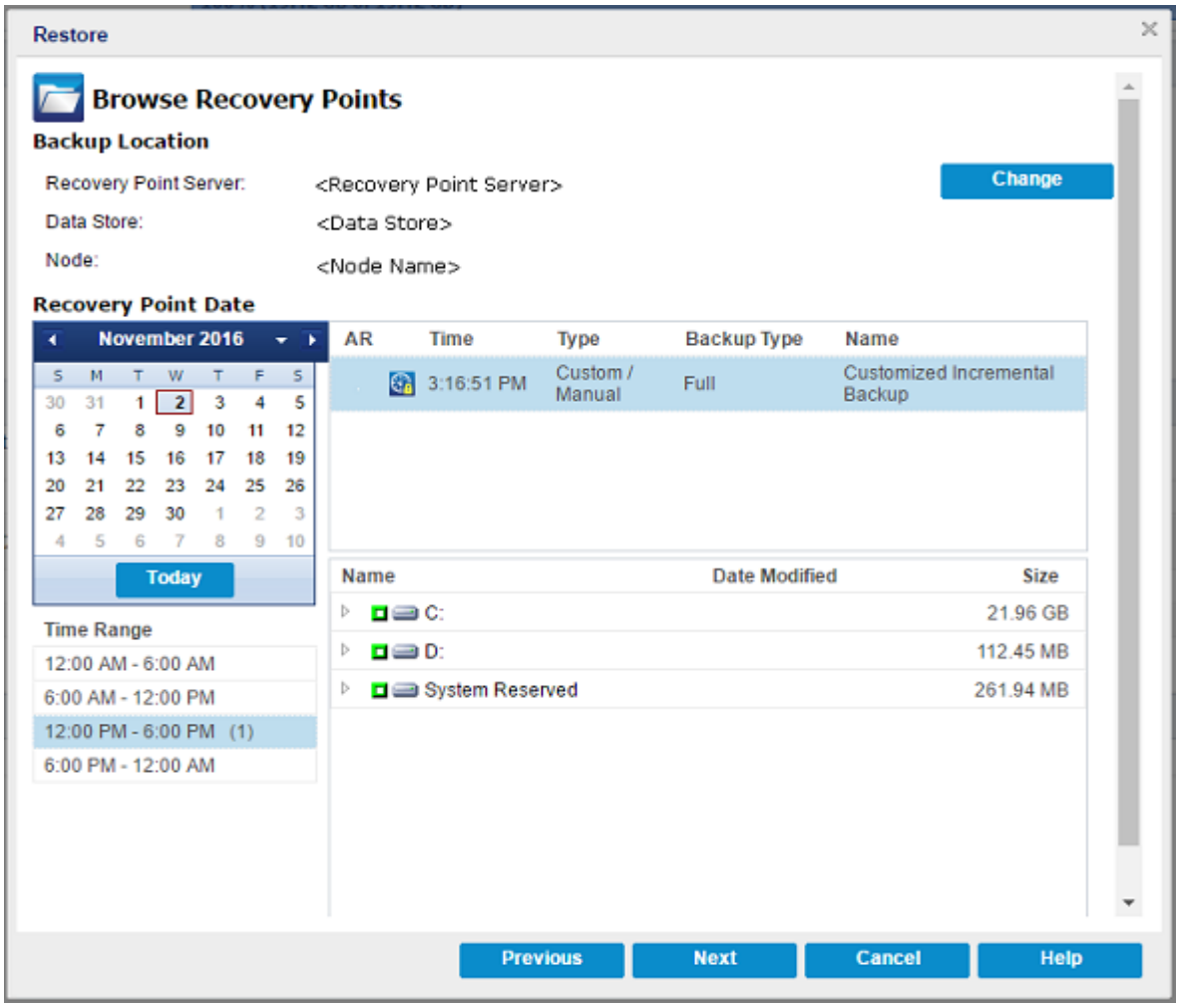
   b. Dalla pagina principale selezionare **Ripristino**.

      Verrà visualizzata la finestra di dialogo di ripristino.

2. Nella finestra di dialogo Ripristino, fare clic su **Sfoglia punti di ripristino**.



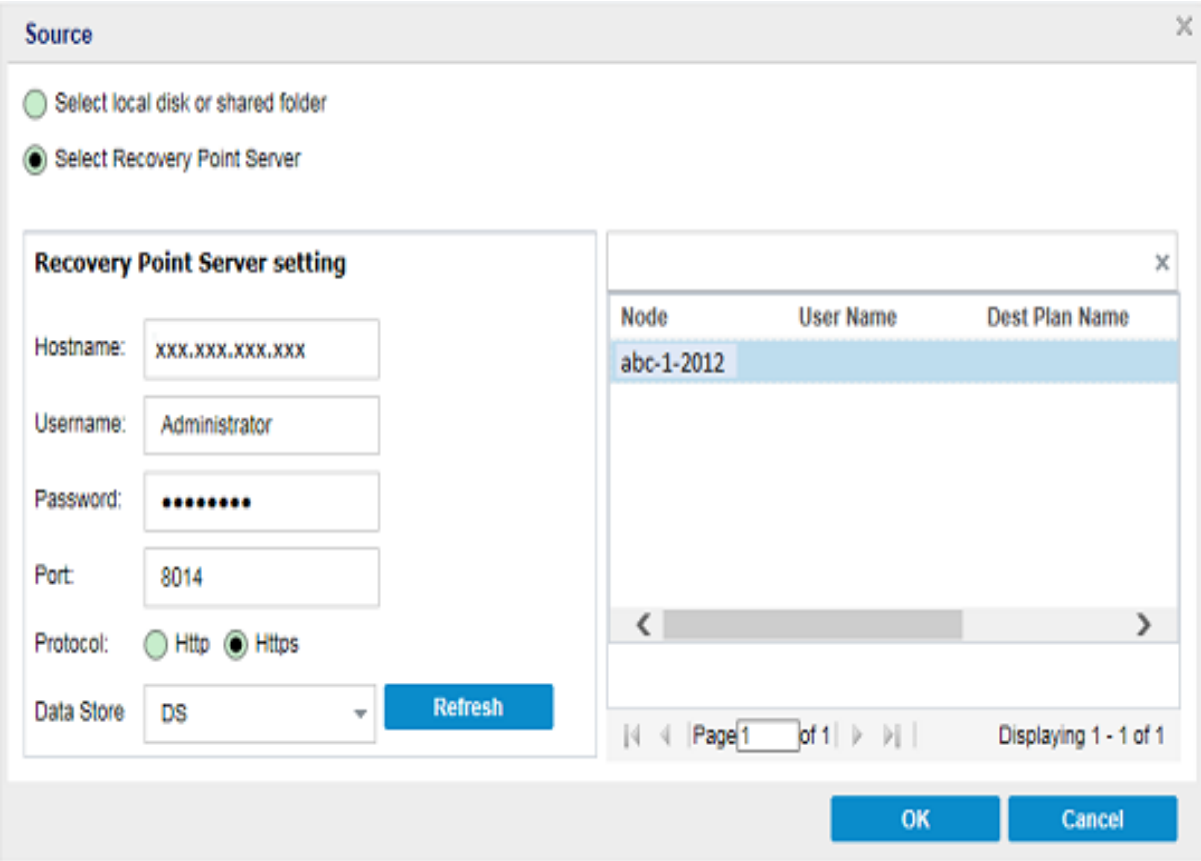
3. Nella pagina Sfoglia punti di ripristino, procedere come segue:



a. Per aggiornare la posizione di backup, fare clic su **Modifica**.

   Viene visualizzata la finestra di dialogo Origine.

b. Nella finestra di dialogo Origine, selezionare una delle seguenti posizioni di backup, quindi fare clic su **OK**:



Selezione di un disco locale o una cartella condivisa

1. Specificare o accedere al percorso di archiviazione delle immagini di backup e selezionare l'origine di backup appropriata.
2. Per verificare la connessione alla posizione specificata, fare clic sul pulsante con una freccia verde. Se necessario, immettere il nome utente e la password per poter accedere alla posizione di origine.

   Viene visualizzata la finestra di dialogo Selezionare la posizione di backup.
3. Selezionare la cartella di archiviazione dei punti di ripristino e fare clic su **OK**.

   La finestra di dialogo Selezionare la posizione di backup viene chiusa e la posizione di backup viene visualizzata nella finestra di dialogo Origine.

   I punti di ripristino vengono elencati nella finestra di dialogo Sfoglia punti di ripristino.

Selezione di un Recovery Point Server

1. Specificare i dettagli dell'impostazione Recovery Point Server e fare clic su **Aggiorna**.

   Tutti gli agenti vengono elencati nella colonna Data Protection Agent (Agente di protezione dati) nella finestra di dialogo Origine.

2. Selezionare l'agente dall'elenco visualizzato.

   I punti di ripristino vengono elencati nella finestra di dialogo Sfoglia punti di ripristino.

c. Selezionare la data dell'immagine di backup che si desidera ripristinare.

   Tutte le date contenenti punti di ripristino per l'origine di backup specificata sono evidenziate in verde.

   Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito (completo, incrementale o di verifica) e al nome del backup.

d. Selezionare un punto di ripristino da ripristinare.

   Viene visualizzato il contenuto di backup (incluse tutte le applicazioni) per i punti di ripristino selezionati.

   Nota: l'icona di un orologio con lucchetto indica che il punto di ripristino contiene informazioni crittografate e potrebbe richiedere una password per il ripristino.

e. Selezionare il contenuto da ripristinare.

   - Per un ripristino a livello di volume, è possibile scegliere di ripristinare l'intero volume oppure alcuni file/cartelle specifici.
   - Per un ripristino a livello di applicazione, è possibile scegliere di ripristinare l'intera applicazione o solo determinati componenti, database, istanze, ecc. dell'applicazione.

4. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

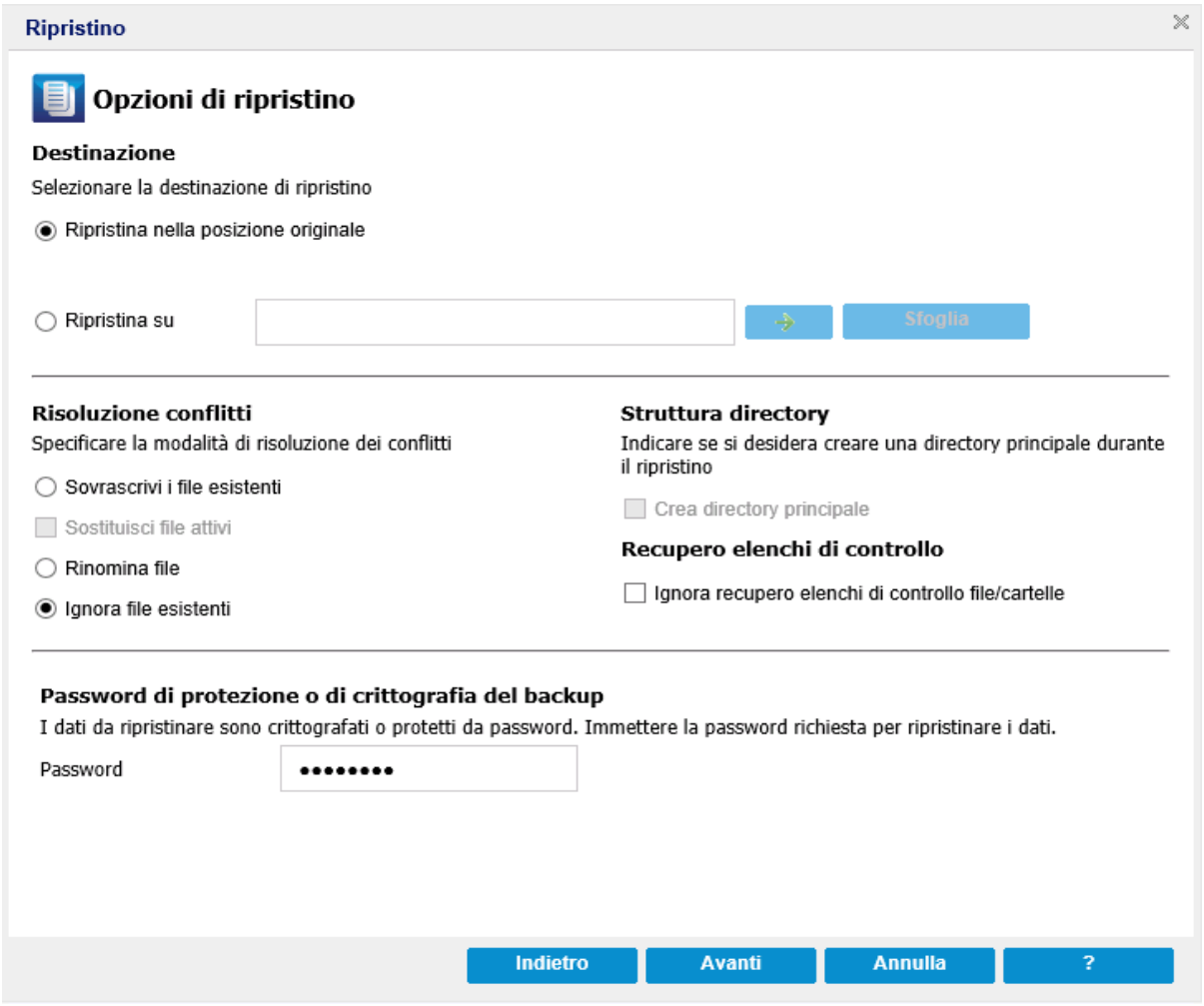
   Il punto di ripristino e il contenuto da ripristinare sono specificati.

Definizione delle opzioni di ripristino

Dopo avere specificato un punto di ripristino e il contenuto da ripristinare, definire le opzioni di copia per il punto di ripristino selezionato. La presente sezione descrive come definire le opzioni di ripristino per il punto di ripristino selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo Opzioni di ripristino, selezionare la destinazione di ripristino.



Le opzioni di destinazione disponibili sono:

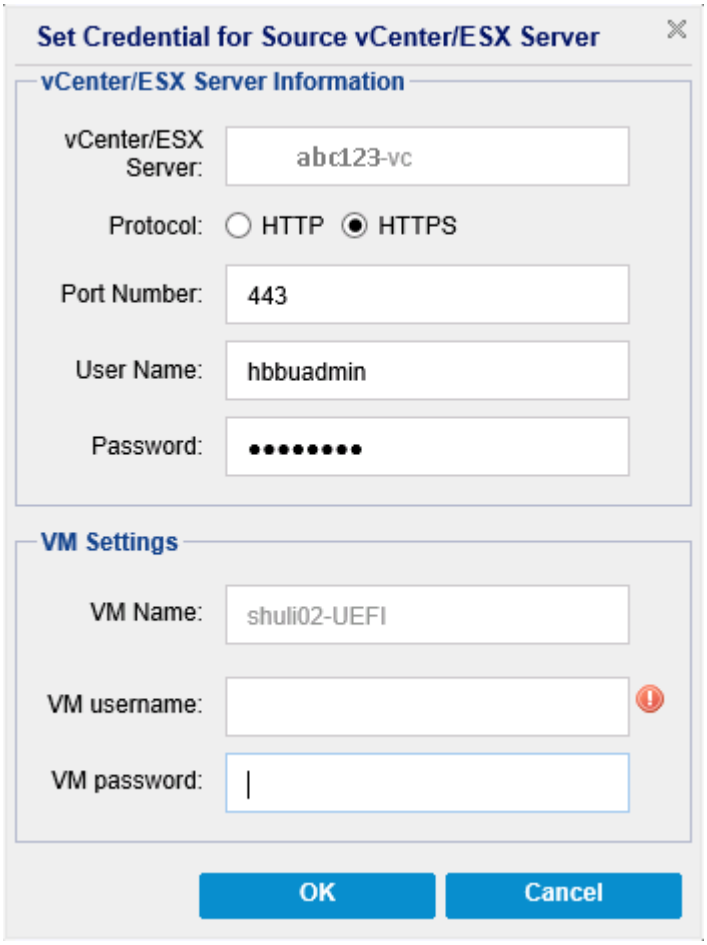
Ripristina in posizione originale

Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

Nota: se è stato eseguito il backup del punto di ripristino tramite il backup senza agente basato su host, per eseguire il ripristino sulla posizione originale

sarà necessario eseguire nuovamente il ripristino sul computer virtuale. In questo caso, viene visualizzata una finestra di dialogo. È possibile immettere le credenziali dell'hypervisor e il sistema operativo del computer virtuale.

Valido per il computer virtuale VMware:



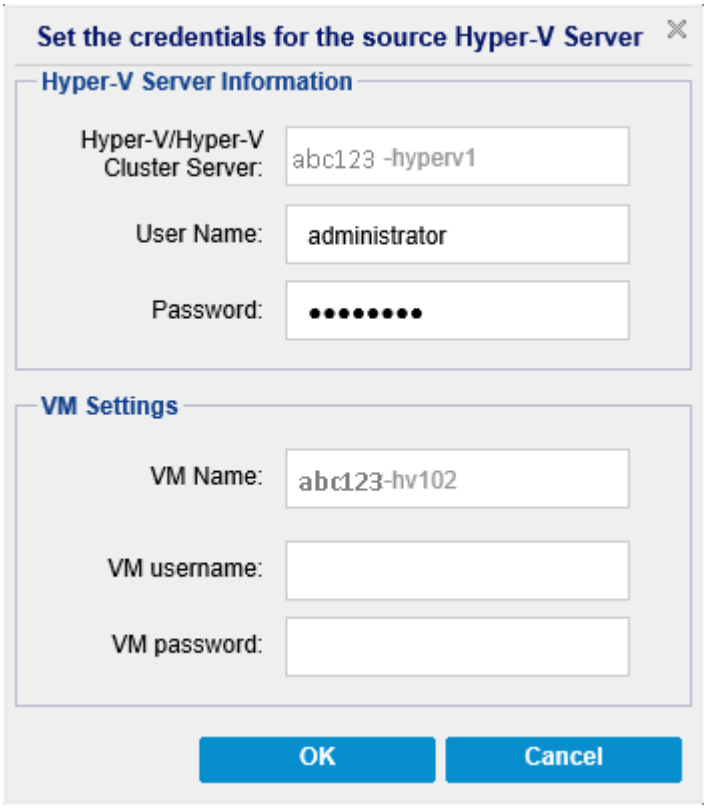
Nota: per poter creare o scrivere i file all'interno del computer virtuale, tenere conto dei requisiti seguenti per le impostazioni e l'autorizzazione dell'account del computer virtuale:

- Gli strumenti VMware vengono installati e sono in esecuzione.
- Il firewall deve consentire la condivisione di file e stampanti.
- L'account può appartenere all'amministratore locale integrato, all'amministratore di dominio integrato o al dominio appartenente al gruppo degli amministratori locali. Se vengono utilizzati altri account, procedere come segue:
  - Disabilitare l'accesso remoto a UAC. Per disabilitare l'accesso UAC remoto, consultare la sezione Importazione di computer virtuali con un account amministrativo aggiuntivo.

- Disabilitare l'UAC nel Local Security Policy disattivando l'impostazione di esecuzione di tutti gli amministratori nella modalità di approvazione dell'amministratore in secpol.msc -> Criteri locali -> Opzioni di protezione. (Secpol.msc è l'editor delle policy di protezione di Microsoft).

  Importante: Non disabilitare l'UAC nella finestra di dialogo Impostazioni di Controllo account utente accessibile dal pannello di controllo.

Per il computer virtuale Hyper-V:



Nota: per poter creare o scrivere i file all'interno del computer virtuale, tenere conto dei requisiti seguenti per le impostazioni e l'autorizzazione dell'account del computer virtuale:

- I servizi di integrazione Hyper-V devono essere installati e in esecuzione.
- Il firewall deve consentire la condivisione di file e stampanti.
- L'account può appartenere all'amministratore locale integrato, all'amministratore di dominio integrato o al dominio appartenente al gruppo degli amministratori locali. Se vengono utilizzati altri account, disattivare l'accesso remoto dell'UAC. Per disabilitare

l'accesso UAC remoto, consultare la sezione Importazione di computer virtuali con un account amministrativo aggiuntivo.

- Se il sistema operativo guest del computer virtuale è Windows versione Client (ad esempio, Windows 10), è necessario configurare manualmente il firewall per consentire Windows Management Instrumentation (WMI).

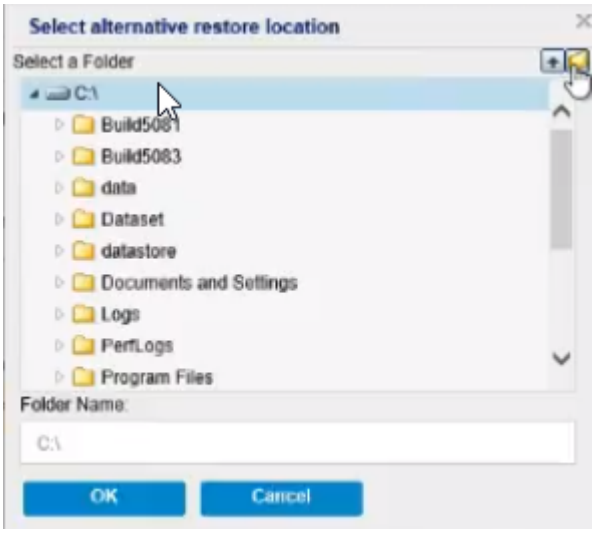
Ripristina su

Esegue il ripristino alla posizione specificata. Per eseguire il ripristino dei dati nella posizione originale, eseguire le seguenti operazioni:

- Per fornire la destinazione, fare clic su **Sfoglia**.

  Viene visualizzata la finestra di dialogo Seleziona posizione di ripristino alternativa.

- Selezionare la cartella esistente o crearne una nuova, se necessario, quindi fare clic su **OK**.



- Per verificare la connessione alla posizione specificata, fare clic sul pulsante con una freccia verde. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso.

2. (Facoltativo) Per abilitare la comunicazione tra l'agente Windows e il Recovery Point Server, selezionare la casella di controllo **Usa rete selezionata per il traffico di ripristino**, quindi selezionare la rete dall'elenco a discesa.

   Note:

   - se la rete di backup selezionata non è accessibile, per continuare il processo di backup con la rete disponibile o con la rete predefinita, fare clic sulla casella di controllo **Procedere con l'esecuzione del processo anche nel caso**

in cui sia impossibile stabilire la connessione alla rete di backup selezionata.

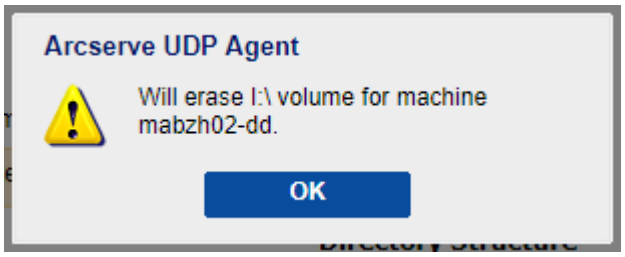
- Per definire i vincoli di SMB Multichannel in modo che i dati vengano trasferiti solo tramite la rete selezionata, selezionare la casella di controllo **Usa l'ethernet apposita se il computer corrente abilita SMB Multichannel**.

  Per impostazione predefinita, questa opzione non è disponibile. Per attivare questa opzione, creare la stringa *UseDedicatedEthernet* nel seguente percorso, quindi impostare il valore di registro su 1:

  SOFTWARE\Arcserve\Unified Data Protection\Engine

  - Quando si esegue un processo di ripristino dalla pagina Nodi, creare una chiave di registro sul proxy di backup.
  - Quando si esegue un processo di ripristino dall'agente normale utilizzando la sessione di backup RPS, creare una chiave di registro sull'agente normale.

3. Per migliorare la velocità effettiva durante il ripristino di un volume di grandi dimensioni con molti file di piccole dimensioni, selezionare un volume quindi, in Ripristino a livello di blocco, fare clic sulla casella di controllo **Esegui ripristino a livello di blocco**. Le altre opzioni vengono disabilitate e viene visualizzata una notifica. Per continuare con il ripristino a livello di blocco, fare clic su **OK**.



Nota: i dati vengono ripristinati nel computer dell'agente UDP corrente e il volume di destinazione viene sovrascritto. Il volume di destinazione non è accessibile durante il processo di ripristino.

4. Specificare l'opzione Risoluzione conflitti che verrà eseguita da Arcserve UDP in caso di conflitti durante il processo di ripristino.

   Le opzioni disponibili sono:

   Sovrascrivi i file esistenti

   Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dai file di backup, indipendentemente dalla loro presenza sul computer.

   Sostituisci file attivi

Consente di sostituire i file attivi dopo il riavvio. Se durante il tentativo di ripristino l'agente Arcserve UDP (Windows) rileva che l'utente sta accedendo al file esistente o che quest'ultimo è momentaneamente in uso, tale file non viene sostituito immediatamente. Per evitare l'insorgere di problemi, i file attivi vengono sostituiti al riavvio successivo del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita con il riavvio successivo).

Questa opzione è disponibile solo se l'opzione **Sovrascrivi i file esistenti** è stata selezionata.

Nota: se l'opzione non è selezionata, tutti i file attivi verranno ignorati durante il processo di ripristino.

Rinomina file

Se il nome file esiste già, consente di creare un nuovo file. Questa opzione consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno quindi ripristinati nel nuovo file.

Ignora file esistenti

Ignora e non sovrascrive (sostituisce) i file esistenti contenuti nella destinazione di ripristino. Solo gli oggetti inesistenti sul computer verranno ripristinati dai file di backup.

Impostazione predefinita: Ignora file esistenti.

5. Per Struttura directory, se si desidera creare una directory principale durante il ripristino, selezionare la casella di controllo **Crea directory principale**.

   La casella di controllo **Crea directory principale** specifica che se l'immagine di backup acquisita contiene una struttura delle directory principali, Arcserve UDP ricrea la stessa struttura della directory principale nel percorso di destinazione di ripristino.

   Se questa opzione non viene selezionata, il file o cartella verranno ripristinati direttamente nella cartella di destinazione.

   Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt e C:\Folder1\SubFolder2\B.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

   - Se si sceglie di ripristinare i file A.txt e B.txt individualmente, la destinazione dei file ripristinati corrisponderà a D:\Restore\A.txt e D:\Restore\B.txt. La directory principale sopra il livello di file specificato non verrà ricreata.
   - Se si sceglie di eseguire il ripristino a partire dal livello SubFolder2, la destinazione dei file ripristinati corrisponderà a D:\Restore\SubFolder2\A.txt e

D:\Restore\SubFolder2\B.txt. La directory principale al di sopra del livello di cartella specificato non verrà ricreata.

Se questa opzione è selezionata, verrà ricreato l'intero percorso della directory principale per i file o le cartelle (compreso il nome del volume) nella cartella di destinazione. Se i file o le cartelle da ripristinare appartengono allo stesso nome del volume, il percorso della directory principale di destinazione non includerà tale nome del volume. Tuttavia, se i file o le cartelle da ripristinare appartengono a diversi nomi di volume, il percorso della directory principale di destinazione includerà il nome del volume.

Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt, C:\Folder1\SubFolder2\B.txt e E:\Folder3\SubFolder4\C.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

- Se si desidera ripristinare soltanto il file A.txt, la destinazione del file ripristinato corrisponderà a D:\Restore\ Folder1\SubFolder2\A.txt (verrà ricreata l'intera directory principale, eccetto il nome del volume).
- Se si esegue il ripristino di entrambi i file A.txt e B.txt, la destinazione dei file ripristinati corrisponderà a D:\Restore\C\Folder1\SubFolder2\A.txt e D:\Restore\E\Folder3\SubFolder4\C.txt (verrà ricreata l'intera directory principale, compreso il nome del volume).

6. Per il recupero di ACL, per ignorare l'autorizzazione originale per i file o le cartelle ripristinati, selezionare la casella di controllo **Ignora recupero elenchi di controllo file/cartelle.** Selezionando questa opzione vengono ereditate le autorizzazioni della cartella di destinazione. In caso contrario, vengono conservate le autorizzazioni originali.
7. Per **Crittografia di backup o Protezione password**, se necessario specificare la password di crittografia di backup quando i dati da ripristinare sono crittografati.

   Se il ripristino viene eseguito dallo stesso computer dell'agente Arcserve UDP (Windows) da cui è stato eseguito il backup crittografato, non è necessario specificare una password. Tuttavia, la password verrà richiesta quando il ripristino viene eseguito da un computer dell'agente Arcserve UDP (Windows) diverso.

   Nota: l'icona di un orologio con lucchetto indica che il punto di ripristino contiene informazioni crittografate e potrebbe richiedere una password per il ripristino.
8. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo Riepilogo ripristino.

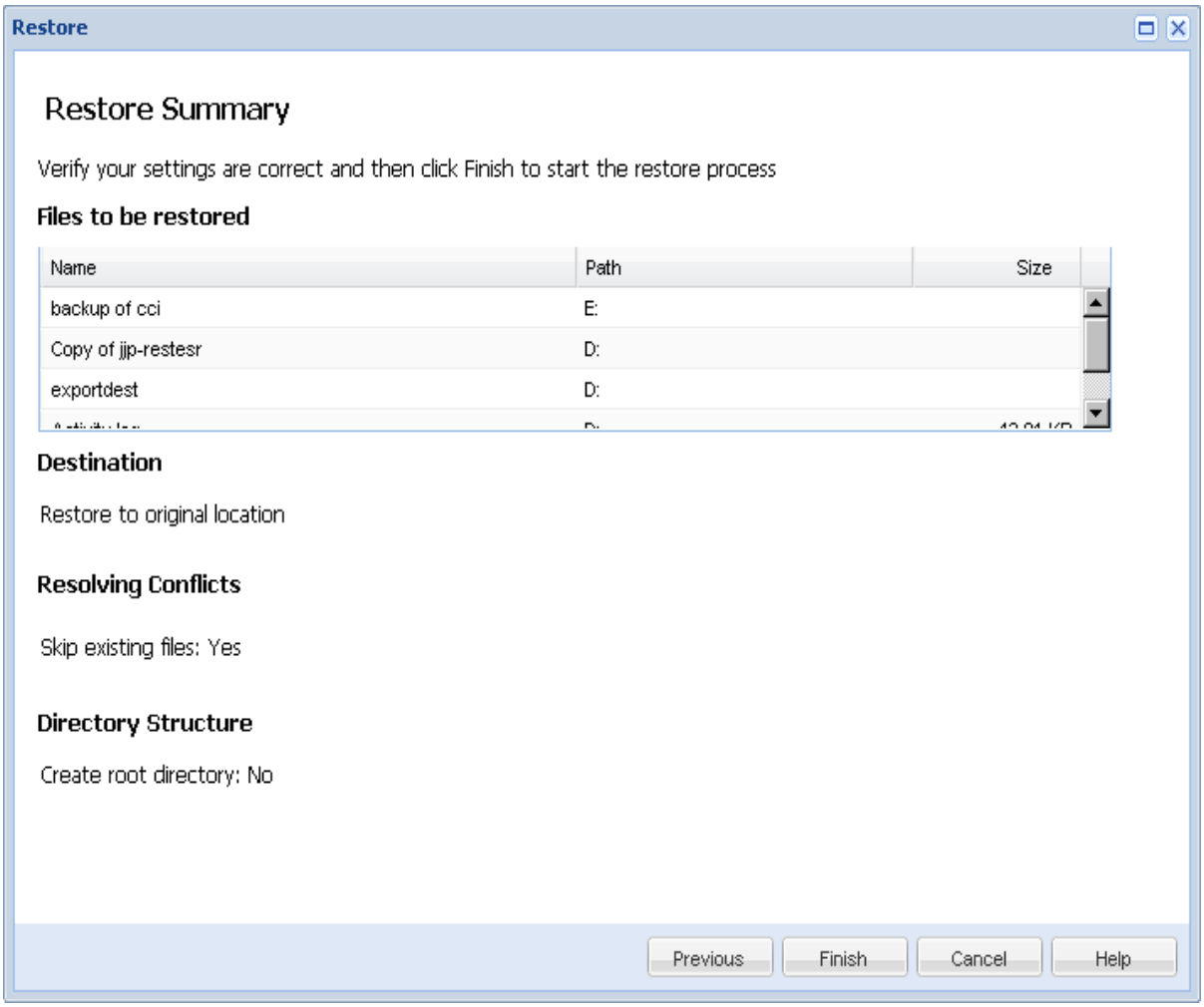
   Le opzioni di ripristino vengono definite per il ripristino da un punto di ripristino.

Ripristino del contenuto del punto di ripristino

Una volta definite le opzioni di ripristino, verificare che le impostazioni siano corrette e confermare il processo di ripristino. La pagina Riepilogo di ripristino consente di verificare tutte le opzioni di ripristino definite e, se necessario, modificarle.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo Riepilogo ripristino, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



2. Eseguire una delle seguenti operazioni:
   - Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.

- Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

Il contenuto del punto di ripristino viene ripristinato.

Verifica del corretto ripristino del contenuto

Una volta completato il processo di ripristino, verificare il ripristino del contenuto nella destinazione specificata.

Effettuare le operazioni seguenti:

1. Dalla console Arcserve UDP, accedere a **Processi** > **Processi completati correttamente**.

   L'elenco dei processi di backup completati viene visualizzato nel riquadro centrale.

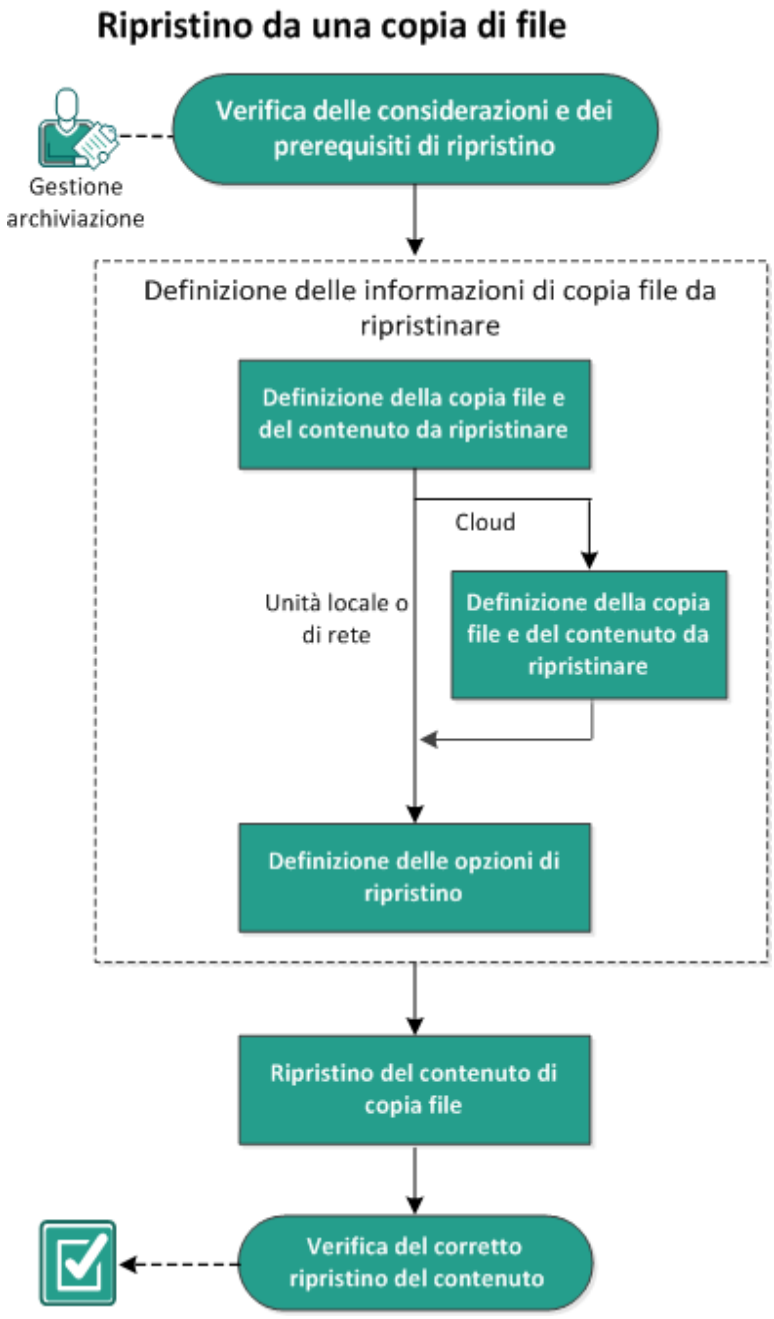
2. Fare clic sul processo di replica inversa completato. Il riquadro destro viene aggiornato.
3. In Dettagli processo, fare clic sul collegamento ipertestuale **Visualizza registri**.
4. Verificare il contenuto per confermare che il processo di ripristino è stato eseguito correttamente.

   Il contenuto ripristinato è stato verificato correttamente.

Ripristino da una copia di file

Ogni volta che Arcserve UDP esegue un processo di copia di file, viene eseguito il backup di tutti i file modificati dall'ultimo processo di copia dei file. Questo metodo di ripristino consente di sfogliare i dati copiati dei file e di specificare esattamente i file da ripristinare.

Il diagramma seguente mostra il processo di ripristino da una copia di file:



Per eseguire il ripristino da una copia file, effettuare le seguenti attività:

1. Verifica delle considerazioni e dei prerequisiti di ripristino
2. Definizione delle informazioni di copia file da ripristinare
    a. Definizione della copia file e del contenuto da ripristinare
        - Definizione della configurazione cloud per il ripristino
    b. Definizione delle opzioni di ripristino
3. Ripristino del contenuto del punto di ripristino
4. Verifica del corretto ripristino del contenuto

Verifica delle considerazioni e dei prerequisiti di ripristino

Verificare i seguenti prerequisiti prima di procedere al ripristino:

- È necessario disporre di almeno una copia file per il ripristino.
- È necessario disporre di una destinazione di copia di file valida e accessibile da cui eseguire il ripristino del contenuto della copia file.
- È necessario disporre di una posizione di destinazione valida e accessibile dove eseguire la copia file.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Verificare le seguenti considerazioni sul ripristino:

- Arcserve UDP consente di eseguire un solo processo di ripristino alla volta. Se si tenta di avviare manualmente un processo di ripristino durante l'esecuzione di un altro, verrà visualizzato un messaggio di avviso ad indicare che è in esecuzione un altro processo, per cui sarà necessario riprovare in seguito.
- Se il ripristino viene eseguito su una destinazione remota e tutte le unità (A - Z) sono occupate, non sarà possibile eseguire il ripristino su posizione remota. L'agente Arcserve UDP (Windows) deve utilizzare una lettera di unità per eseguire il montaggio del percorso di destinazione remoto.
- Migliorare il processo di copia file per ottimizzare le prestazioni:
  - La Copia file è in grado di inviare più blocchi alla volta alla destinazione (ArchMultChunkIO).
  - La Copia file consente di copiare più di un file alla volta dalla destinazione (ThreadsForArchive).
  - Il ripristino da una copia file è in grado di eseguire il download di più di un file alla volta (ThreadsForRestore).
  - La Sincronizzazione di catalogo utilizza thread multipli (ThreadForCatalogSync).

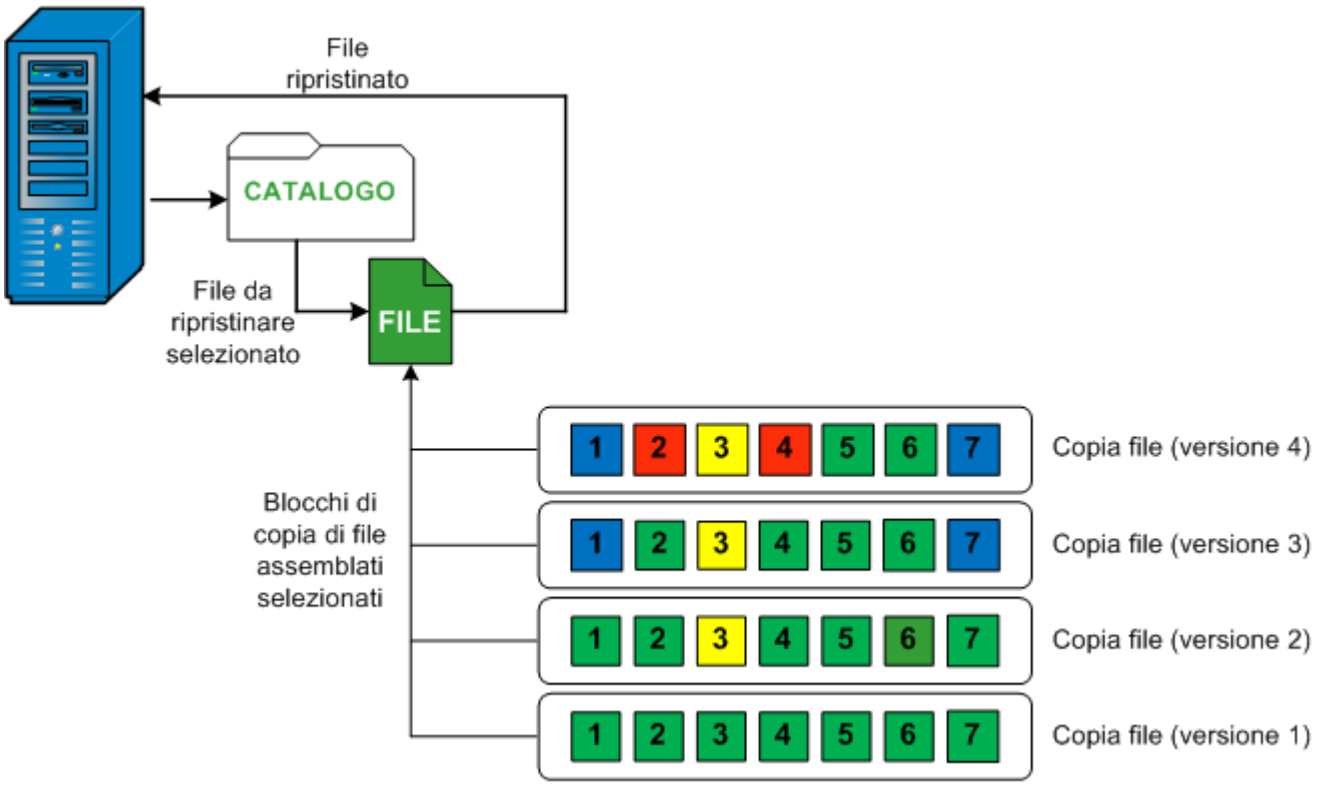
  È possibile modificare i valori del registro di sistema di copia file modificando il valore DWORD appropriato. Per ulteriori informazioni, consultare la sezione Configurazione delle impostazioni di copia file per il miglioramento delle prestazioni della *Guida in linea dell'agente per Windows*.
- (Facoltativo) Comprendere il funzionamento del processo di ripristino. Per ulteriori informazioni, consultare la sezione Funzionamento del ripristino a livello di

file.

Funzionamento del ripristino a livello di file

Durante un processo di copia file, ciascun file di backup è costituito da un insieme di blocchi che definiscono un file specifico. Per ciascuna versione del file sottoposto a backup viene creato un file di catalogo simultaneamente ai blocchi individuali utilizzati per tali file. Nel caso in cui sia necessario ripristinare un file specifico, è possibile individuare il file che si desidera ripristinare e le versioni di copia file che si desidera utilizzare. Arcserve UDP acquisisce la raccolta della versione dei blocchi utilizzati per la copia di file del file specificato, ne esegue il montaggio e ripristina il file.

Nel seguente diagramma di flusso è possibile visualizzare il processo di ripristino di un file specifico in Arcserve UDP:



Definizione delle informazioni di copia file da ripristinare

Arcserve UDP include un'opzione per il ripristino dei dati da una copia file. L'obiettivo di un processo di ripristino è quello di identificare rapidamente i dati necessari e di recuperarli dalla posizione di backup appropriata. Per ciascun processo di ripristino è richiesta un'origine e una destinazione.

Il processo per il ripristino da una copia file è il seguente:

- Definizione della copia file e del contenuto da ripristinare
- Definizione delle opzioni di ripristino

Definizione della copia file e del contenuto da ripristinare

Utilizzare l'opzione **Sfoglia copie file** per eseguire il ripristino da una copia file. Questo metodo di ripristino consente di sfogliare i dati copiati dei file e di specificare esattamente i file da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere alla finestra di dialogo per la selezione del metodo di ripristino in uno dei modi seguenti:

   Da Arcserve UDP:

   a. Accedere ad Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

      Nota: Viene effettuato automaticamente l'accesso al nodo agente e la finestra di dialogo per la selezione del metodo di ripristino viene visualizzata dal nodo agente.

   Dall'agente Arcserve UDP (Windows):

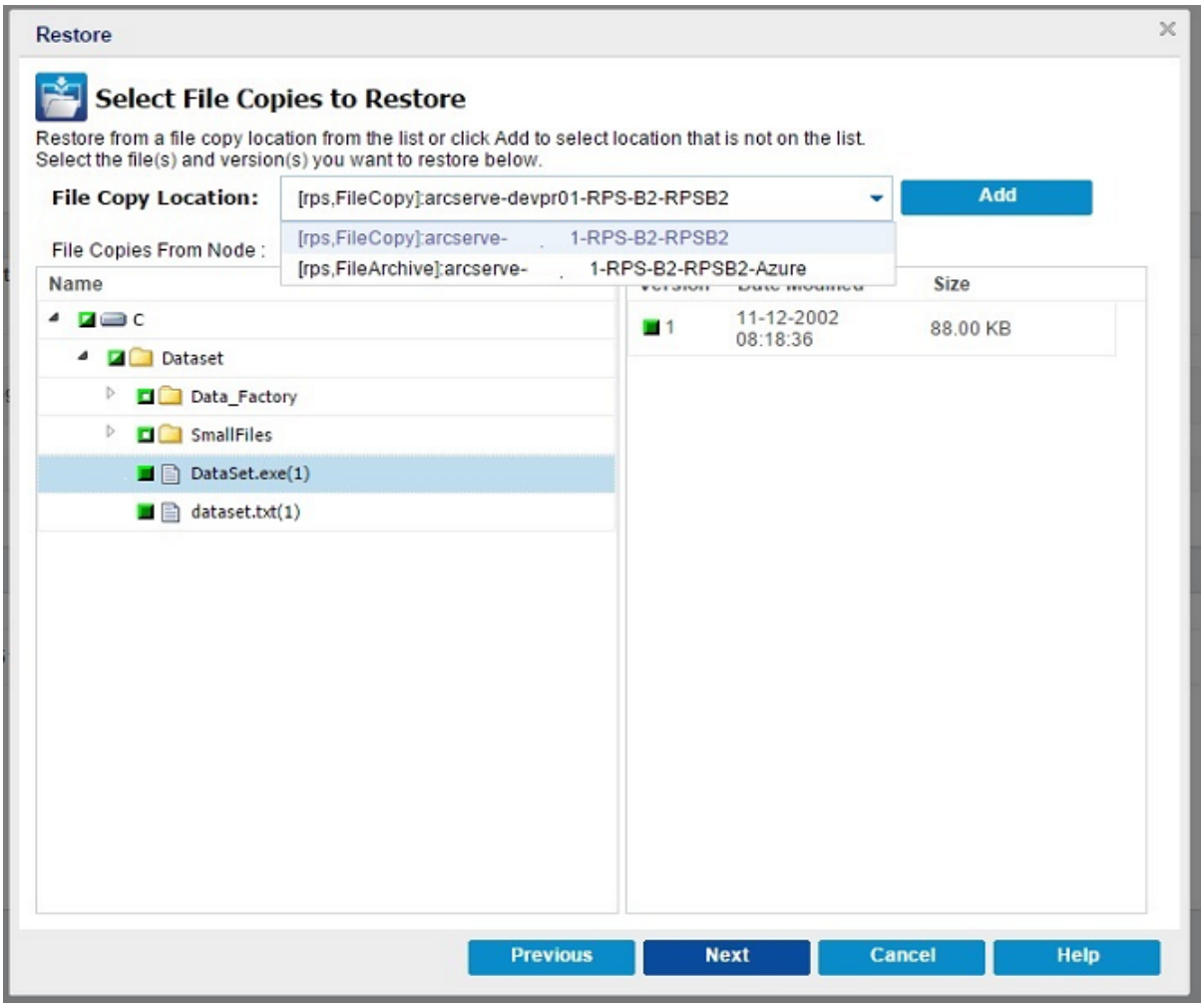
   a. Accedere all'agente Arcserve UDP (Windows).

   b. Dalla pagina principale selezionare **Ripristino**.

   Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

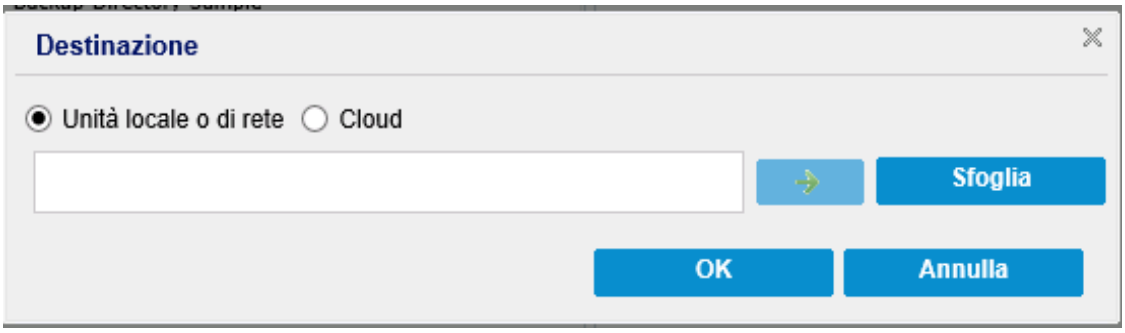
2. Fare clic sull'opzione **Sfoglia copie file**.

   Verrà visualizzata la finestra di dialogo di **ripristino.** La destinazione visualizzata nel campo **Ripristina da** corrisponde alla destinazione di **copia file** configurata per impostazione predefinita.



3. Se necessario, è possibile fare clic su **Aggiungi** per selezionare un percorso alternativo in cui memorizzare le immagini di copia dei file.

   Viene visualizzata la finestra di dialogo **Destinazione** con le opzioni relative alla destinazione alternativa disponibile.



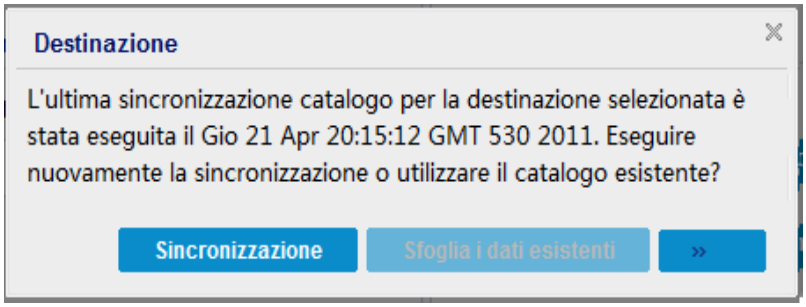
Unità locale o di rete

Visualizza la finestra di dialogo di **selezione della posizione di backup**, che consente di individuare e selezionare una posizione alternativa su unità locali o di rete.

Cloud

Visualizza la finestra di dialogo **Configurazione cloud**, che consente di accedere e configurare una posizione cloud alternativa. Per ulteriori informazioni su questa finestra di dialogo, consultare la sezione Definizione della configurazione cloud per il ripristino.

Indipendentemente dal tipo di selezione (**ripristino da un'unità locale, da un'unità di rete** o da **cloud**), quando la destinazione viene modificata verso un'altra posizione, verrà visualizzata una finestra di dialogo in cui viene richiesto se si desidera eseguire una nuova sincronizzazione del catalogo o leggere il catalogo esistente.



- Se si esegue la sincronizzazione del catalogo per la prima volta, il pulsante **Sfoglia i dati esistenti** è disabilitato perché il catalogo di copia file non esiste in locale.
- Se è stata eseguita una sincronizzazione del catalogo in precedenza, questa finestra di dialogo conterrà i dettagli relativi all'ultima sincronizzazione a partire dalla destinazione. Se vengono eseguiti più processi di copia file dopo l'ora indicata, il catalogo potrebbe non essere sincronizzato. È possibile selezionare l'opzione **Sincronizzazione** per verificare che il catalogo di copia file sia aggiornato.

1. Fare clic su **Sincronizzazione** per scaricare sul computer locale il catalogo di copia file dalla destinazione di copia file specificata e consentire un'esplorazione più veloce.

2. Fare clic su **Sfoglia i dati esistenti** per utilizzare il catalogo di copia file disponibile in locale senza ripetere il download o la sincronizzazione.

4. Nel riquadro sinistro, specificare i dati di copia file da ripristinare. È possibile selezionare cartelle o file di copia file da ripristinare.

   Quando si seleziona un singolo file da ripristinare, tutte le versioni di copie di file del file in questione verranno visualizzate nel riquadro destro. Se sono disponibili più versioni, sarà necessario selezionare la versione di copia file che si desidera ripristinare.

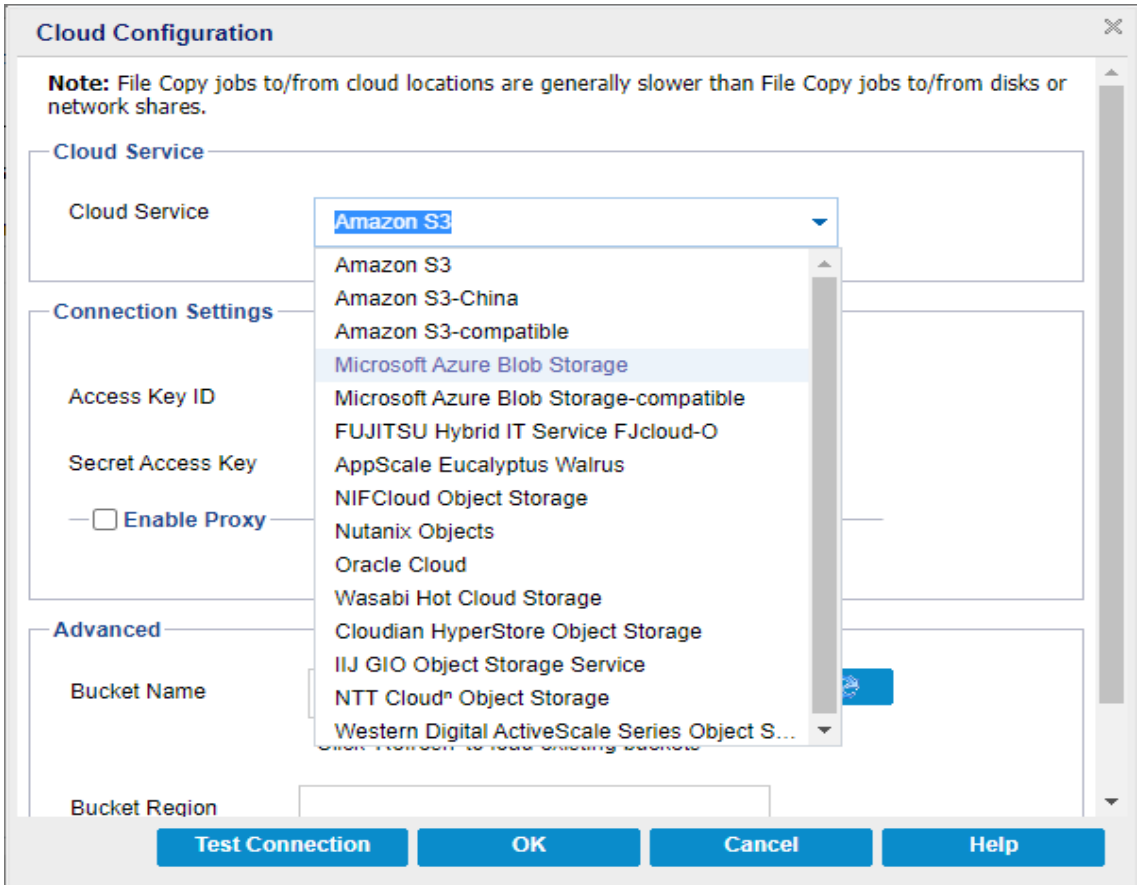
5. Dopo aver selezionato la cartella del file copiato o la versione di file da ripristinare, fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Opzioni di ripristino**.

   La **copia file e il contenuto da ripristinare** sono specificati.

Definizione della configurazione cloud per il ripristino

Nota: la procedura riportata di seguito è valida solo in caso di ripristino di un file o una cartella da una posizione cloud di copia file o archiviazione file.



Le opzioni disponibili sono Amazon S3, compatibile con Amazon S3, Windows Azure, compatibile con Windows Azure, FUJITSU Hybrid IT Service FJcloud-O ed Eucalyptus-Walrus. Il fornitore selezionato per impostazione predefinita è Amazon S3.

Nota: se si utilizza Eucalyptus-Walrus come fornitore cloud di copia dei file, non sarà possibile copiare file il cui percorso supera i 170 caratteri.

Le opzioni di configurazione disponibili per ciascun fornitore cloud sono simili (con alcune differenze terminologiche). In caso di differenze viene fornita una descrizione.

1. Dall'opzione **Sfoglia copie file** o dall'opzione **Trova file/cartelle da ripristinare, fare clic su Aggiungi**.

   Verrà visualizzata la finestra di dialogo **Destinazione**.

2. Selezionare **Cloud** e fare clic su **Sfoglia**.

   Viene visualizzata la finestra di dialogo **Configurazione cloud**.

3. Immettere le seguenti informazioni:

Nome archiviazione

Specifica il nome del servizio dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome di archiviazione univoco.

Servizio di archiviazione

Selezionare il servizio dall'elenco a discesa. L'opzione di configurazione dipende dal servizio di archiviazione selezionato.

ID del codice di accesso/Nome account/ID query

Indica l'utente che richiede l'accesso a questa posizione.

Per questo campo, Amazon S3 utilizza l'ID del codice di accesso, Windows Azure. FUJITSU Hybrid IT Service FJcloud-O utilizza Nome account, mentre Eucalyptus-Walrus utilizza ID query.

Codice di accesso segreto/Chiave privata

Poiché il codice di accesso non viene crittografato, la chiave privata si utilizza per verificare l'autenticità della richiesta di accesso.

Importante! Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

Per questo campo, Amazon S3 utilizza Codice di accesso segreto. Windows Azure, FUJITSU Hybrid IT Service FJcloud-O e Eucalyptus-Walrus utilizzano la chiave segreta.

Impostazioni proxy

Specifica le impostazioni del server proxy fornite. Selezionare **Connetti tramite server proxy** per abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

Nota: La funzionalità di proxy non è disponibile per Eucalyptus-Walrus.

Nome bucket/Contenitore

Tutti i file e le cartelle spostati o copiati sul sistema del fornitore cloud vengono archiviati e organizzati in bucket o contenitori. I bucket sono dei contenitori di file utilizzati per raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

Per questo campo, Amazon S3 ed Eucalyptus-Walrus utilizzano Nome bucket. Windows Azure e FUJITSU Hybrid IT Service FJcloud-O utilizzano il contenitore.

Nota: a partire da questo punto del passaggio, è possibile applicare le operazioni relative ai bucket ai contenitori, salvo diversamente specificato.

Area di bucket

Fa riferimento all'area di bucket in Amazon e FUJITSU Hybrid IT Service FJcloud-O.

Numero di contratto

Indica il numero del contratto fornito da FUJITSU Hybrid IT Service FJcloud-O.

ID progetto

Indica l'ID del progetto generato da FUJITSU Hybrid IT Service FJcloud-O.

Abilita riduzione di archiviazione dei dati ridondanti

Con Amazon S3, è possibile selezionare questa opzione per abilitare la riduzione di archiviazione dei dati ridondanti (RRS). L'opzione di archiviazione RSS di Amazon S3 consente di ridurre i costi mediante l'archiviazione dei dati non critici e riproducibili a livelli di ridondanza inferiori rispetto ai livelli di archiviazione standard di Amazon S3. Entrambe le opzioni di archiviazione (con ridondanza standard e ridotta) consentono di archiviare i dati su più dispositivi e periferiche. Tuttavia la riduzione di archiviazione dei dati ridondanti consente di eseguire un numero minore di repliche, riducendo in tal modo i costi. L'archiviazione standard di Amazon S3 e la riduzione di archiviazione dei dati ridondanti presentano gli stessi valori di latenza e velocità. Per impostazione predefinita questa opzione non è selezionata, in quanto Amazon S3 utilizza l'opzione di archiviazione standard.

4. Per verificare la connessione al percorso cloud specificato, fare clic su **Verifica connessione**.
5. Fare clic su **OK**.

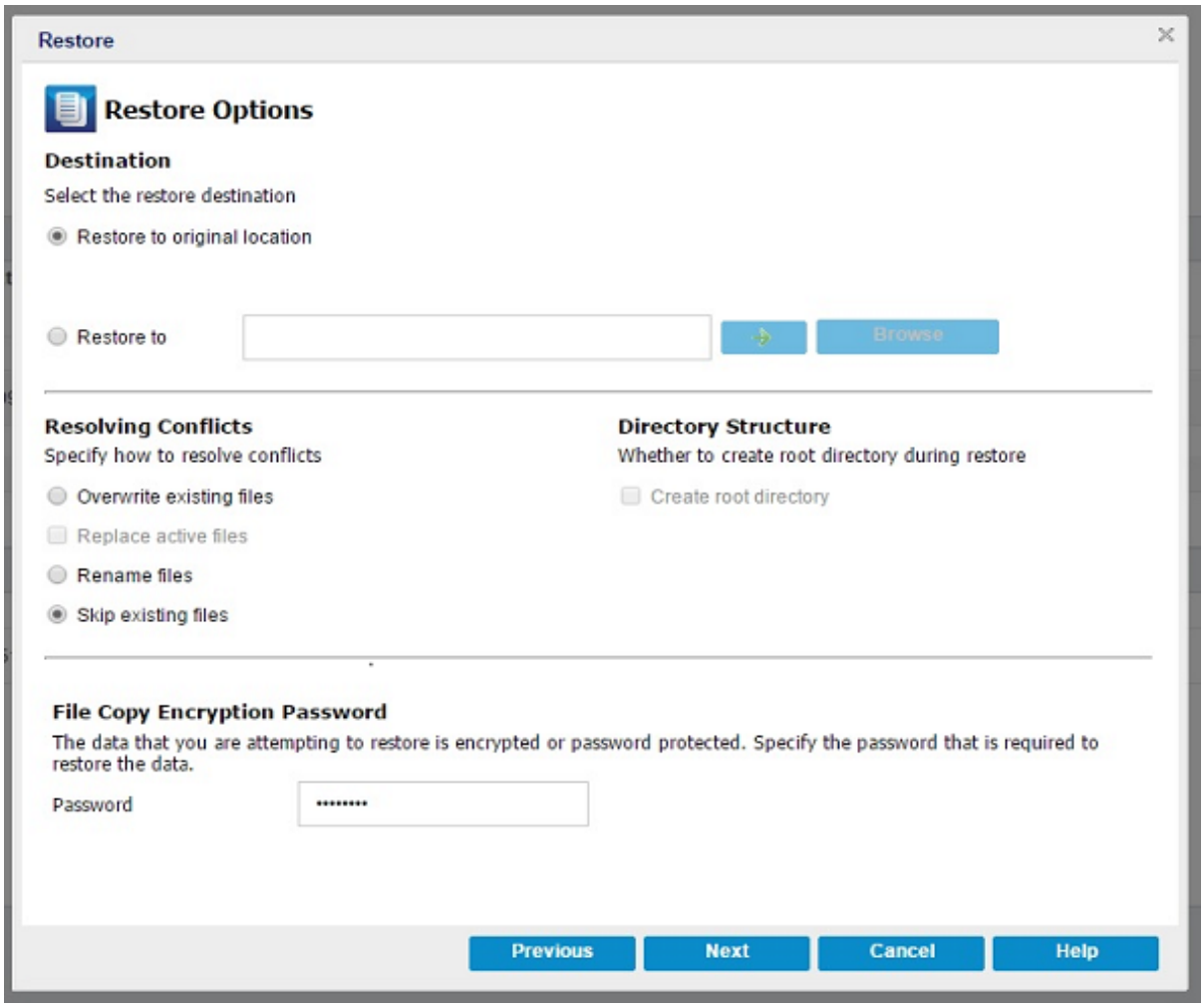
   L'account cloud viene aggiunto alla console.

Definizione delle opzioni di ripristino

Dopo aver specificato le informazioni di copia file per il ripristino, definire le opzioni di copia per il contenuto e la copia file selezionata.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Opzioni di ripristino**, selezionare la destinazione di ripristino.



Le opzioni di destinazione disponibili sono:

Ripristina in posizione originale

Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

Ripristina su

Esegue il ripristino alla posizione specificata. Per verificare la connessione al percorso specificato, fare clic sulla freccia verde. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso.

2. Specificare l'opzione **Risoluzione conflitti** che verrà eseguita da Arcserve UDP in caso di conflitti durante il processo di ripristino.

   Le opzioni disponibili sono:

   Sovrascrivi i file esistenti

   Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dai file di backup, indipendentemente dalla loro presenza sul computer.

   Sostituisci file attivi

   Consente di sostituire i file attivi dopo il riavvio. Se durante il tentativo di ripristino l'agente Arcserve UDP (Windows) rileva che l'utente sta accedendo al file esistente o che quest'ultimo è momentaneamente in uso, tale file non viene sostituito immediatamente. Per evitare l'insorgere di problemi, i file attivi vengono sostituiti al riavvio successivo del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita con il riavvio successivo).

   Questa opzione è disponibile solo se l'opzione **Sovrascrivi i file esistenti** è stata selezionata.

   Nota: se l'opzione non è selezionata, tutti i file attivi verranno ignorati durante il processo di ripristino.

   Rinomina file

   Se il nome file esiste già, consente di creare un nuovo file. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno quindi ripristinati nel nuovo file.

   Ignora file esistenti

   Ignora e non sovrascrive (sostituisce) i file esistenti contenuti nella destinazione di ripristino. Solo gli oggetti inesistenti sul computer verranno ripristinati dai file di backup.

   Impostazione predefinita: Ignora file esistenti.

3. Specificare la **struttura di directory** per creare una directory principale durante il ripristino.

   Crea directory principale

   Se l'immagine di backup acquisita contiene una struttura delle directory principali, Arcserve UDP ricrea la stessa struttura della directory principale nel percorso di destinazione di ripristino.

   Se questa opzione non viene selezionata, il file o cartella verrà ripristinato direttamente nella cartella di destinazione.

   Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt e C:\Folder1\SubFolder2\B.txt e durante il ripristino è stata specificata la destinazione D:\Restore.

   - Se si sceglie di ripristinare i file A.txt e B.txt individualmente, la destinazione dei file ripristinati corrisponderà a D:\Restore\A.txt e D:\Restore\B.txt. La directory principale sopra il livello di file specificato non verrà ricreata.
   - Se si sceglie di eseguire il ripristino a partire dal livello SubFolder2, la destinazione dei file ripristinati corrisponderà a D:\Restore\SubFolder2\A.txt e D:\Restore\SubFolder2\B.txt. La directory principale al di sopra del livello di cartella specificato non verrà ricreata.

   Se questa opzione è selezionata, verrà ricreato l'intero percorso della directory principale per i file o le cartelle (compreso il nome del volume) nella cartella di destinazione. Se i file o le cartelle da ripristinare appartengono allo stesso nome del volume, il percorso della directory principale di destinazione non includerà tale nome del volume. Tuttavia, se i file o le cartelle da ripristinare appartengono a diversi nomi di volume, il percorso della directory principale di destinazione includerà il nome del volume.

   Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt, C:\Folder1\SubFolder2\B.txt e E:\Folder3\SubFolder4\C.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

   - Se si desidera ripristinare soltanto il file A.txt, la destinazione del file ripristinato corrisponderà a D:\Restore\ Folder1\SubFolder2\A.txt (verrà ricreata l'intera directory principale, eccetto il nome del volume).
   - Se si esegue il ripristino di entrambi i file A.txt e B.txt, la destinazione dei file ripristinati corrisponderà a D:\Restore\C\Folder1\SubFolder2\A.txt e D:\Restore\E\Folder3\SubFolder4\C.txt (verrà ricreata l'intera directory principale, compreso il nome del volume).

4. Specificare la password di crittografia in **Password di crittografia per la copia file.**

5. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Riepilogo ripristino**.

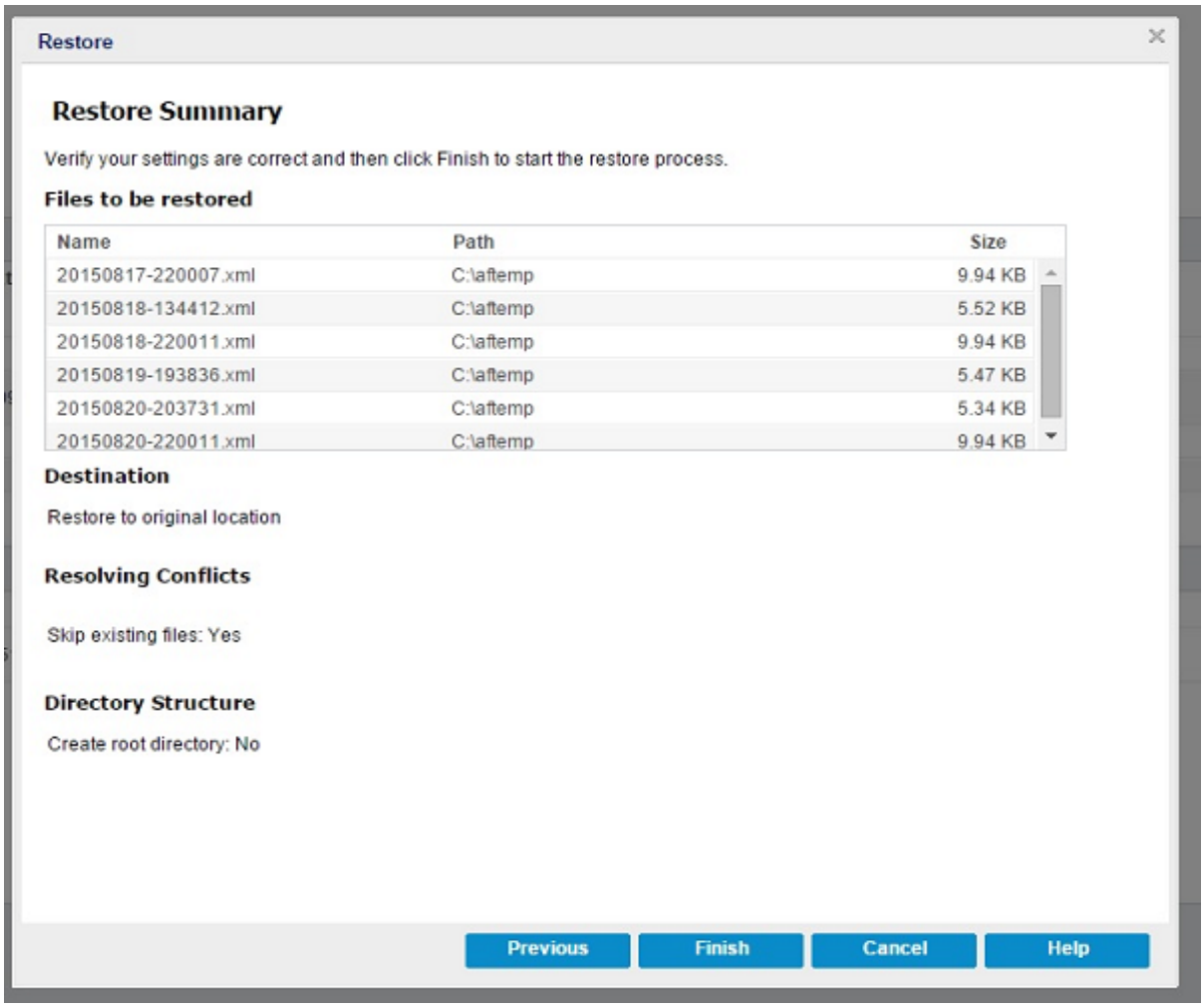
   Le opzioni di ripristino vengono definite per il ripristino da una copia file.

Ripristino del contenuto di copia file

Una volta definite le opzioni di ripristino, verificare che le impostazioni siano corrette e confermare il processo di ripristino. Il **riepilogo di ripristino** consente di verificare tutte le opzioni di ripristino definite e, se necessario, modificarle.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Riepilogo ripristino**, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



- Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
- Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

Il contenuto di copia file viene ripristinato.

Verifica del corretto ripristino del contenuto

Una volta completato il processo di ripristino, verificare il ripristino del contenuto nella destinazione specificata.

Effettuare le operazioni seguenti:

1. Accedere alla destinazione di ripristino specificata.

   Viene visualizzato un elenco di cartelle.

2. Individuare il file utilizzato per il ripristino del contenuto.

   Ad esempio, se si seleziona di ripristinare il file **A.txt** nella destinazione di ripristino D:\Restore, accedere al seguente percorso:

   D:\Restore\A.txt

3. Verificare il contenuto per confermare che il processo di ripristino è stato eseguito correttamente.

   Il contenuto ripristinato è stato verificato correttamente.

Ripristino da un archivio di file

Ogni volta che Arcserve UDP esegue un processo di copia di un archivio di file, viene eseguito il backup di tutti i file modificati dall'ultimo processo di archiviazione dei file. Questo metodo di ripristino consente di sfogliare i file archiviati e di specificare esattamente i file da ripristinare.

Il processo di ripristino di archiviazione dei file corrisponde al ripristino di copia file.

Per eseguire il ripristino da un archivio di file, effettuare le seguenti attività:

1. Verifica delle considerazioni e dei prerequisiti di ripristino
2. Definizione delle informazioni di copia file da ripristinare
    a. Definizione della copia file e del contenuto da ripristinare
        - Definizione della configurazione cloud per il ripristino
    b. Definizione delle opzioni di ripristino
3. Ripristino del contenuto del punto di ripristino
4. Verifica del corretto ripristino del contenuto

Verifica delle considerazioni e dei prerequisiti di ripristino

Verificare i seguenti prerequisiti prima di procedere al ripristino:

- È necessario disporre di almeno una copia file per il ripristino.
- È necessario disporre di una destinazione di copia di file valida e accessibile da cui eseguire il ripristino del contenuto della copia file.
- È necessario disporre di una posizione di destinazione valida e accessibile dove eseguire la copia file.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Verificare le seguenti considerazioni sul ripristino:

- Arcserve UDP consente di eseguire un solo processo di ripristino alla volta. Se si tenta di avviare manualmente un processo di ripristino durante l'esecuzione di un altro, verrà visualizzato un messaggio di avviso ad indicare che è in esecuzione un altro processo, per cui sarà necessario riprovare in seguito.
- Se il ripristino viene eseguito su una destinazione remota e tutte le unità (A - Z) sono occupate, non sarà possibile eseguire il ripristino su posizione remota. L'agente Arcserve UDP (Windows) deve utilizzare una lettera di unità per eseguire il montaggio del percorso di destinazione remoto.
- Migliorare il processo di copia file per ottimizzare le prestazioni:
  - La Copia file è in grado di inviare più blocchi alla volta alla destinazione (ArchMultChunkIO).
  - La Copia file consente di copiare più di un file alla volta dalla destinazione (ThreadsForArchive).
  - Il ripristino da una copia file è in grado di eseguire il download di più di un file alla volta (ThreadsForRestore).
  - La Sincronizzazione di catalogo utilizza thread multipli (ThreadForCatalogSync).

  È possibile modificare i valori del registro di sistema di copia file modificando il valore DWORD appropriato. Per ulteriori informazioni, consultare la sezione Configurazione delle impostazioni di copia file per il miglioramento delle prestazioni della *Guida in linea dell'agente per Windows*.
- (Facoltativo) Comprendere il funzionamento del processo di ripristino. Per ulteriori informazioni, consultare la sezione Funzionamento del ripristino a livello di

file.

Definizione delle informazioni di copia file da ripristinare

Arcserve UDP include un'opzione per il ripristino dei dati da una copia file. L'obiettivo di un processo di ripristino è quello di identificare rapidamente i dati necessari e di recuperarli dalla posizione di backup appropriata. Per ciascun processo di ripristino è richiesta un'origine e una destinazione.

Il processo per il ripristino da una copia file è il seguente:

- Definizione della copia file e del contenuto da ripristinare
- Definizione delle opzioni di ripristino

Definizione della copia file e del contenuto da ripristinare

Utilizzare l'opzione **Sfoglia copie file** per eseguire il ripristino da una copia file. Questo metodo di ripristino consente di sfogliare i dati copiati dei file e di specificare esattamente i file da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere alla finestra di dialogo per la selezione del metodo di ripristino in uno dei modi seguenti:

   Da Arcserve UDP:

   a. Accedere ad Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

      Nota: Viene effettuato automaticamente l'accesso al nodo agente e la finestra di dialogo per la selezione del metodo di ripristino viene visualizzata dal nodo agente.

   Dall'agente Arcserve UDP (Windows):

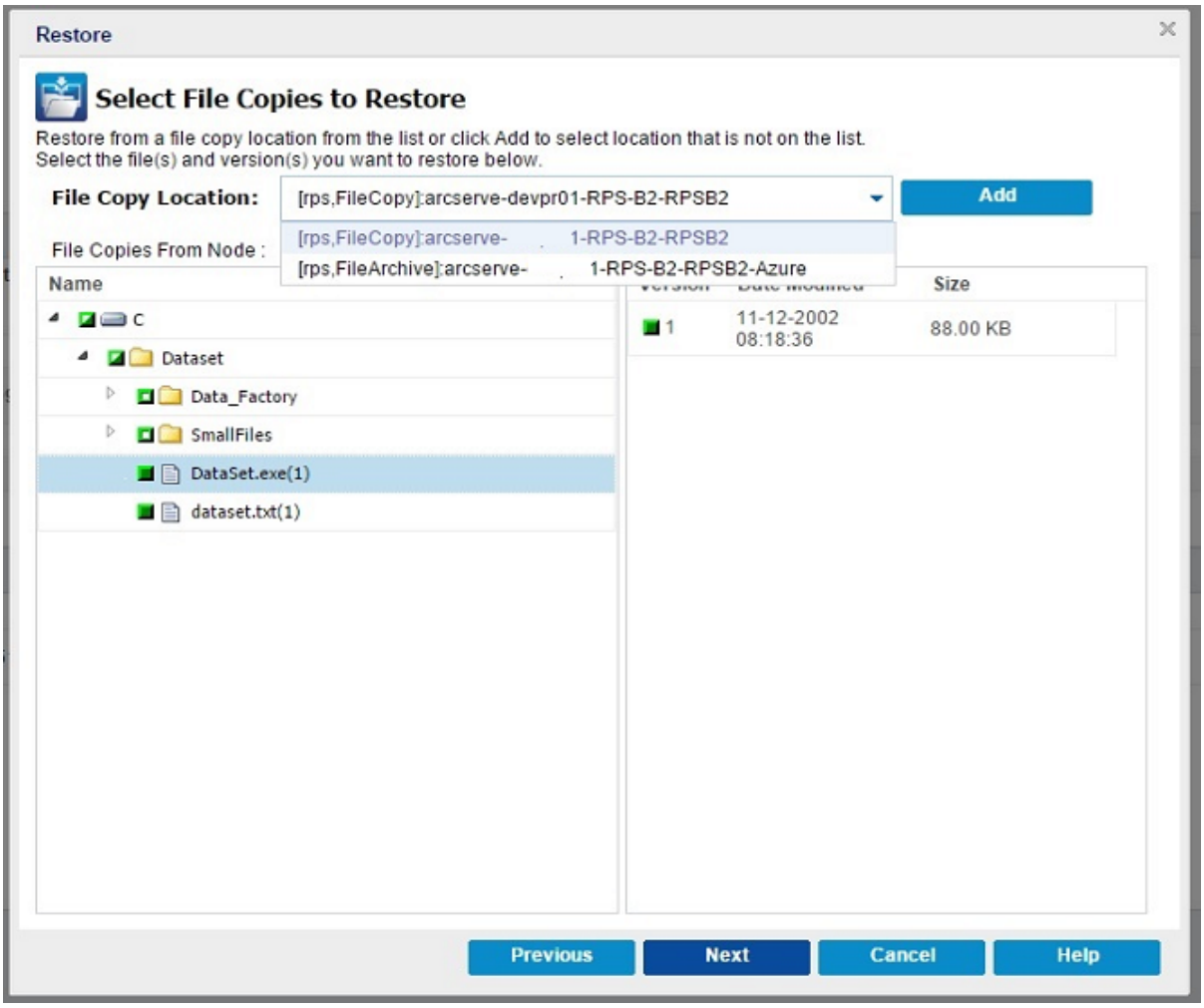
   a. Accedere all'agente Arcserve UDP (Windows).

   b. Dalla pagina principale selezionare **Ripristino**.

   Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

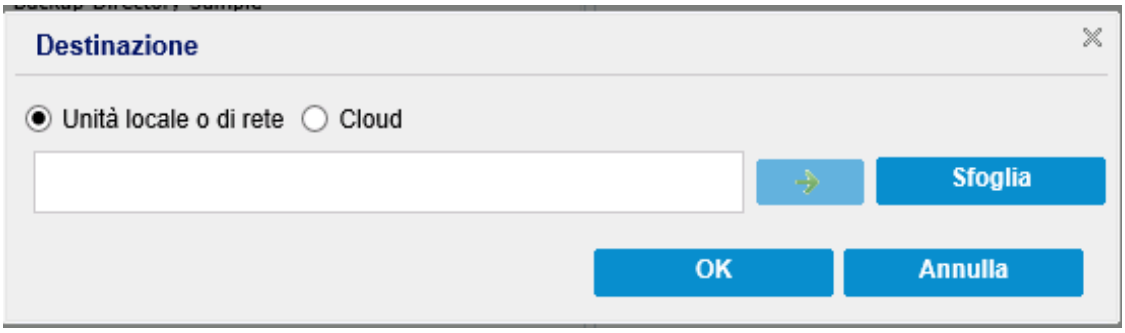
2. Fare clic sull'opzione **Sfoglia copie file**.

   Verrà visualizzata la finestra di dialogo di **ripristino.** La destinazione visualizzata nel campo **Ripristina da** corrisponde alla destinazione di **copia file** configurata per impostazione predefinita.



3. Se necessario, è possibile fare clic su **Aggiungi** per selezionare un percorso alternativo in cui memorizzare le immagini di copia dei file.

   Viene visualizzata la finestra di dialogo **Destinazione** con le opzioni relative alla destinazione alternativa disponibile.



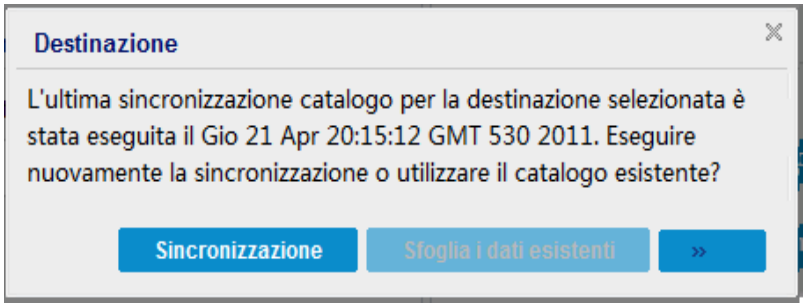
Unità locale o di rete

Visualizza la finestra di dialogo di **selezione della posizione di backup**, che consente di individuare e selezionare una posizione alternativa su unità locali o di rete.

Cloud

Visualizza la finestra di dialogo **Configurazione cloud**, che consente di accedere e configurare una posizione cloud alternativa. Per ulteriori informazioni su questa finestra di dialogo, consultare la sezione Definizione della configurazione cloud per il ripristino.

Indipendentemente dal tipo di selezione (**ripristino da un'unità locale, da un'unità di rete** o da **cloud**), quando la destinazione viene modificata verso un'altra posizione, verrà visualizzata una finestra di dialogo in cui viene richiesto se si desidera eseguire una nuova sincronizzazione del catalogo o leggere il catalogo esistente.



- Se si esegue la sincronizzazione del catalogo per la prima volta, il pulsante **Sfoglia i dati esistenti** è disabilitato perché il catalogo di copia file non esiste in locale.
- Se è stata eseguita una sincronizzazione del catalogo in precedenza, questa finestra di dialogo conterrà i dettagli relativi all'ultima sincronizzazione a partire dalla destinazione. Se vengono eseguiti più processi di copia file dopo l'ora indicata, il catalogo potrebbe non essere sincronizzato. È possibile selezionare l'opzione **Sincronizzazione** per verificare che il catalogo di copia file sia aggiornato.

1. Fare clic su **Sincronizzazione** per scaricare sul computer locale il catalogo di copia file dalla destinazione di copia file specificata e consentire un'esplorazione più veloce.

2. Fare clic su **Sfoglia i dati esistenti** per utilizzare il catalogo di copia file disponibile in locale senza ripetere il download o la sincronizzazione.

4. Nel riquadro sinistro, specificare i dati di copia file da ripristinare. È possibile selezionare cartelle o file di copia file da ripristinare.

   Quando si seleziona un singolo file da ripristinare, tutte le versioni di copie di file del file in questione verranno visualizzate nel riquadro destro. Se sono disponibili più versioni, sarà necessario selezionare la versione di copia file che si desidera ripristinare.

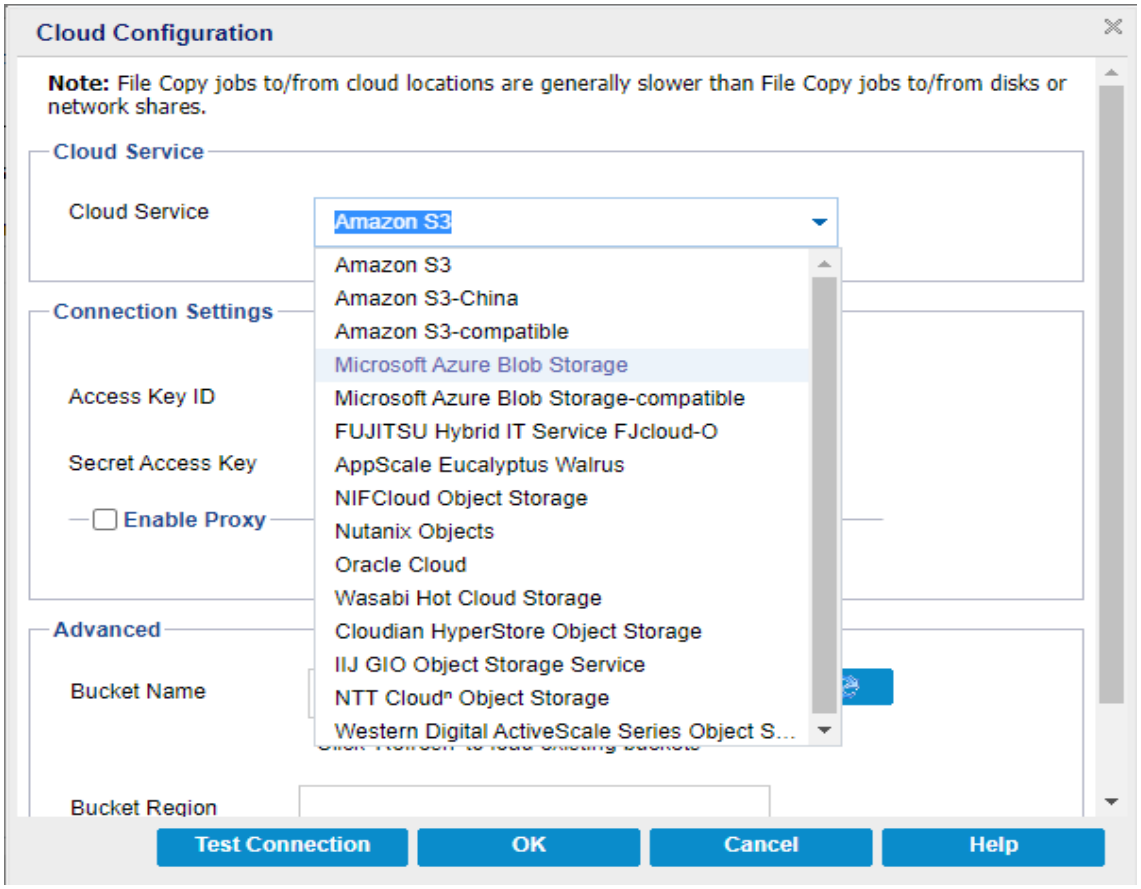
5. Dopo aver selezionato la cartella del file copiato o la versione di file da ripristinare, fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Opzioni di ripristino**.

   La **copia file e il contenuto da ripristinare** sono specificati.

Definizione della configurazione cloud per il ripristino

Nota: la procedura riportata di seguito è valida solo in caso di ripristino di un file o una cartella da una posizione cloud di copia file o archiviazione file.



Le opzioni disponibili sono Amazon S3, compatibile con Amazon S3, Windows Azure, compatibile con Windows Azure, FUJITSU Hybrid IT Service FJcloud-O ed Eucalyptus-Walrus. Il fornitore selezionato per impostazione predefinita è Amazon S3.

Nota: se si utilizza Eucalyptus-Walrus come fornitore cloud di copia dei file, non sarà possibile copiare file il cui percorso supera i 170 caratteri.

Le opzioni di configurazione disponibili per ciascun fornitore cloud sono simili (con alcune differenze terminologiche). In caso di differenze viene fornita una descrizione.

1. Dall'opzione **Sfoglia copie file** o dall'opzione **Trova file/cartelle da ripristinare, fare clic su Aggiungi**.

   Verrà visualizzata la finestra di dialogo **Destinazione**.

2. Selezionare **Cloud** e fare clic su **Sfoglia**.

   Viene visualizzata la finestra di dialogo **Configurazione cloud**.

3. Immettere le seguenti informazioni:

Nome archiviazione

Specifica il nome del servizio dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome di archiviazione univoco.

Servizio di archiviazione

Selezionare il servizio dall'elenco a discesa. L'opzione di configurazione dipende dal servizio di archiviazione selezionato.

ID del codice di accesso/Nome account/ID query

Indica l'utente che richiede l'accesso a questa posizione.

Per questo campo, Amazon S3 utilizza l'ID del codice di accesso, Windows Azure. FUJITSU Hybrid IT Service FJcloud-O utilizza Nome account, mentre Eucalyptus-Walrus utilizza ID query.

Codice di accesso segreto/Chiave privata

Poiché il codice di accesso non viene crittografato, la chiave privata si utilizza per verificare l'autenticità della richiesta di accesso.

Importante! Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

Per questo campo, Amazon S3 utilizza Codice di accesso segreto. Windows Azure, FUJITSU Hybrid IT Service FJcloud-O e Eucalyptus-Walrus utilizzano la chiave segreta.

Impostazioni proxy

Specifica le impostazioni del server proxy fornite. Selezionare **Connetti tramite server proxy** per abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Quindi, occorre fornire le informazioni di autenticazione (nome dominio\nome utente e password) necessarie per l'utilizzo del server proxy.

Nota: La funzionalità di proxy non è disponibile per Eucalyptus-Walrus.

Nome bucket/Contenitore

Tutti i file e le cartelle spostati o copiati sul sistema del fornitore cloud vengono archiviati e organizzati in bucket o contenitori. I bucket sono dei contenitori di file utilizzati per raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

Per questo campo, Amazon S3 ed Eucalyptus-Walrus utilizzano Nome bucket. Windows Azure e FUJITSU Hybrid IT Service FJcloud-O utilizzano il contenitore.

Nota: a partire da questo punto del passaggio, è possibile applicare le operazioni relative ai bucket ai contenitori, salvo diversamente specificato.

Area di bucket

Fa riferimento all'area di bucket in Amazon e FUJITSU Hybrid IT Service FJcloud-O.

Numero di contratto

Indica il numero del contratto fornito da FUJITSU Hybrid IT Service FJcloud-O.

ID progetto

Indica l'ID del progetto generato da FUJITSU Hybrid IT Service FJcloud-O.

Abilita riduzione di archiviazione dei dati ridondanti

Con Amazon S3, è possibile selezionare questa opzione per abilitare la riduzione di archiviazione dei dati ridondanti (RRS). L'opzione di archiviazione RSS di Amazon S3 consente di ridurre i costi mediante l'archiviazione dei dati non critici e riproducibili a livelli di ridondanza inferiori rispetto ai livelli di archiviazione standard di Amazon S3. Entrambe le opzioni di archiviazione (con ridondanza standard e ridotta) consentono di archiviare i dati su più dispositivi e periferiche. Tuttavia la riduzione di archiviazione dei dati ridondanti consente di eseguire un numero minore di repliche, riducendo in tal modo i costi. L'archiviazione standard di Amazon S3 e la riduzione di archiviazione dei dati ridondanti presentano gli stessi valori di latenza e velocità. Per impostazione predefinita questa opzione non è selezionata, in quanto Amazon S3 utilizza l'opzione di archiviazione standard.

4. Per verificare la connessione al percorso cloud specificato, fare clic su **Verifica connessione**.
5. Fare clic su **OK**.

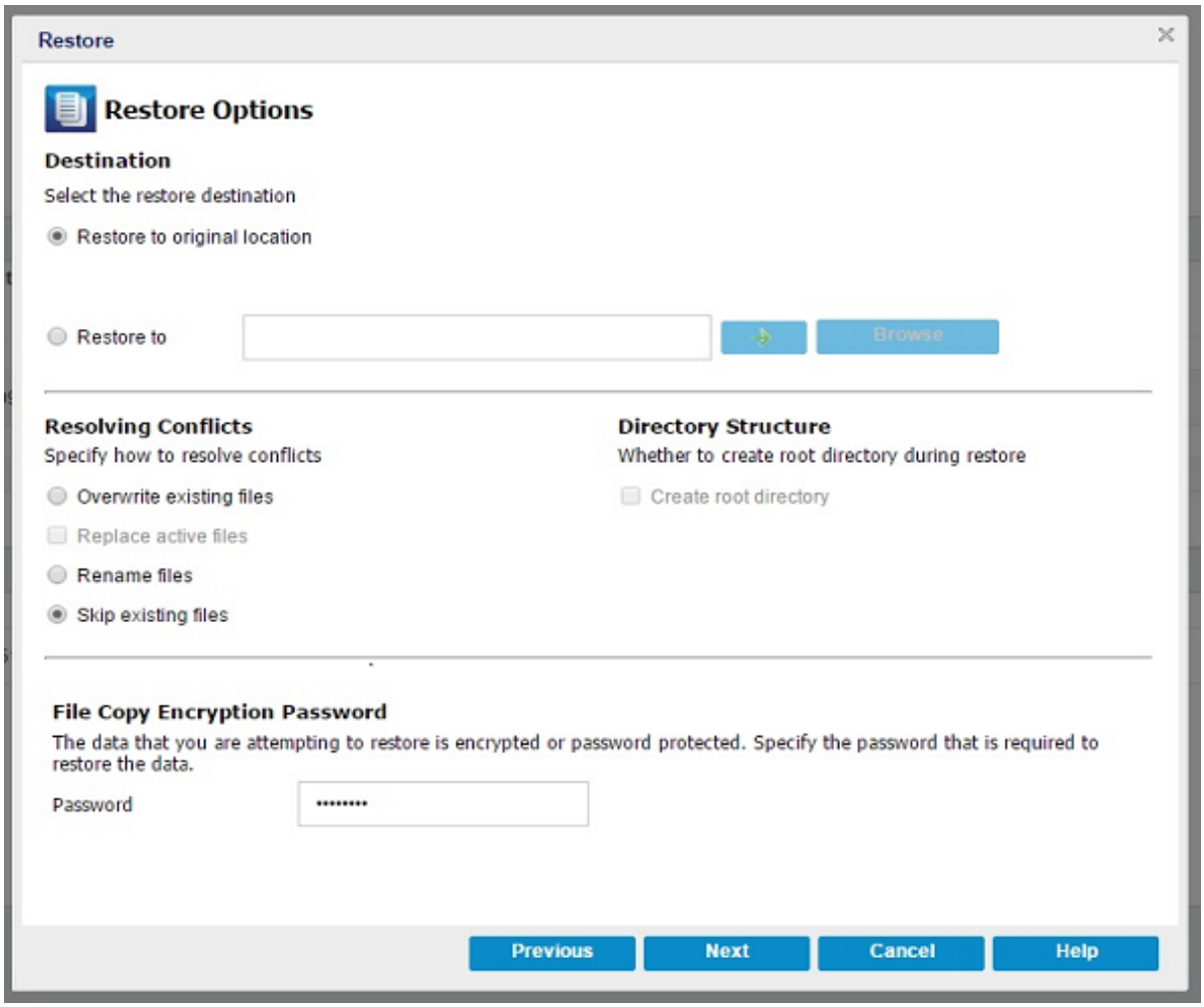
   L'account cloud viene aggiunto alla console.

Definizione delle opzioni di ripristino

Dopo aver specificato le informazioni di copia file per il ripristino, definire le opzioni di copia per il contenuto e la copia file selezionata.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Opzioni di ripristino**, selezionare la destinazione di ripristino.



Le opzioni di destinazione disponibili sono:

Ripristina in posizione originale

Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

Ripristina su

Esegue il ripristino alla posizione specificata. Per verificare la connessione al percorso specificato, fare clic sulla freccia verde. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso.

2. Specificare l'opzione **Risoluzione conflitti** che verrà eseguita da Arcserve UDP in caso di conflitti durante il processo di ripristino.

   Le opzioni disponibili sono:

   Sovrascrivi i file esistenti

   Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dai file di backup, indipendentemente dalla loro presenza sul computer.

   Sostituisci file attivi

   Consente di sostituire i file attivi dopo il riavvio. Se durante il tentativo di ripristino l'agente Arcserve UDP (Windows) rileva che l'utente sta accedendo al file esistente o che quest'ultimo è momentaneamente in uso, tale file non viene sostituito immediatamente. Per evitare l'insorgere di problemi, i file attivi vengono sostituiti al riavvio successivo del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita con il riavvio successivo).

   Questa opzione è disponibile solo se l'opzione **Sovrascrivi i file esistenti** è stata selezionata.

   Nota: se l'opzione non è selezionata, tutti i file attivi verranno ignorati durante il processo di ripristino.

   Rinomina file

   Se il nome file esiste già, consente di creare un nuovo file. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno quindi ripristinati nel nuovo file.

   Ignora file esistenti

   Ignora e non sovrascrive (sostituisce) i file esistenti contenuti nella destinazione di ripristino. Solo gli oggetti inesistenti sul computer verranno ripristinati dai file di backup.

   Impostazione predefinita: Ignora file esistenti.

3. Specificare la **struttura di directory** per creare una directory principale durante il ripristino.

   Crea directory principale

   Se l'immagine di backup acquisita contiene una struttura delle directory principali, Arcserve UDP ricrea la stessa struttura della directory principale nel percorso di destinazione di ripristino.

   Se questa opzione non viene selezionata, il file o cartella verrà ripristinato direttamente nella cartella di destinazione.

   Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt e C:\Folder1\SubFolder2\B.txt e durante il ripristino è stata specificata la destinazione D:\Restore.

   - Se si sceglie di ripristinare i file A.txt e B.txt individualmente, la destinazione dei file ripristinati corrisponderà a D:\Restore\A.txt e D:\Restore\B.txt. La directory principale sopra il livello di file specificato non verrà ricreata.
   - Se si sceglie di eseguire il ripristino a partire dal livello SubFolder2, la destinazione dei file ripristinati corrisponderà a D:\Restore\SubFolder2\A.txt e D:\Restore\SubFolder2\B.txt. La directory principale al di sopra del livello di cartella specificato non verrà ricreata.

   Se questa opzione è selezionata, verrà ricreato l'intero percorso della directory principale per i file o le cartelle (compreso il nome del volume) nella cartella di destinazione. Se i file o le cartelle da ripristinare appartengono allo stesso nome del volume, il percorso della directory principale di destinazione non includerà tale nome del volume. Tuttavia, se i file o le cartelle da ripristinare appartengono a diversi nomi di volume, il percorso della directory principale di destinazione includerà il nome del volume.

   Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt, C:\Folder1\SubFolder2\B.txt e E:\Folder3\SubFolder4\C.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

   - Se si desidera ripristinare soltanto il file A.txt, la destinazione del file ripristinato corrisponderà a D:\Restore\ Folder1\SubFolder2\A.txt (verrà ricreata l'intera directory principale, eccetto il nome del volume).
   - Se si esegue il ripristino di entrambi i file A.txt e B.txt, la destinazione dei file ripristinati corrisponderà a D:\Restore\C\Folder1\SubFolder2\A.txt e D:\Restore\E\Folder3\SubFolder4\C.txt (verrà ricreata l'intera directory principale, compreso il nome del volume).

4. Specificare la password di crittografia in **Password di crittografia per la copia file.**

5. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Riepilogo ripristino**.

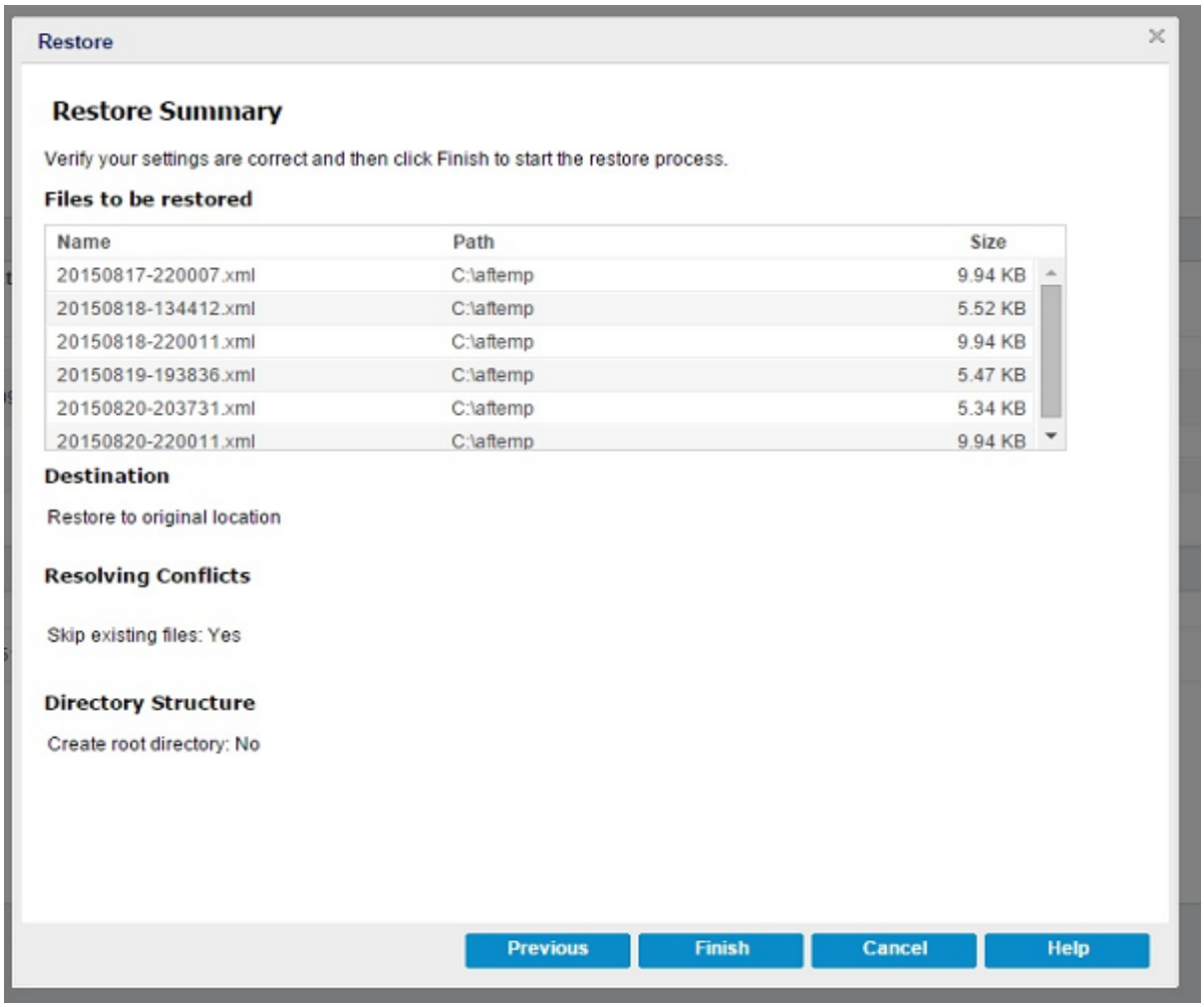
   Le opzioni di ripristino vengono definite per il ripristino da una copia file.

Ripristino del contenuto del punto di ripristino

Una volta definite le opzioni di ripristino, verificare che le impostazioni siano corrette e confermare il processo di ripristino. Il **riepilogo di ripristino** consente di verificare tutte le opzioni di ripristino definite e, se necessario, modificarle.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Riepilogo ripristino**, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



- Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
- Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

Il contenuto di copia file viene ripristinato.

Verifica del corretto ripristino del contenuto

Una volta completato il processo di ripristino, verificare il ripristino del contenuto nella destinazione specificata.

Effettuare le operazioni seguenti:

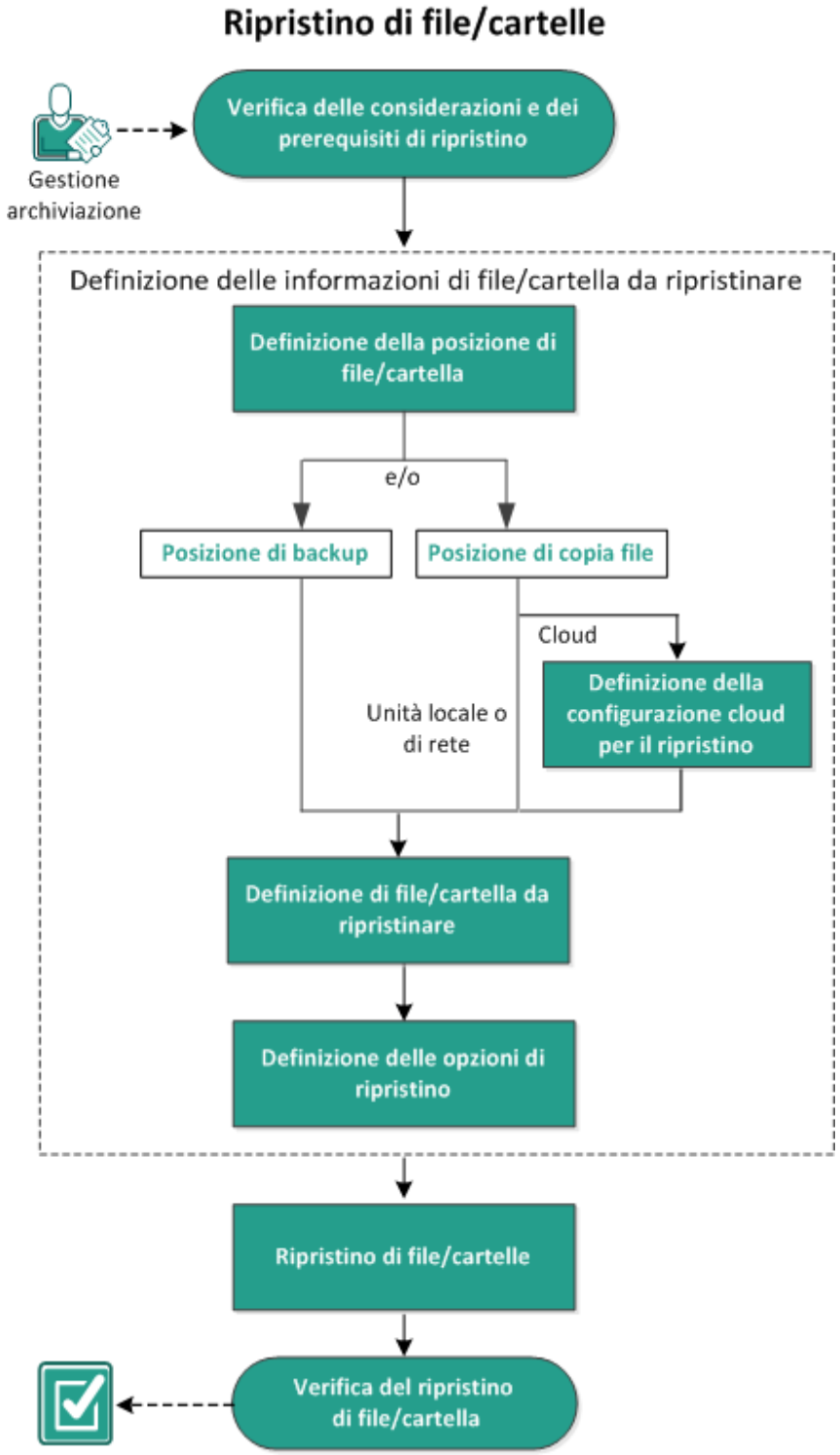
1. Accedere alla casella di posta di destinazione.
2. Verificare l'elemento della casella di posta ripristinato.
3. Verificare che il contenuto sia stato ripristinato.

   Il contenuto ripristinato è stato verificato correttamente.

Ripristino di file/cartelle

Al completamento di ogni backup, Arcserve UDP include tutti i file e le cartelle nell'immagine snapshot del backup. Questo metodo di ripristino consente di specificare esattamente i file e le cartelle che si desidera ripristinare.

Il diagramma seguente illustra il processo di ripristino per file/cartelle specifici:



Per eseguire il ripristino di file/cartelle, procedere come segue:

1. Verifica delle considerazioni e dei prerequisiti di ripristino
2. Definizione delle informazioni di file/cartella da ripristinare
    a. Definizione della posizione di file/cartella
        - Definizione della configurazione cloud per il ripristino
    b. Definizione di file/cartella da ripristinare
    c. Definizione delle opzioni di ripristino
3. Ripristino di file/cartelle
4. Verifica del ripristino di file/cartella

Verifica delle considerazioni e dei prerequisiti di ripristino

Verificare i seguenti prerequisiti prima di procedere al ripristino:

- È necessario disporre di almeno un backup o una copia del file per il ripristino.
- È necessario disporre di una destinazione di backup o copia di file valida e accessibile da cui eseguire il ripristino del contenuto di backup o copia del file.
- È necessario disporre di una posizione di destinazione valida e accessibile in cui ripristinare il contenuto di backup o di copia del file.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Verificare le seguenti considerazioni sul ripristino:

- Per un punto di ripristino che non dispone di un catalogo di file system creato, per far sì che sia possibile accedere e selezionare file/cartelle da ripristinare dall'interfaccia utente, prima di eseguire il backup l'account o gruppo dovrebbe avere accesso a tutti i file e cartelle su tutti i volumi con accesso di lettura e elenco.

  Il sistema locale (SYSTEM) o il gruppo di amministratori predefinito (BUILTIN\Administrators) deve essere aggiunto agli elenchi di controllo delle cartelle in modo che l'agente Arcserve UDP (Windows) sia in grado di accedere a un backup senza la necessità di generare un catalogo file system. Altrimenti, l'agente Arcserve UDP (Windows) non sarà in grado di accedere alle cartelle dall'interfaccia utente del ripristino.

- (Facoltativo) Comprendere il funzionamento del processo di ripristino. Per ulteriori informazioni, consultare la sezione Funzionamento del ripristino a livello di file.

  Nota: Il processo di ripristino da una posizione di copia del file è simile al ripristino da una posizione di backup.

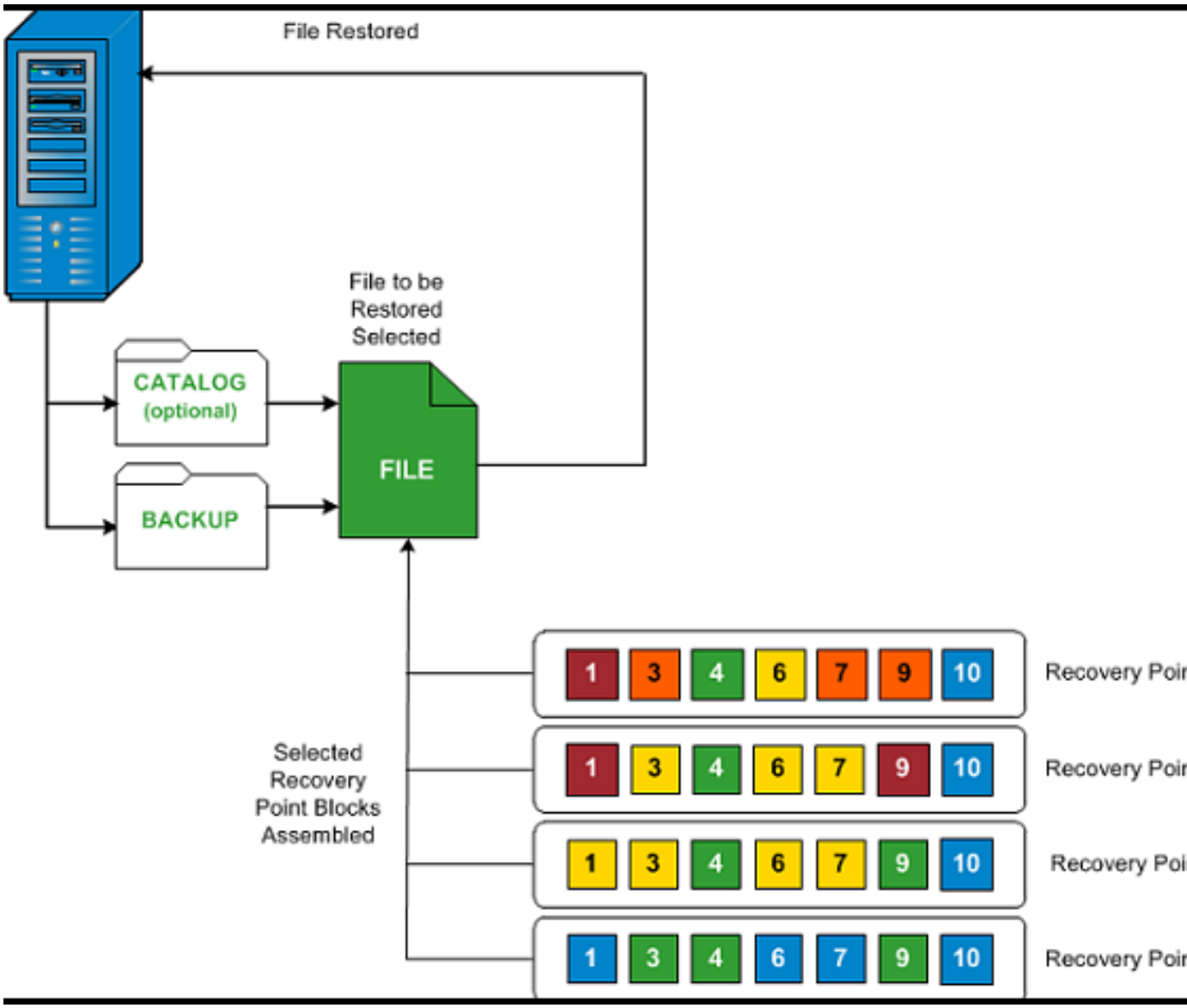
- (Facoltativo) Rivedere i file ignorati durante il ripristino. Per ulteriori informazioni, consultare la sezione File ignorati durante il ripristino.

Funzionamento del ripristino a livello di file

Durante il processo di backup a livello di blocco, ciascun file di backup include un insieme di blocchi che definiscono tale file. Nel caso in cui sia necessario ripristinare un file specifico, è possibile individuare il file che si desidera ripristinare e il punto di ripristino che si desidera utilizzare. L'agente Arcserve UDP (Windows) esegue la raccolta della versione dei blocchi utilizzati per il punto di ripristino del file specificato, li riassembla ed esegue il ripristino del file.

Nota: quando vengono specificate le impostazioni di backup, è possibile creare un catalogo di file durante il backup. Questo catalogo di file consente di accedere più velocemente alle sessioni di backup durante il ripristino. Se si sceglie di non creare il catalogo durante il backup, sarà tuttavia possibile crearlo in un secondo momento.

Nel seguente diagramma di flusso è possibile visualizzare il processo di ripristino di un file specifico in Arcserve UDP.


File Restored
File to be Restored Selected
CATALOG (optional)
BACKUP
FILE
Selected Recovery Point Blocks Assembled
1 3 4 6 7 9 10
Recovery Poir
1 3 4 6 7 9 10
Recovery Poir
1 3 4 6 7 9 10
Recovery Poi
1 3 4 6 7 9 10
Recovery Poir

File ignorati durante il ripristino

Durante un ripristino con l'agente Arcserve UDP (Windows), è possibile che alcuni file vengano ignorati intenzionalmente.

I file e le cartelle nella tabella seguente vengono ignorati durante il ripristino se si verificano le due condizioni seguenti:

- I file vengono ignorati se esistono prima del ripristino e l'opzione di conflitto è Ignora file esistenti.
- I file e le cartelle elencati nella tabella seguente vengono ignorati poiché non costituiscono un componente importante di Windows o dell'agente Arcserve UDP (Windows).

Sistema operativo	Cartella o posizione	Nome di file o cartella	Note
Tutto	Cartella root di ciascun volume	CAVolTrc.dat	Utilizzato dal driver di rilevamento di Arcserve UDP.
		cavoltrcsnapshot.dat	
		System Volume Information*	Utilizzato per salvare file/cartelle con un sistema Windows, ad esempio file di copia shadow del volume.
		RECYCLER*	Utilizzato solamente su partizioni NTFS. Contiene un cestino per ogni utente che accede al computer, ordinato in base al rispettivo ID di sicurezza (SID).
		$Recycle.Bin*	Quando si elimina un file da Gestione risorse o da Risorse del computer, il file viene archiviato nel cestino finché non si svuota il cestino o si ripristina il file.
	Qualsiasi cartella con file di immagini	Thumbs.db	Archivia le immagini di anteprima per la visualizzazione Anteprima di Esplora risorse.
	Cartella root del volume	PageFile.Sys	File di scambio per la memoria virtuale di Windows.
		Hiberfil.sys	File per l'ibernazione usato per salvare i dati di sistema quando si attiva la modalità di ibernazione.

I file e le cartelle seguenti vengono ignorati soltanto quando si esegue il ripristino nella posizione originale o in una posizione alternativa:

Sistema	Cartella o posizione	Nome di file o cartella	Nota

ope-rativo			
Tutto	Cartella specificata nel record di valore in: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Tutti i file/cartelle (in modo ricorsivo)	La cartella contiene un file .dll memorizzato nella cache che viene utilizzato per il controllo dei file di sistema (SFC). I contenuti della directory di cache dll di sistema vengono ricostruiti mediante SFC.
	%SystemRoot%\SYSTEM32\dllCache		
	Cartella principale di quorum_device	MSCS*	Utilizzato per Microsoft Cluster Server.

	%SystemRoot%\SYSTEM32\	perf?00?.dat	Dati relativi alle prestazioni utilizzati dal contatore delle prestazioni di Windows.

		perf?00?.bak	

		CATROOT*	Utilizzato per le firme digitali dei record Protezione file Windows (WFP) installati nel sistema operativo (ad esempio DLL, EXE, SYS, OCX e così via) per evitare che siano eliminati o sostituiti con versioni precedenti.
	%SystemRoot%\inetsrv\	metabase.bin	File binario metabase delle versioni di IIS precedenti alla 6.0.
	File o cartella specificato nel valore eccetto l'Archivio comune SIS in HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup	Tutti i file/cartelle (in modo ricorsivo)	I file e le cartelle non devono essere sottoposti a backup e ripristino. Per ulte-

			riori informazioni, fare clic sul seguente collegamento.
XP W2003	Volume di sistema	NTLDR	Caricatore di avvio principale.
		BOOT.INI	Contiene la configurazione di avvio (se assente, il valore predefinito NTLDR sarà impostato su \Windows nella prima partizione del primo disco rigido).
		NTDETECT.COM	Richiesto per l'avvio del sistema operativo basato su NT. Rileva le informazioni hardware di base necessarie per il

			corretto avvio.
Vista e sistemi successivi	Cartella root del volume di sistema	boot*	Cartella di avvio per Windows.
		bootmgr	File di Windows Boot Manager.
		EFI\Microsoft\Boot*	Usata per l'avvio EFI.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Archivia i file di traccia ETW (estensione .etl) per le sessioni di traccia degli eventi in tempo reale.
		config\RegBack*	Backup della tabella del registro di sistema attuale.
Win8 e sistemi successivi	Volume di sistema	swapfile.sys	File del controller di sistema, in genere di circa 256 MB. Viene utilizzato da applicazioni come

			Metro che non si adattano alle caratteristiche di paging tradizionali (schema di utilizzo, crescita, spazio riservato) di pagefile.sys.
		BOOTNXT	Utilizzato per l'avvio da un sistema operativo diverso da Windows 8. Creato durante l'abilitazione delle opzioni di avvio e aggiornato da Windows.

Il Registro attività fornisce le seguenti informazioni:

- Informazioni di data e ora: File system jobxxxx ignorati. È possibile utilizzare l'opzione Ripristino bare metal (BMR) per ripristinarli.
- Informazioni di data e ora: File o directory jobxxxx ignorati. L'elenco dei file o delle directory ignorati è disponibile in: C:\Programmi\Arcserve\Unified Data Protection\Engine\Logs\Restore-<YYYYMMDD>-<hhmmss>-<Process ID>-<Job ID>.log.

Definizione delle informazioni di file/cartella da ripristinare

Arcserve UDP fornisce un'opzione per individuare e ripristinare un determinato file o cartella. L'obiettivo di un processo di ripristino è quello di identificare rapidamente i dati necessari e di recuperarli dalla posizione di backup appropriata. Per ciascun processo di ripristino è richiesta un'origine e una destinazione.

Il processo interessato nel ripristino mediante individuazione di file/cartelle è il seguente:

1. Definizione della posizione di file/cartella
   - Definizione della configurazione cloud per il ripristino
2. Definizione di file/cartella da ripristinare
3. Definizione delle opzioni di ripristino

Definizione della posizione di file/cartella

Utilizzare l'opzione **Trova file/cartelle** per ripristinare file e cartelle. Questo metodo di ripristino consente di specificare esattamente i file o le cartelle da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere alla finestra di dialogo per la selezione del metodo di ripristino in uno dei modi seguenti:

   Da Arcserve UDP:

   a. Accedere ad Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

      Nota: Viene effettuato automaticamente l'accesso al nodo agente e la finestra di dialogo per la selezione del metodo di ripristino viene visualizzata dal nodo agente.

   Dall'agente Arcserve UDP (Windows):

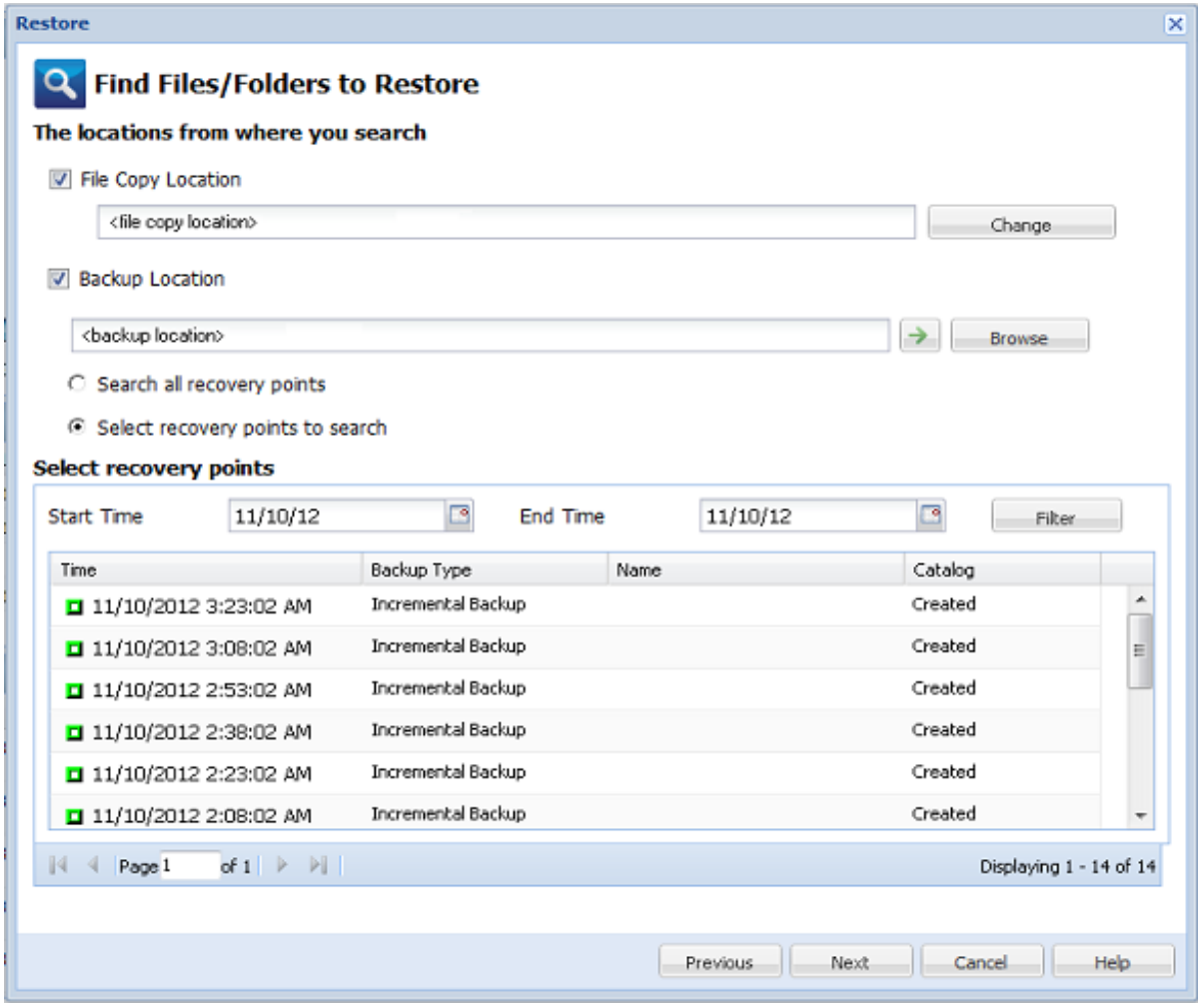
   a. Accedere all'agente Arcserve UDP (Windows).

   b. Dalla pagina principale selezionare **Ripristino**.

   Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

2. Fare clic sull'opzione **Trova file/cartelle da ripristinare**.

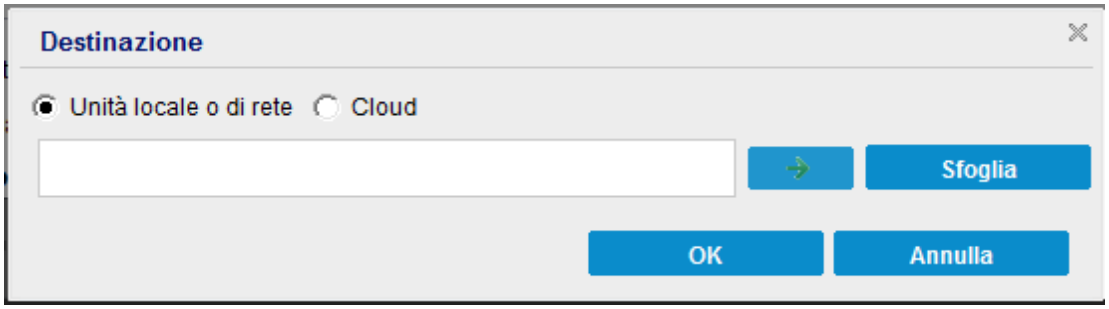
   Verrà visualizzata la finestra di dialogo **Trova file/cartelle da ripristinare**.



3. Selezionare la casella di controllo **Posizione di copia file** e fare clic sul pulsante **Cambia** per modificare la posizione con la destinazione in cui sono archiviate le immagini di copia file.

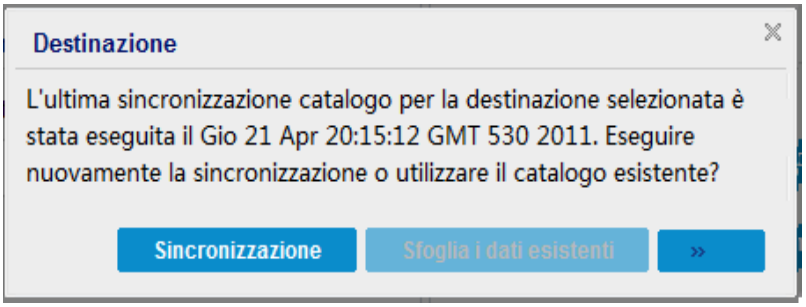
   Viene visualizzata la finestra di dialogo **Destinazione** in cui è possibile selezionare l'**unità locale, di rete** o **cloud**.

   Nota: per impostazione predefinita, i campi **Posizione di backup** e **Posizione di copia file** visualizzano il percorso corrispondente usato per le destinazioni più recenti di backup/copia file.



- L'opzione **Unità locale o di rete** consente di specificare o cercare la posizione di archiviazione delle immagini di copia file.
- Fare clic sull'icona di convalida con la freccia verde per verificare che l'accesso alla posizione di origine sia stato eseguito correttamente.
- Selezionando **Cloud**, specificare una posizione cloud oppure fare clic sul pulsante **Configura** per visualizzare la finestra di dialogo **Configurazione cloud**. Per ulteriori informazioni, consultare la sezione Definizione della configurazione cloud per il ripristino.

  Indipendentemente dal tipo di selezione (**ripristino da un'unità locale, da un'unità di rete** o da **cloud**), quando la destinazione viene modificata verso un'altra posizione, verrà visualizzata una finestra di dialogo in cui viene richiesto se si desidera eseguire una nuova sincronizzazione del catalogo o leggere il catalogo esistente.



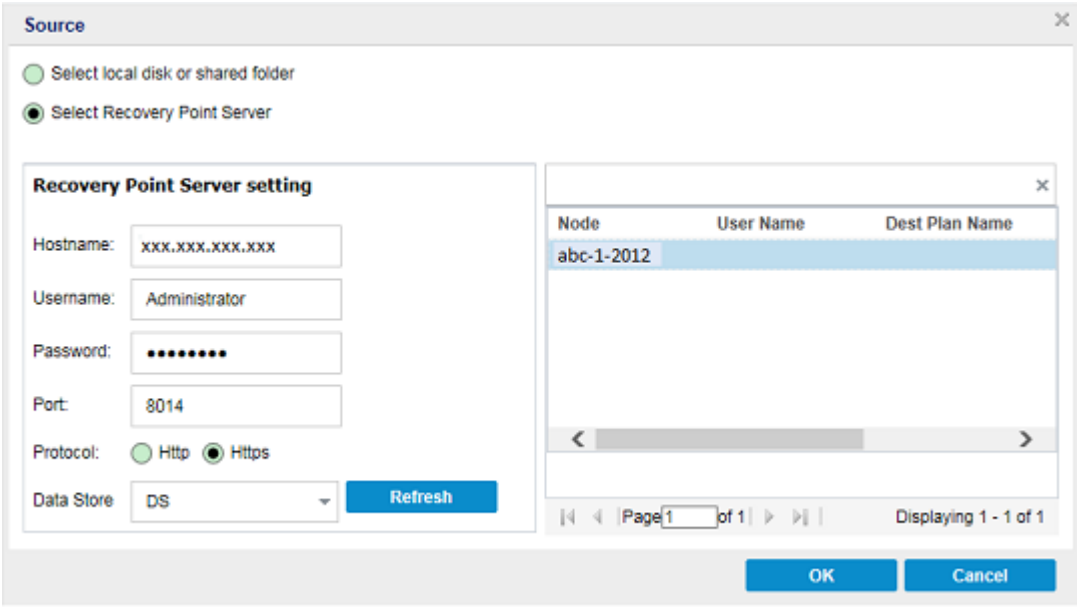
  - Se si esegue la sincronizzazione del catalogo per la prima volta, il pulsante **Sfoglia i dati esistenti** è disabilitato perché il catalogo di copia file non esiste in locale.
  - Se una sincronizzazione di catalogo è stata eseguita precedentemente, questa finestra di dialogo conterrà dettagli relativi all'ultima sincronizzazione del catalogo a partire dalla destinazione. Se vengono eseguiti più processi di copia file dopo l'ora indicata, il catalogo potrebbe non essere sincronizzato. È possibile selezionare l'opzione **Sincronizzazione** per verificare che il catalogo di copia file sia aggiornato.

    1. Fare clic su **Sincronizzazione** per scaricare sul computer locale il catalogo di copia file dalla destinazione di copia file specificata e consentire un'esplorazione più veloce.

    2. Fare clic su **Sfoglia i dati esistenti** per utilizzare il catalogo di copia file disponibile in locale senza ripeterne il download o la sincronizzazione.

4. Selezionare la casella di controllo **Posizione di backup** e fare clic su **Cambia** per modificare la posizione di backup.

Viene visualizzata la finestra di dialogo **Origine** in cui è possibile selezionare la posizione di backup.



5. Selezionare una delle seguenti opzioni nella finestra di dialogo **Origine**:

   Selezione di un disco locale o una cartella condivisa

   a. Specificare o accedere al percorso di archiviazione delle immagini di backup e selezionare l'origine di backup appropriata.

      Per verificare la connessione al percorso specificato, fare clic sulla freccia verde. Se necessario, immettere le credenziali Nome utente e Password per poter accedere alla posizione di origine.

      Viene visualizzata la finestra di dialogo **Selezionare la posizione di backup**.

   b. Selezionare la cartella di archiviazione dei punti di ripristino e fare clic su **OK**.

      La finestra di dialogo **Selezionare la posizione di backup viene chiusa** e la posizione di backup viene visualizzata nella finestra di dialogo **Origine**.

   c. Fare clic su **OK**.

      I punti di ripristino sono elencati nella finestra di dialogo **Trova file/cartelle da ripristinare**.

   Selezione di un Recovery Point Server

   a. Specificare i dettagli dell'impostazione Recovery Point Server e fare clic su **Aggiorna**.

Tutti gli agenti vengono elencati nella colonna **Data Protection Agent** (Agente di protezione dati) nella finestra di dialogo **Origine**.

b. Selezionare l'agente dall'elenco visualizzato e fare clic su **OK**.

I punti di ripristino sono elencati nella finestra di dialogo **Trova file/cartelle da ripristinare**.

Nota: Se si seleziona un agente diverso e se i punti di ripristino sono crittografati, si deve fornire la password di crittografia quando richiesto.

6. Selezionare una delle opzioni seguenti per cercare punti di ripristino:

Cerca tutti i punti di ripristino

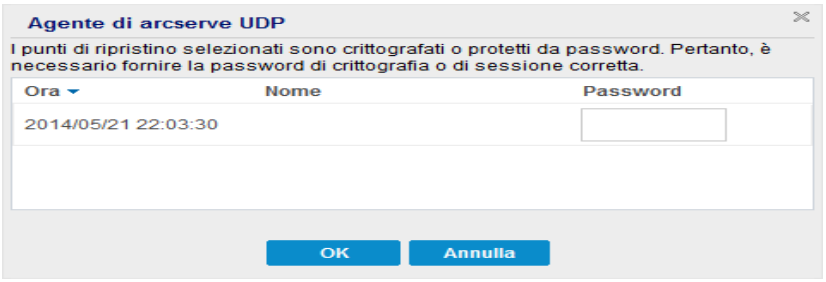
Cerca il file o la cartella in tutti i punti di ripristino archiviati nella posizione fornita. Specificare il file o la cartella di cui si desidera effettuare la ricerca nella finestra di dialogo **Trova file/cartelle da ripristinare**.

Seleziona punti di ripristino per la ricerca

Visualizza i punti di ripristino compresi nel periodo di tempo specificato. È possibile specificare l'ora di inizio e l'ora di fine, quindi selezionare il punto di ripristino dal periodo di tempo specificato.

7. Selezionare il punto di ripristino e fare clic su **Avanti**.

Nota: se si è selezionato un agente diverso nella finestra di dialogo **Origine** e se i punti di ripristino sono crittografati, viene visualizzata la finestra di dialogo Crittografia. Immettere la password e fare clic su **OK**.



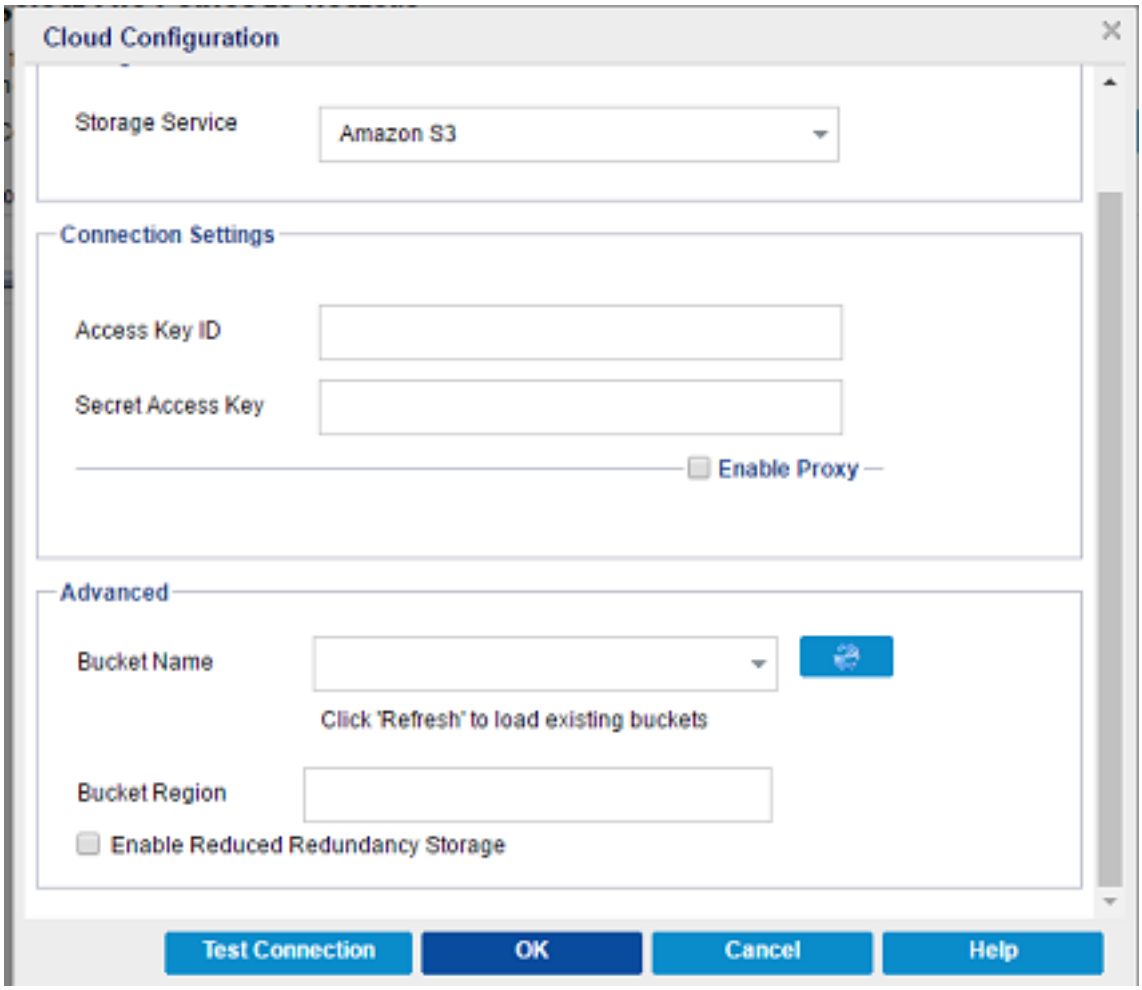
Verrà visualizzata la finestra di dialogo **Trova file/cartelle da ripristinare**.

Viene specificata la posizione di **backup o di copia file**.

Definizione della configurazione cloud per il ripristino

Nota: la procedura riportata di seguito è valida solo in caso di ripristino di un file/-cartella da una posizione cloud di copia file.

Dalle opzioni **Sfoglia copia file** o **Trova file/cartelle da ripristinare**, fare clic sul pulsante **Configura** per visualizzare la finestra di dialogo **Configurazione cloud**.



Effettuare le operazioni seguenti:

1. Utilizzare il menu a discesa della finestra di dialogo **Configurazione cloud** per selezionare il tipo di fornitore cloud che si desidera utilizzare per il ripristino. Le opzioni disponibili sono **Amazon S3**, **Windows Azure**, **FUJITSU Hybrid IT Service FJcloud-O** e **Eucalyptus-Walrus**. Il fornitore selezionato per impostazione predefinita è **Amazon S3**. Per ulteriori informazioni su Fujitsu Cloud (Windows Azure) e FUJITSU Hybrid IT Service FJcloud-O, consultare le sezioni Panoramica e Registrazione.

   Nota: dopo avere codificato il nome del bucket, se la lunghezza del percorso è superiore a 170 caratteri, Eucalyptus-Walrus non sarà in grado di eseguire la copia dei file.

2. Specificare le **opzioni di configurazione**.

   Le opzioni di configurazione disponibili per ciascun fornitore cloud sono simili (con alcune differenze terminologiche). In caso di differenze viene fornita una descrizione.

   a. Specificare le **impostazioni di connessione**.

      URL del fornitore

      Specifica l'indirizzo URL del provider cloud.

      Per Amazon S3 e Windows Azure, l'URL del fornitore viene compilato automaticamente. Per Eucalyptus-Walrus, è invece necessario immettere manualmente l'URL del fornitore, nel formato specificato.

      ID del codice di accesso/Nome account/ID query

      Indica l'utente che richiede l'accesso a questa posizione.

      Per questo campo, Amazon S3 utilizza l'ID del codice di accesso, Windows Azure. FUJITSU Hybrid IT Service FJcloud-O utilizza Nome account, mentre Eucalyptus-Walrus utilizza ID query.

      Codice di accesso segreto/Chiave privata

      Poiché il codice di accesso non viene crittografato, la chiave privata si utilizza per verificare l'autenticità della richiesta di accesso.

      Importante! Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

      Per questo campo, Amazon S3 utilizza Codice di accesso segreto. Windows Azure, FUJITSU Hybrid IT Service FJcloud-O ed Eucalyptus-Walrus uilizzano la chiave segreta.

      Abilita proxy

      Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l’autenticazione per il server proxy. Sarà quindi necessario fornire le informazioni di autenticazione (nome utente e password) richieste per utilizzare il server proxy.

      (La funzionalità di proxy non è disponibile per Eucalyptus-Walrus).

b. Definizione delle **impostazioni avanzate**.

Nome bucket/Contenitore

Tutti i file e le cartelle spostati o copiati sul sistema del fornitore cloud vengono archiviati e organizzati in bucket o contenitori. I bucket sono dei contenitori di file utilizzati per raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

Selezionare un nome per il bucket dall'elenco a discesa. Per aggiornare l'elenco dei bucket disponibili, fare clic sul pulsante **Aggiorna**.

Per questo campo, Amazon S3 ed Eucalyptus-Walrus utilizzano Nome bucket. Windows Azure e FUJITSU Hybrid IT Service FJcloud-O utilizzano il contenitore.

Area di bucket

Fa riferimento all'area di bucket in Amazon e FUJITSU Hybrid IT Service FJcloud-O.

Numero di contratto

Indica il numero del contratto fornito da FUJITSU Hybrid IT Service FJcloud-O.

ID progetto

Indica l'ID del progetto generato da FUJITSU Hybrid IT Service FJcloud-O.

Abilita riduzione di archiviazione dei dati ridondanti

Con Amazon S3, è possibile selezionare questa opzione per abilitare la riduzione di archiviazione dei dati ridondanti (RRS). L'opzione di archiviazione RSS di Amazon S3 consente di ridurre i costi mediante l'archiviazione dei dati non critici e riproducibili a livelli di ridondanza inferiori rispetto ai livelli di archiviazione standard di Amazon S3. Entrambe le opzioni di archiviazione (con ridondanza standard e ridotta) consentono di archiviare i dati su più dispositivi e periferiche. Tuttavia la riduzione di archiviazione dei dati ridondanti consente di eseguire un numero minore di repliche, riducendo in tal modo i costi. L'archiviazione standard di Amazon S3 e la riduzione di archiviazione dei dati ridondanti presentano gli stessi valori di latenza e velocità. Per impostazione predefinita questa opzione non è selezionata, in quanto Amazon S3 utilizza l'opzione di archiviazione standard.

3. Per verificare la connessione al percorso cloud specificato, fare clic su **Verifica connessione**.

4. Fare clic su **OK** per uscire dalla finestra di dialogo **Configurazione cloud**.

Definizione di file/cartella da ripristinare

Dopo avere specificato la posizione di backup o di copia file, cercare il nome del file o della cartella da ripristinare. Se il file presenta più versioni di copia, tutte le versioni vengono elencate per data in ordine crescente.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Trova file/cartelle da ripristinare**, specificare l'oggetto da cercare (nome del file o della cartella da ripristinare).

   Nota: Il campo **Nome file** supporta la ricerca per nome completo e con caratteri jolly. Se non si conosce il nome file completo, è possibile semplificare i risultati della ricerca immettendo i caratteri jolly "*" e "?" nel campo Nome file.

   I caratteri jolly supportati per il nome dei file o delle cartelle sono i seguenti:

   - Utilizzare l'asterisco per sostituire zero o più caratteri nel nome di un file o di una cartella.
   - Utilizzare il punto interrogativo per sostituire un singolo carattere nel nome di un file o di una cartella.

   Ad esempio, specificando *.txt, la ricerca restituirà tutti i file con estensione .txt.

2. (Facoltativo) Immettere un percorso per filtrare ulteriormente la ricerca e specificare se includere le directory secondarie.

3. Fare clic su **Trova** per avviare la ricerca.

   I risultati della ricerca vengono visualizzati. Se i file dispongono di più versioni di copia, tutte le versioni verranno elencate per data in ordine crescente. La ricerca indica anche se il file è stato sottoposto a backup o se è stato copiato.

4. Selezionare la versione (occorrenza) del file o della cartella da ripristinare e fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Opzioni di ripristino**.

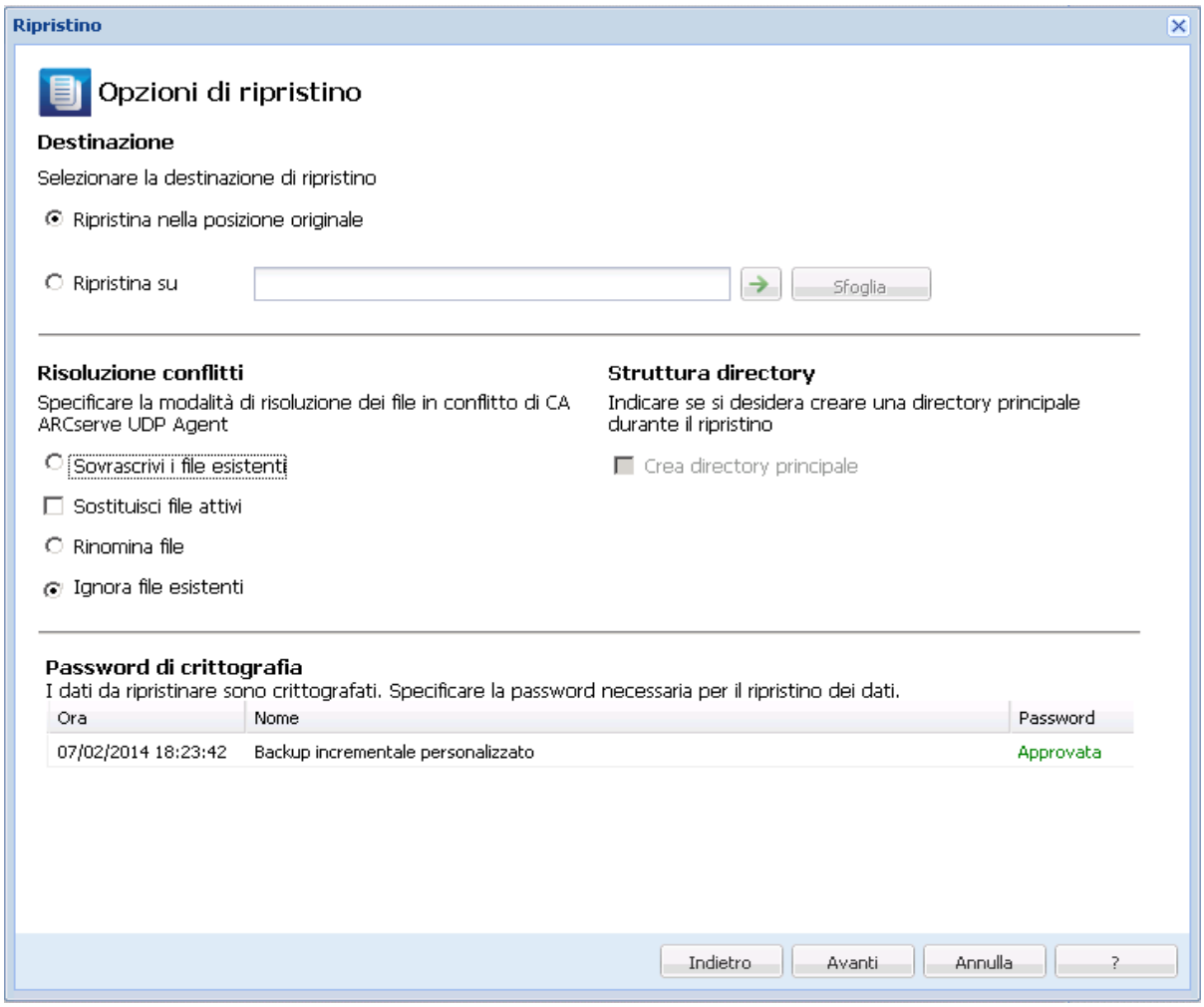
   Viene specificato il nome di file/cartella da ripristinare.

Definizione delle opzioni di ripristino

Dopo avere specificato il file o la cartella da ripristinare, definire le opzioni di ripristino per l'oggetto selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Opzioni di ripristino**, specificare la destinazione di ripristino.



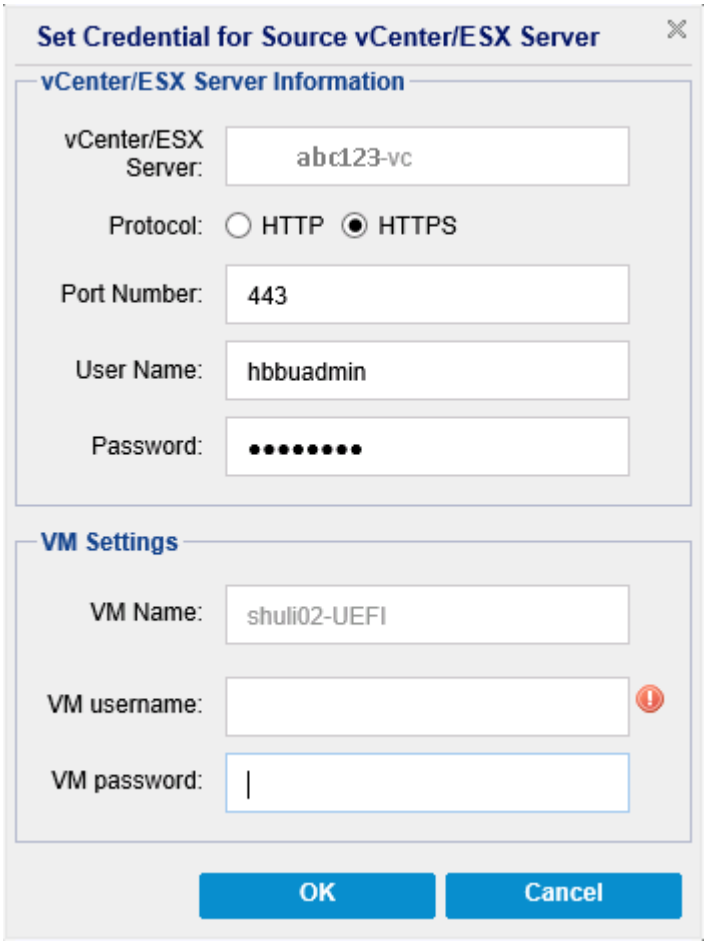
Le opzioni di destinazione disponibili sono:

Ripristina in posizione originale

Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

Nota: se è stato eseguito il backup del punto di ripristino tramite il backup senza agente basato su host, per eseguire il ripristino sulla posizione originale sarà necessario eseguire nuovamente il ripristino sul computer virtuale. In questo caso, viene visualizzata una finestra di dialogo. È possibile immettere le credenziali dell'hypervisor e il sistema operativo del computer virtuale.

Valido per il computer virtuale VMware:



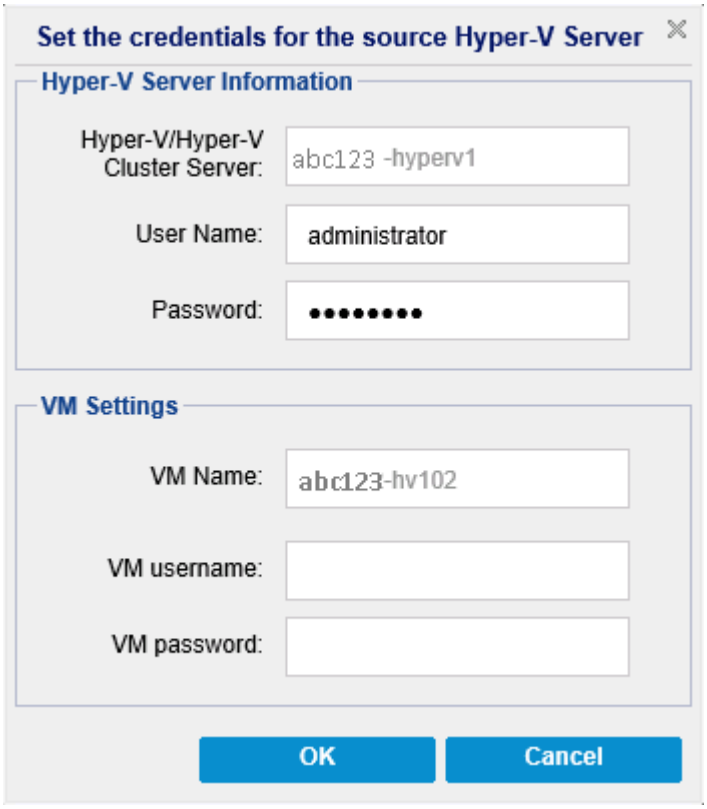
Nota: per poter creare o scrivere i file all'interno del computer virtuale, prendere in considerazione i seguenti requisiti per le impostazioni e l'autorizzazione di account del computer virtuale:

- Gli strumenti VMware vengono installati e sono in esecuzione.
- Il firewall deve consentire la condivisione di file e stampanti.
- L'account può appartenere all'amministratore locale integrato, all'amministratore di dominio integrato o al dominio appartenente al gruppo degli amministratori locali. Se vengono utilizzati altri account:

- Disabilitare l'accesso remoto a UAC. Per disabilitare l'accesso UAC remoto, consultare la sezione Importazione di computer virtuali con un account amministrativo aggiuntivo.
- Disabilitare l'UAC nel Local Security Policy disattivando l'impostazione di esecuzione di tutti gli amministratori nella modalità di approvazione dell'amministratore in secpol.msc -> Criteri locali -> Opzioni di protezione. (Secpol.msc è l'editor delle policy di protezione di Microsoft).

  Importante: non disabilitare l'UAC nella finestra di dialogo Impostazioni di Controllo account utente accessibile dal pannello di controllo.

Per il computer virtuale Hyper-V:



Nota: per poter creare o scrivere i file all'interno del computer virtuale, prendere in considerazione i seguenti requisiti per le impostazioni e l'autorizzazione di account del computer virtuale:

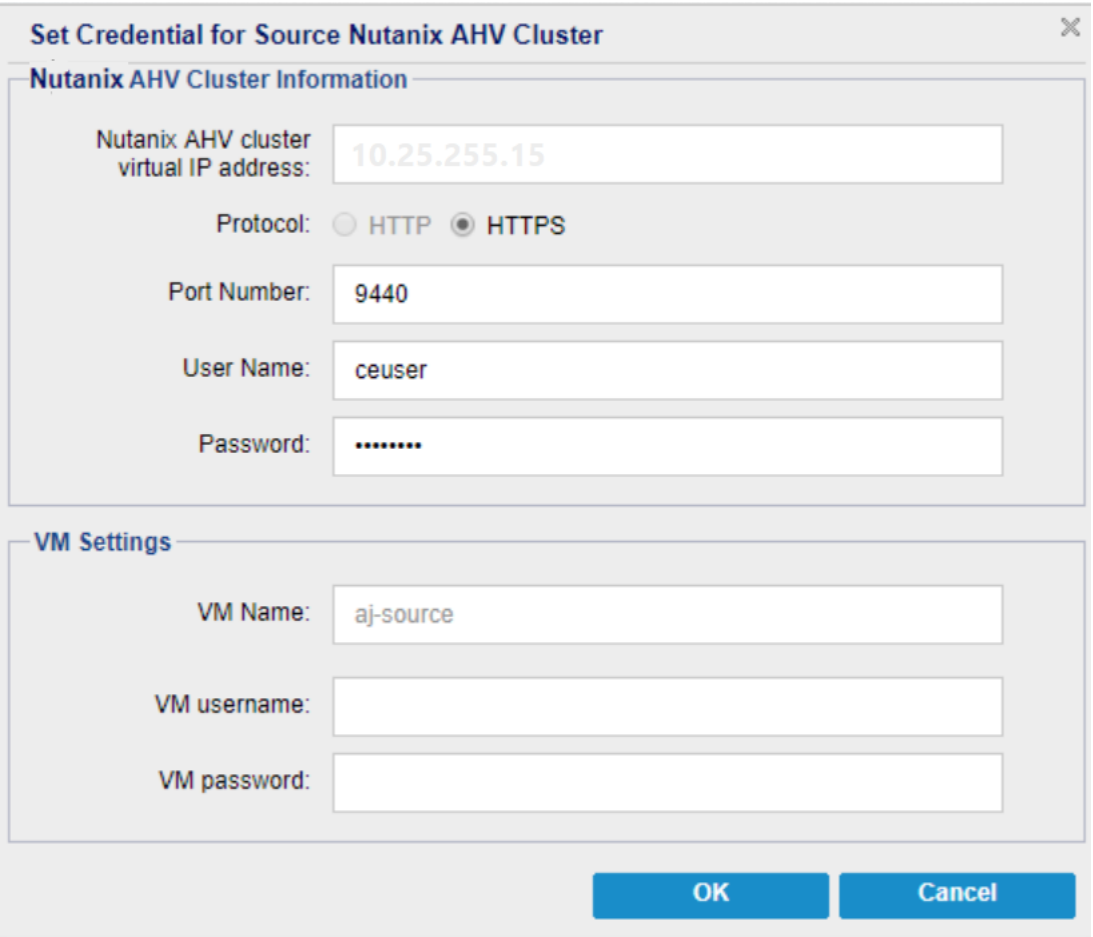
- I servizi di integrazione Hyper-V devono essere installati e in esecuzione.
- Il firewall deve consentire la condivisione di file e stampanti.

- L'account può appartenere all'amministratore locale integrato, all'amministratore di dominio integrato o al dominio appartenente al gruppo degli amministratori locali. Se vengono utilizzati altri account:

  Disabilitare l'accesso remoto a UAC. Per disabilitare l'accesso UAC remoto, consultare la sezione Importazione di computer virtuali con un account amministrativo aggiuntivo.

- Se il sistema operativo guest del computer virtuale è Windows versione Client (ad esempio, Windows 10), è necessario configurare manualmente il firewall per consentire Windows Management Instrumentation (WMI).

Per il computer virtuale Nutanix



Note: per poter creare o scrivere i file all'interno del computer virtuale, tenere conto dei requisiti seguenti per le impostazioni e l'autorizzazione dell'account del computer virtuale:

- Il firewall deve consentire la condivisione di file e stampanti.

- L'account può appartenere all'amministratore locale integrato, all'amministratore di dominio integrato o al dominio appartenente al gruppo degli amministratori locali. Se vengono utilizzati altri account:

  Disabilitare l'accesso remoto a UAC. Per disabilitare l'accesso UAC remoto, consultare la sezione Importazione di computer virtuali con un account amministrativo aggiuntivo.
- Il firewall deve consentire la Strumentazione gestione Windows (WMI).

Ripristina su

Esegue il ripristino alla posizione specificata. Per verificare la connessione al percorso specificato, fare clic sulla freccia verde. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso.

2. Specificare l'opzione **Risoluzione conflitti** che verrà eseguita da Arcserve UDP in caso di conflitti durante il processo di ripristino.

   Le opzioni disponibili sono:

   Sovrascrivi i file esistenti

   Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dai file di backup, indipendentemente dalla loro presenza sul computer.

   Sostituisci file attivi

   Consente di sostituire i file attivi dopo il riavvio. Se durante il tentativo di ripristino l'agente Arcserve UDP (Windows) rileva che l'utente sta accedendo al file esistente o che quest'ultimo è momentaneamente in uso, tale file non viene sostituito immediatamente. Per evitare l'insorgere di problemi, i file attivi vengono sostituiti al riavvio successivo del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita con il riavvio successivo).

   Questa opzione è disponibile solo se l'opzione **Sovrascrivi i file esistenti** è stata selezionata.

   Nota: se l'opzione non è selezionata, tutti i file attivi verranno ignorati durante il processo di ripristino.

   Rinomina file

   Se il nome file esiste già, consente di creare un nuovo file. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno quindi ripristinati nel nuovo file.

   Ignora file esistenti

Ignora e non sovrascrive (sostituisce) i file esistenti contenuti nella destinazione di ripristino. Solo gli oggetti inesistenti sul computer verranno ripristinati dai file di backup.

Impostazione predefinita: Ignora file esistenti.

3. Specificare la **struttura di directory** per creare una directory principale durante il ripristino.

Crea directory principale

Se l'immagine di backup acquisita contiene una struttura delle directory principali, Arcserve UDP ricrea la stessa struttura della directory principale nel percorso di destinazione di ripristino.

Se questa opzione non viene selezionata, il file o cartella verrà ripristinato direttamente nella cartella di destinazione.

Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt e C:\Folder1\SubFolder2\B.txt e durante il ripristino è stata specificata la destinazione D:\Restore.

- Se si sceglie di ripristinare i file A.txt e B.txt individualmente, la destinazione dei file ripristinati corrisponderà a D:\Restore\A.txt e D:\Restore\B.txt. La directory principale sopra il livello di file specificato non verrà ricreata.
- Se si sceglie di eseguire il ripristino a partire dal livello SubFolder2, la destinazione dei file ripristinati corrisponderà a D:\Restore\SubFolder2\A.txt e D:\Restore\SubFolder2\B.txt. La directory principale al di sopra del livello di cartella specificato non verrà ricreata.

Se questa opzione è selezionata, verrà ricreato l'intero percorso della directory principale per i file o le cartelle (compreso il nome del volume) nella cartella di destinazione. Se i file o le cartelle da ripristinare appartengono allo stesso nome del volume, il percorso della directory principale di destinazione non includerà tale nome del volume. Tuttavia, se i file o le cartelle da ripristinare appartengono a diversi nomi di volume, il percorso della directory principale di destinazione includerà il nome del volume.

Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt, C:\Folder1\SubFolder2\B.txt e E:\Folder3\SubFolder4\C.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

- Se si desidera ripristinare soltanto il file A.txt, la destinazione del file ripristinato corrisponderà a D:\Restore\ Folder1\SubFolder2\A.txt (verrà ricreata l'intera directory principale, eccetto il nome del volume).

- Se si esegue il ripristino di entrambi i file A.txt e B.txt, la destinazione dei file ripristinati corrisponderà a D:\Restore\C\Folder1\SubFolder2\A.txt e D:\Restore\E\Folder3\SubFolder4\C.txt (verrà ricreata l'intera directory principale, compreso il nome del volume).

4. La **password di crittografia** della destinazione di copia file viene caricata automaticamente. Se si sceglie una destinazione alternativa per il ripristino, sarà necessario immettere la password manualmente.
5. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Riepilogo ripristino**.

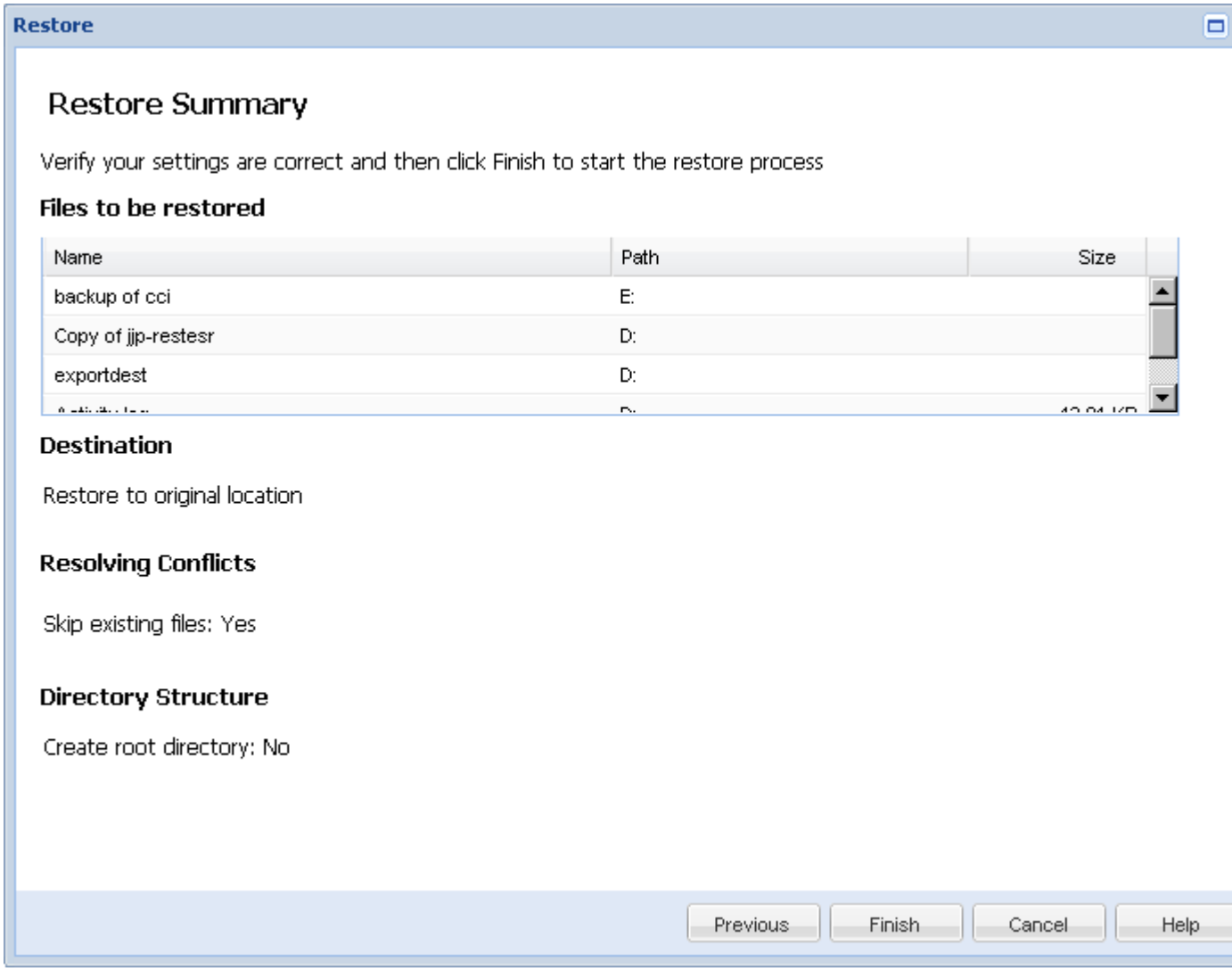
   Le opzioni di ripristino vengono definite per file/cartelle da ripristinare.

Ripristino di file/cartelle

Il **Riepilogo ripristino** consente di verificare tutte le opzioni di ripristino definite e, se necessario, di modificarle.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Riepilogo ripristino**, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



- Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
- Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

Viene ripristinato il file/cartella specificato.

Verifica del ripristino di file/cartella

Dopo il completamento del processo di ripristino, verificare che il file/cartella sia stato ripristinato nella destinazione specificata.

Effettuare le operazioni seguenti:

1. Accedere alla destinazione di ripristino specificata.

   Viene visualizzato un elenco di cartelle.

2. Individuare il file utilizzato per il ripristino del contenuto.

   Ad esempio, se si seleziona di ripristinare il file A.txt nella destinazione di ripristino D:\Restore, accedere al percorso seguente:

   D:\Restore\A.txt.

3. Verificare il contenuto del file/cartella ripristinato.

   Il contenuto ripristinato è stato verificato correttamente.

Esecuzione di un ripristino bare metal tramite un computer virtuale Virtual Standby o un computer virtuale istantaneo

Il processo di ripristino bare metal (BMR) consiste nel ripristino di interi sistemi ed include la reinstallazione del sistema operativo e delle applicazioni software nonché il ripristino di dati e impostazioni. Il processo di ripristino bare metal consente di eseguire facilmente il ripristino completo di un computer, incluso in caso di hardware diverso. È possibile eseguire il ripristino bare metal poiché durante il processo di backup a livello di blocco, l'agente Arcserve UDP (Windows) acquisisce non solo i dati, ma anche tutte le informazioni relative alle seguenti applicazioni:

- Sistema operativo
- Applicazioni installate
- Impostazioni di configurazione
- Driver necessari

  Le informazioni necessarie per l'esecuzione di una ricostruzione completa di interi sistemi da bare metal vengono sottoposte a backup in una serie di blocchi ed archiviate nella posizione di backup.

Per eseguire un ripristino bare metal da un computer virtuale, utilizzare uno dei metodi riportati di seguito:

- Connessione diretta al server ESX mediante l'indirizzo IP
- Aggiunta dell'impostazione DNS corretta nel computer di ripristino bare metal e risoluzione del nome host sull'indirizzo IP

Completare le attività seguenti per eseguire un ripristino bare metal tramite un computer virtuale Virtual Standby o un computer virtuale istantaneo:

1. Verifica delle considerazioni e dei prerequisiti del ripristino bare metal
2. Definizione delle opzioni di ripristino bare metal
   - Recupero mediante computer virtuale Virtual Standby Hyper-V o computer virtuale istantaneo
   - Recupero mediante computer virtuale Virtual Standby VMware o computer virtuale istantaneo
   - Esecuzione del ripristino bare metal in modalità rapida
   - Esecuzione del ripristino bare metal in modalità avanzata
3. Verifica della corretta esecuzione del ripristino bare metal

4. Informazioni di riferimento del ripristino bare metal
5. Risoluzione dei problemi relativi al ripristino bare metal

Verifica delle considerazioni e dei prerequisiti del ripristino bare metal

Verificare l'esistenza dei seguenti prerequisiti prima di procedere a un ripristino bare metal:

- È necessario disporre di una delle seguenti immagini:
  - Un'immagine ISO di ripristino bare metal masterizzata su un CD/DVD
  - Un'immagine ISO di ripristino bare metal masterizzata su una periferica USB portatile

  Nota: L'agente Arcserve UDP (Windows) utilizza un'utilità di kit di avvio per combinare un'immagine WinPE e un'immagine dell'agente Arcserve UDP (Windows) per la creazione di un'immagine ISO del ripristino bare metal. Tale immagine viene quindi masterizzata su un supporto di avvio. Sarà quindi possibile utilizzare tali supporti di avvio (CD/DVD o periferica USB) per avviare il nuovo sistema del computer e consentire l'avvio del processo di ripristino bare metal. Al fine di garantire che l'immagine salvata corrisponda sempre alla versione più recente, creare una nuova immagine ISO per ogni aggiornamento dell'agente Arcserve UDP (Windows).
- Almeno un backup completo.
- Almeno 1 GB di RAM installato sul computer virtuale e il server di origine di cui si sta eseguendo il recupero.
- Se si desidera eseguire il recupero di computer virtuali VMware su computer virtuali VMware configurati come server fisici, verificare che gli strumenti VMware siano installati sul computer virtuale di destinazione.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Verificare le seguenti considerazioni sul ripristino:

- Il processo di ripristino bare metal non cambia, indipendentemente dal metodo utilizzato per la creazione dell'immagine del kit di avvio.

  Nota: Il processo di ripristino bare metal non è in grado di creare spazi di archiviazione. Se il computer di origine dispone di spazi di archiviazione, durante il ripristino bare metal non sarà possibile creare spazi di archiviazione sul computer di destinazione. È inoltre possibile eseguire il ripristino di tali volumi su dischi o volumi regolari oppure creare manualmente spazi di archiviazione prima dell'esecuzione del ripristino bare metal ed eseguire il ripristino dei dati negli spazi di archiviazione creati.

- Il ripristino dei dischi dinamici viene eseguito solo a livello del disco. Se il backup dei dati avviene su un volume locale che risiede su un disco dinamico, tale disco non potrà essere ripristinato durante il ripristino bare metal. In tal caso, per eseguire il ripristino durante il ripristino bare metal è necessario eseguire una delle attività seguenti e quindi eseguire il ripristino bare meta dal punto di ripristino copiato:
  - Eseguire il backup su un volume di un'altra unità.
  - Eseguire il backup su una condivisione remota.
  - Copiare un punto di ripristino su una destinazione diversa.

  Nota: Se si esegue il ripristino bare metal con dischi dinamici multipli, il ripristino potrà non riuscire a causa di alcuni errori imprevisti (come errori di avvio, volumi dinamici non riconosciuti e così via). Se ciò si verifica, sarà necessario eseguire il ripristino del disco mediante ripristino bare metal quindi, una volta riavviato il computer, sarà possibile ripristinare i volumi dinamici in un ambiente normale.
- In caso di ripristino bare metal su un computer virtuale Hyper-V con un disco da 4 KB, aggiungere questo disco al controller SCSI. Se viene aggiunto al controller IDE, il disco non verrà rilevato nel sistema Windows PE.
- (Facoltativo) Verificare le informazioni di riferimento del ripristino bare metal. Per ulteriori informazioni, consultare i seguenti argomenti:
  - Funzionamento del ripristino bare metal
  - Sistemi operativi che supportano la conversione UEFI/BIOS
  - Gestione del menu delle operazioni di ripristino bare metal

Verificare le seguenti considerazioni:

- Se si esegue l'aggiornamento a una versione o release più recente di Arcserve UDP, è necessario ricreare l'immagine ISO di ripristino bare metal secondo il livello di Windows AIK o ADK appropriato per includere il supporto delle funzionalità e delle correzioni di errori più recenti. Tuttavia, una volta creata un'immagine ISO di ripristino bare metal, è possibile utilizzare il file .ISO per lo stesso livello di sistema operativo. I seguenti livelli di sistema operativo possono utilizzare la stessa immagine ISO:
  - ISO creata mediante Windows 7 WAIK (valido per Windows 2003, Vista, 2008, 2008 R2)
  - ISO creato mediante Windows 8/8.1 ADK (valido per Windows 8, 8.1, Server 2012, Server 2012 R2)
  - ISO creata mediante Windows 10 ADK (valido per Windows 10)

Definizione delle opzioni di ripristino bare metal

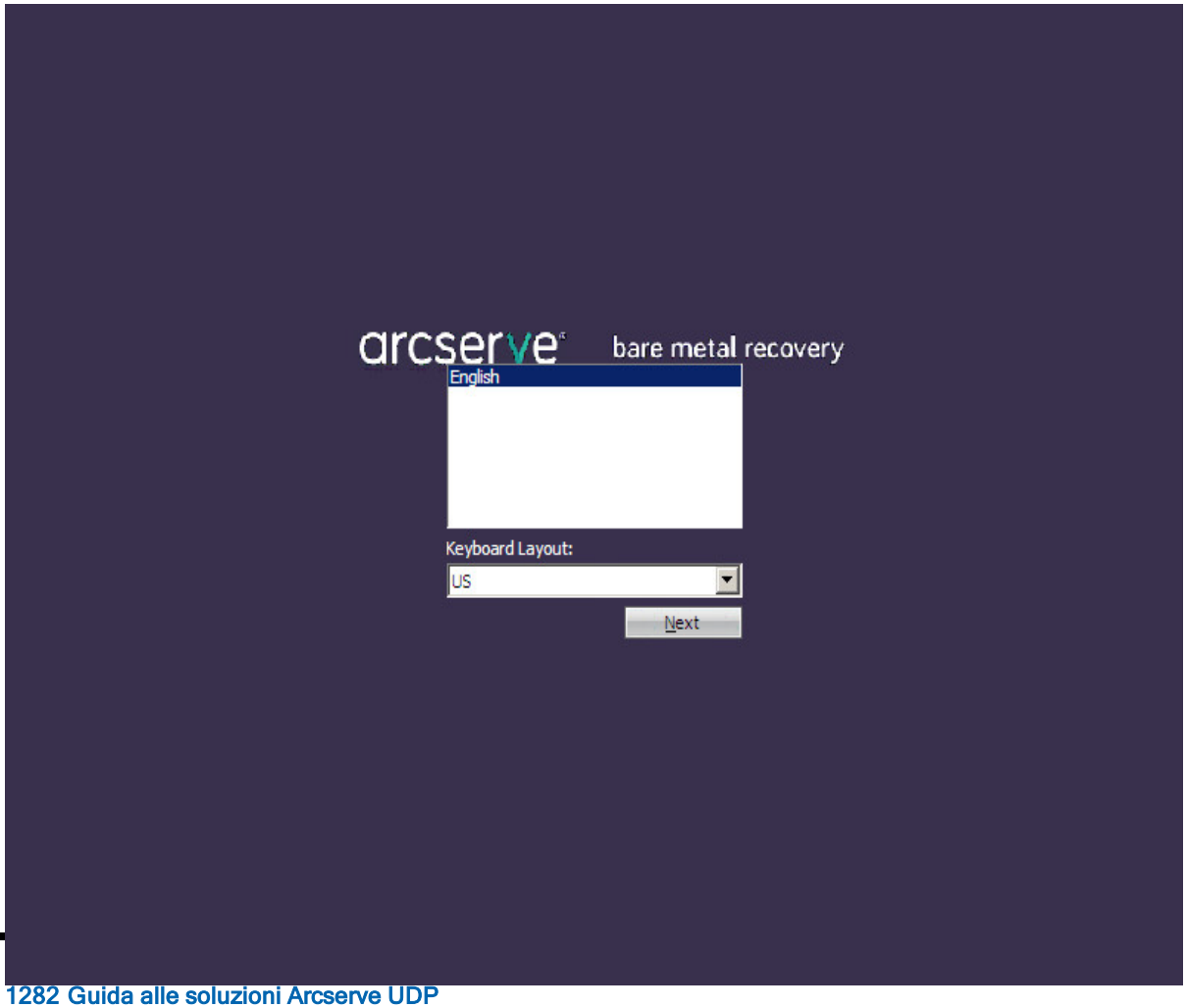
Prima di avviare il processo di ripristino bare metal, è necessario specificare alcune opzioni preliminari relative al ripristino.

Effettuare le operazioni seguenti:

1. Inserire il supporto contenente l'immagine del kit di avvio salvata e avviare il computer.
   - Se si utilizza un'immagine ISO di ripristino bare metal masterizzata su CD/DVD, inserire il CD/DVD salvato.
   - Se si utilizza un'immagine ISO di ripristino bare metal masterizzata su una periferica USB, inserire la periferica USB salvata.

   Verrà visualizzata la schermata dell'**utilità di installazione BIOS**.
2. In questa schermata, selezionare l'opzione dell'**utilità di installazione BIOS** o l'opzione USB per inizializzare il processo di avvio. Selezionare un'architettura (x86/-x64) e premere **Invio** per continuare.

   Viene visualizzata la schermata di selezione della lingua dell'agente Arcserve UDP (Windows).
3. Selezionare una lingua e fare clic su **Avanti** per continuare.



Il processo di ripristino bare metal viene avviato e viene visualizzata la schermata della procedura guidata di ripristino bare metal.



La schermata della procedura guidata del ripristino bare metal consente di selezionare il tipo di ripristino bare metal che si desidera eseguire:

- **Ripristino da un backup di Arcserve Unified Data Protection**

  Utilizzare questa opzione per eseguire il ripristino da una cartella di destinazione del backup o da un archivio dati.

  Questa opzione consente di ripristinare i dati di cui è stato eseguito il backup mediante l'agente Arcserve UDP (Windows). Questa opzione viene utilizzata nel caso di sessioni di backup eseguite con l'agente Arcserve UDP (Windows) oppure con l'applicazione Arcserve UDP Host-Based VM Backup.

  Per ulteriori informazioni, consultare la sezione Esecuzione di un ripristino bare metal tramite un backup nella Guida in linea.

- **Ripristino da un computer virtuale Virtual Standby**

  Utilizzare questa opzione per eseguire un ripristino virtual-to-physical (V2P) da un computer virtuale Virtual Standby o da un computer virtuale istantaneo. Virtual-to-physical (V2P) è un termine che fa riferimento alla migrazione di un sistema operativo, dei programmi applicativi e dei dati da un computer virtuale o una partizione del disco al disco rigido principale di un computer. La destinazione può essere uno o più computer.

- **L'origine è su un computer VMware**

  Consente di eseguire il recupero dei dati per un computer la cui conversione virtuale viene eseguita da un computer virtuale VMware. Questa opzione viene utilizzata per l'applicazione del computer virtuale istantaneo o Arcserve Central Virtual Standby.

  Nota: L'opzione consente di eseguire il recupero dei dati solo se la conversione virtuale in un file VMDK (per VMware) è stata eseguita mediante un computer virtuale istantaneo o Arcserve Central Virtual Standby.

  Se si seleziona questa opzione, consultare la sezione Recupero mediante computer virtuale Virtual Standby VMware o computer virtuale istantaneo per continuare la procedura.

- **L'origine è su un computer Hyper-V**

  Consente di eseguire il recupero dei dati per un computer la cui conversione virtuale viene eseguita da un computer virtuale Hyper-V. Questa opzione viene utilizzata per l'applicazione del computer virtuale istantaneo o Arcserve Central Virtual Standby.

  Nota: L'opzione consente di eseguire il recupero dei dati solo se la conversione virtuale in un file VHD (per Hyper-V) è stata eseguita mediante un computer virtuale istantaneo o Arcserve Central Virtual Standby.

  Se si seleziona questa opzione, consultare la sezione Recupero mediante computer virtuale Virtual Standby Hyper-V o computer virtuale istantaneo per continuare la procedura.

4. Selezionare **Eseguire il recupero da un computer virtuale Virtual Standby**. Selezionare quindi una delle origini.

   Se è stata selezionata l'opzione **L'origine è su un computer VMware**, consultare la sezione Recupero mediante computer virtuale Virtual Standby VMware o computer virtuale istantaneo per procedere.

   Se è stata selezionata l'opzione **L'origine è su un computer Hyper-V**, consultare la sezione Recupero mediante computer virtuale Virtual Standby Hyper-V o computer virtuale istantaneo per procedere.

Recupero mediante computer virtuale Virtual Standby Hyper-V o computer virtuale istantaneo

L'agente Arcserve UDP (Windows) consente di eseguire il ripristino bare metal dei computer virtual-to-physical (V2P). Questa funzionalità consente di eseguire il recupero V2P a partire dallo stato più recente di un computer virtuale di standby o istantaneo e ridurre, in tal modo, le perdite sul computer di produzione.

Effettuare le operazioni seguenti:

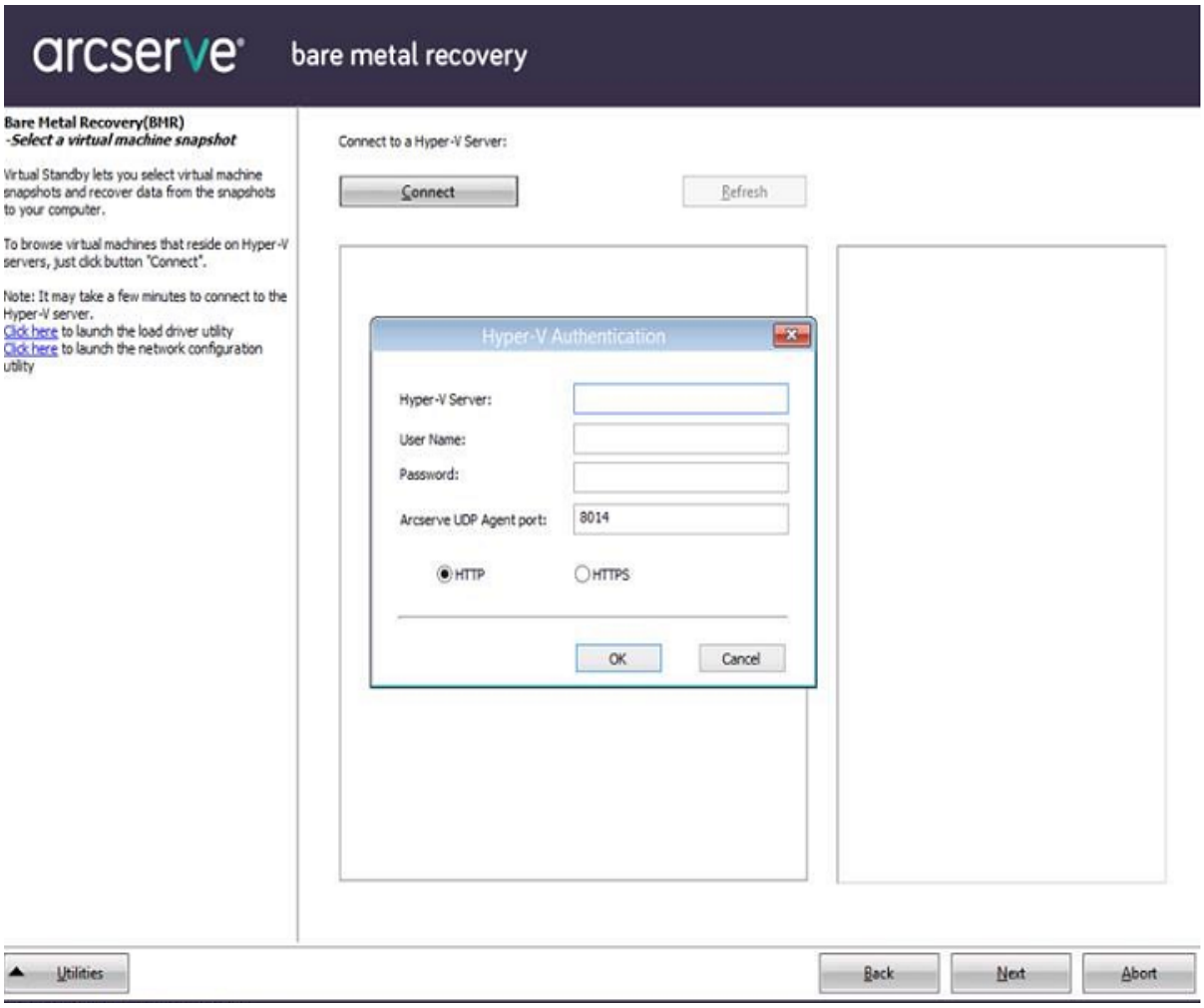
1. Dalla schermata della procedura guidata relativa al tipo di ripristino bare metal (BMR), selezionare l'opzione **Eseguire il recupero da un computer virtuale Virtual Standby** e l'opzione **L'origine è su un computer Hyper-V**.

   Utilizzare questa opzione per eseguire un ripristino virtual-to-physical da un computer virtuale Virtual Standby o da un computer virtuale istantaneo. Virtual-to-physical è un termine che fa riferimento alla migrazione di un sistema operativo, dei programmi applicativi e dei dati da un computer virtuale o una partizione del disco al disco rigido principale di un computer. La destinazione può essere uno o più computer.



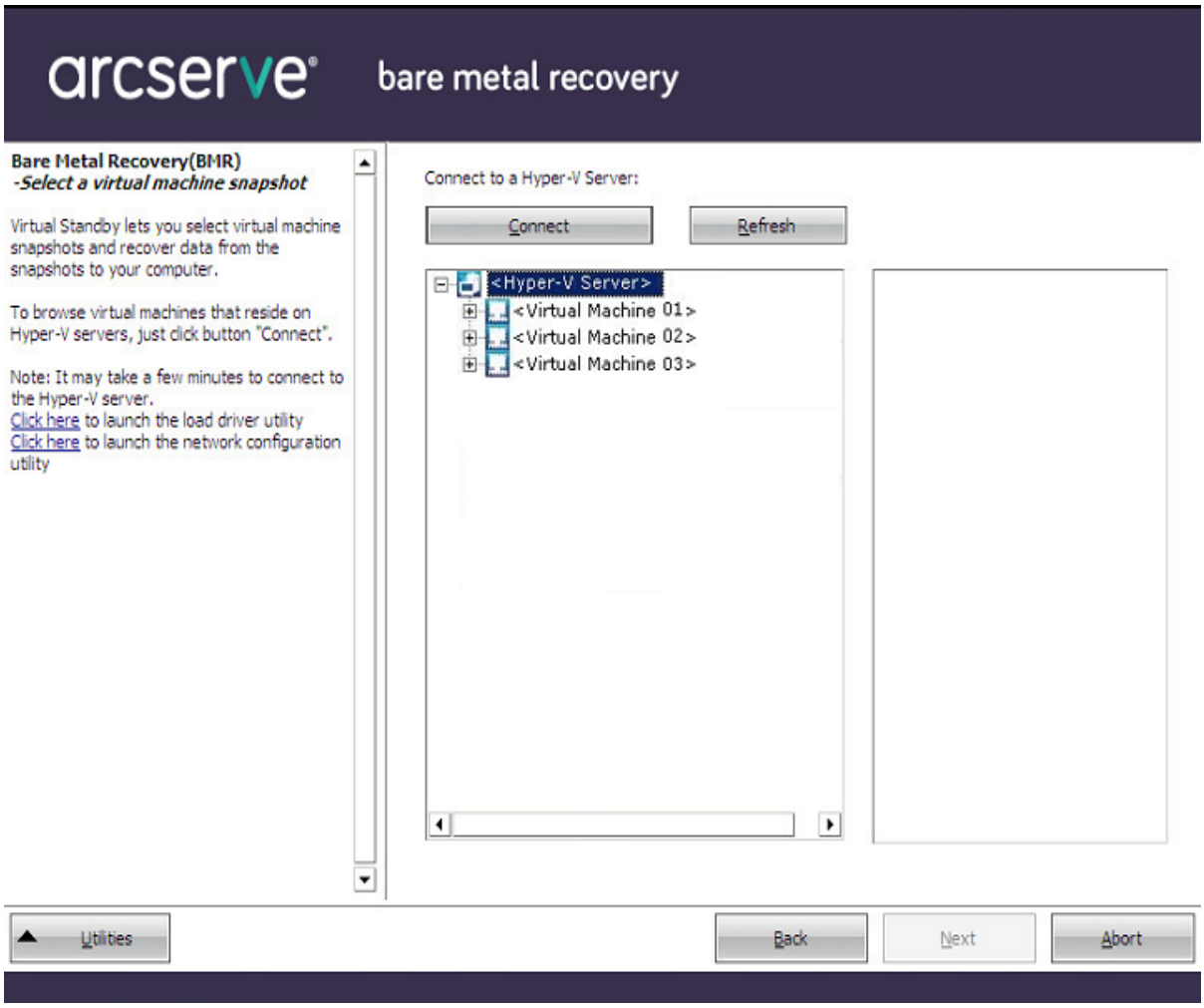
2. Fare clic su **Avanti**.

   Verrà visualizzata la schermata Selezionare una snapshot del computer virtuale con la finestra di dialogo Autenticazione Hyper-V in cui vengono richiesti i dettagli relativi al server Hyper-V.



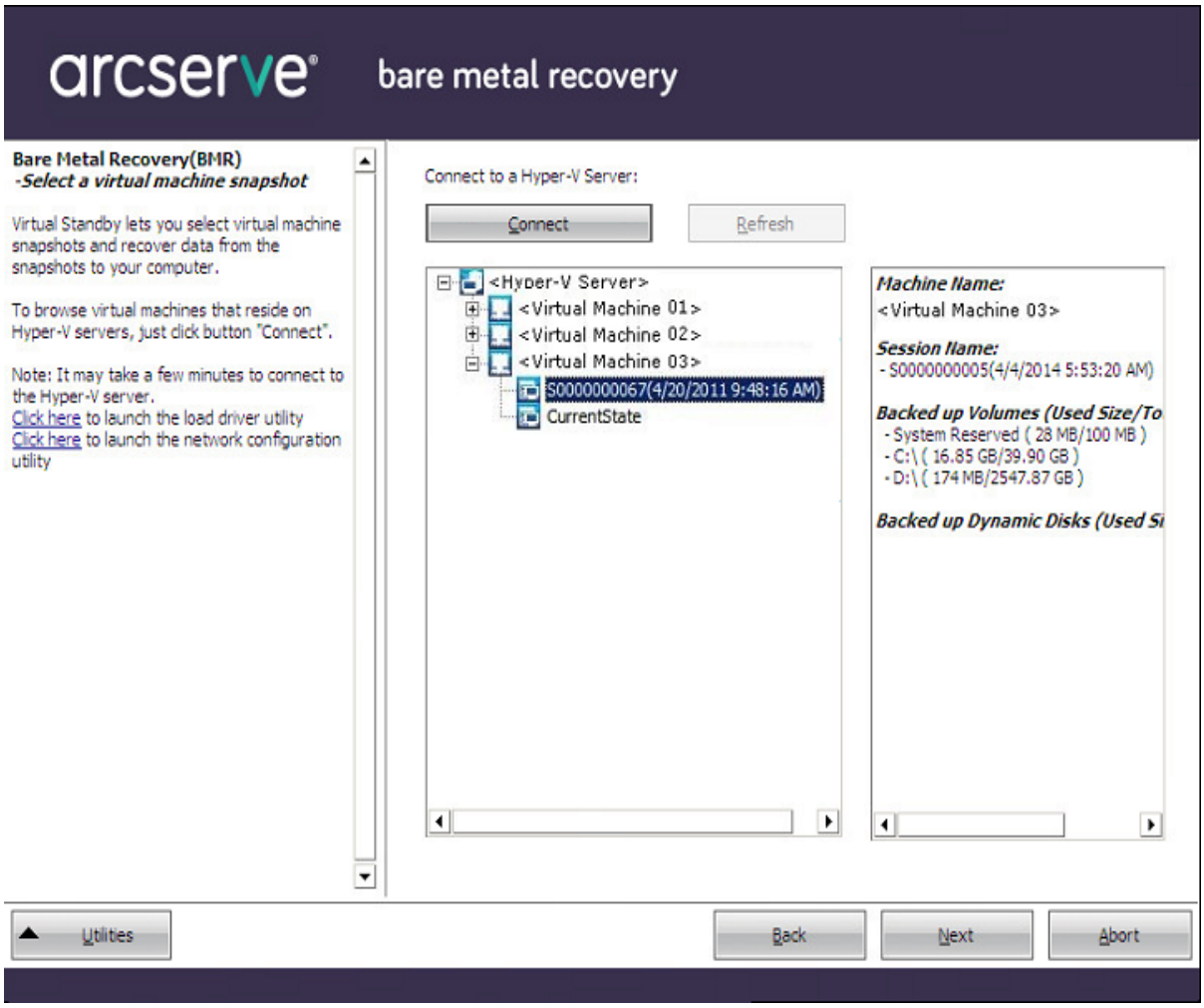
3. Immettere le informazioni di autenticazione e fare clic su **OK**.

   L'Agente Arcserve Unified Data Protection per Windows individua e visualizza il server Hyper-V con un elenco di tutti i computer virtuali che vengono convertiti sul server Hyper-V specificato mediante Arcserve Central Virtual Standby o il computer virtuale istantaneo.



4. Selezionare il computer virtuale contenente le snapshot del punto di ripristino per l'immagine di backup.

   Verranno visualizzate le sessioni di backup (snapshot del punto di ripristino) del computer virtuale selezionato.



5. Selezionare la sessione di backup del computer virtuale (snapshot del punto di ripristino) che si desidera recuperare.

   Le informazioni relative alla snapshot del punto di ripristino selezionato (nome del computer virtuale, nome della sessione di backup, volumi di backup) verranno visualizzati nel riquadro di destra.

   Dopo aver selezionato uno dei punti di ripristino presenti nell'elenco, è possibile selezionare il punto di ripristino corrispondente allo **Stato corrente** o allo **Stato più recente**.

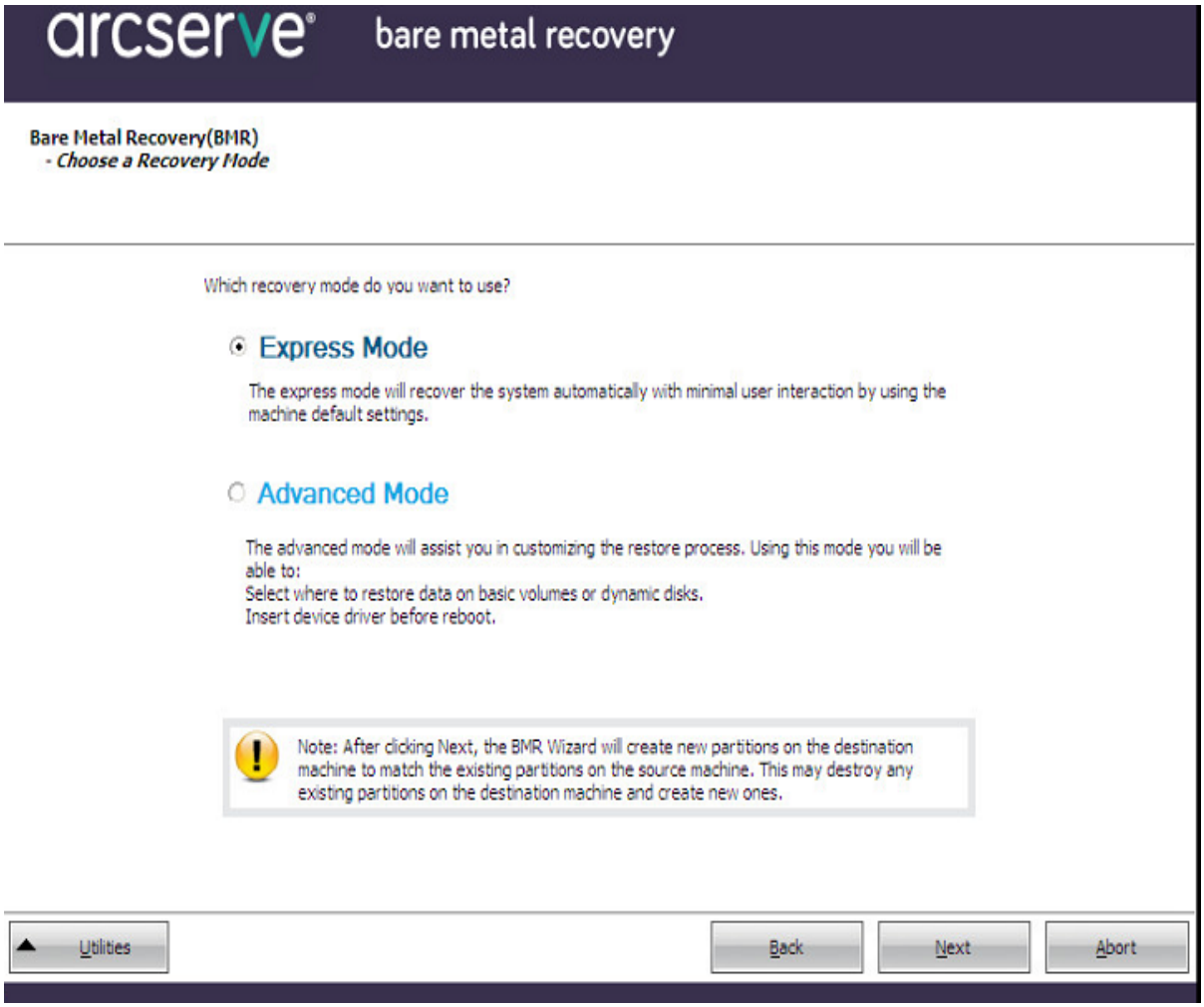
   - Se il computer virtuale utilizzato per il recupero viene acceso, verrà visualizzato lo **stato corrente** del punto di ripristino.

     Nota: Se il computer virtuale è attivato, qualsiasi modifica apportata ai dati nel computer virtuale dopo l'avvio del processo di ripristino bare metal non verrà recuperata.

   - Se il computer virtuale utilizzato per il recupero viene spento, verrà visualizzato lo **stato più recente** del punto di ripristino.

6. Verificare che il punto di ripristino selezionato sia corretto, quindi selezionare **Avanti**.

   Verrà visualizzata la scherma della procedura guidata di ripristino bare metal e le opzioni della modalità di recupero.



   Le opzioni disponibili sono **Modalità avanzata** e **Modalità rapida**.

   - Selezionare **Modalità rapida** se si desidera intervenire in modo limitato nel processo di recupero. Per ulteriori informazioni, consultare la sezione Esecuzione del ripristino bare metal in modalità rapida.
   - Selezionare **Modalità avanzata** per personalizzare il processo di recupero. Per ulteriori informazioni, consultare la sezione Esecuzione del ripristino bare metal in modalità avanzata.

   Impostazione predefinita: Modalità rapida.

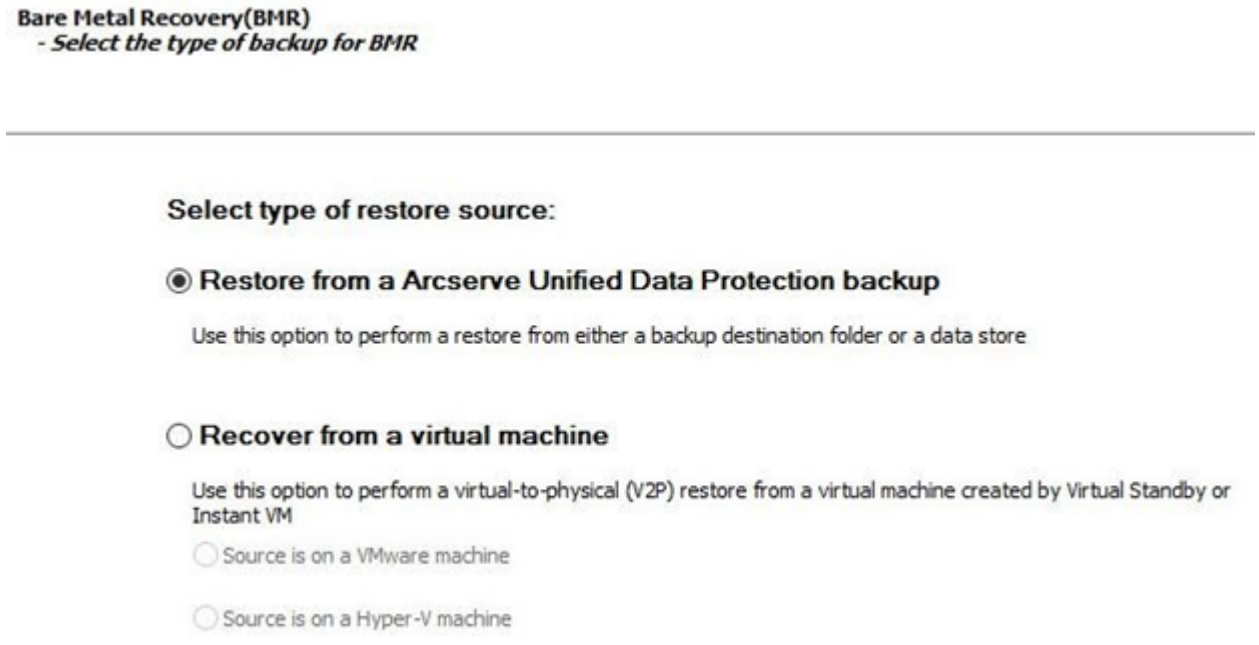
Recupero mediante computer virtuale Virtual Standby VMware o computer virtuale istantaneo

L'agente Arcserve UDP (Windows) consente di eseguire il ripristino bare metal dei computer virtual-to-physical (V2P). Questa funzionalità consente di eseguire il recupero V2P a partire dallo stato più recente di un computer virtuale di standby e ridurre, in tal modo, le perdite sul computer di produzione.

Effettuare le operazioni seguenti:

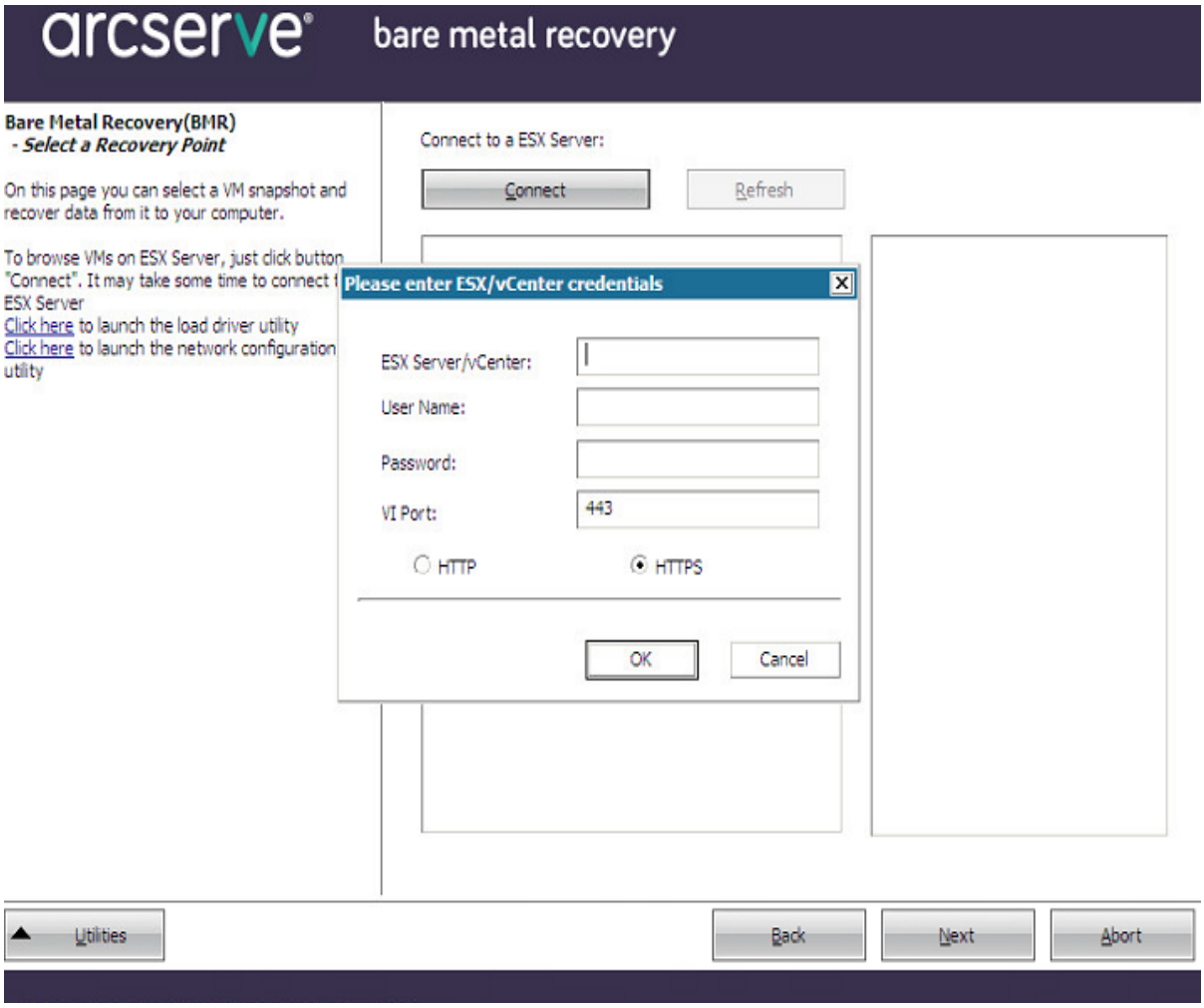
1. Dalla schermata della selezione guidata del tipo di ripristino bare metal (BMR), selezionare l'opzione **Recupera da computer virtuale** e l'opzione **L'origine è su un computer VMware**.

   Utilizzare questa opzione per eseguire un ripristino virtual-to-physical da un computer virtuale Virtual Standby o da un computer virtuale istantaneo. Virtual-to-physical è un termine che fa riferimento alla migrazione di un sistema operativo, dei programmi applicativi e dei dati da un computer virtuale o una partizione del disco al disco rigido principale di un computer. La destinazione può essere uno o più computer.



2. Fare clic su **Avanti**.

   Verrà visualizzata la schermata **Selezionare un punto di ripristino** con la finestra di dialogo delle **credenziali di ESX/VC**.



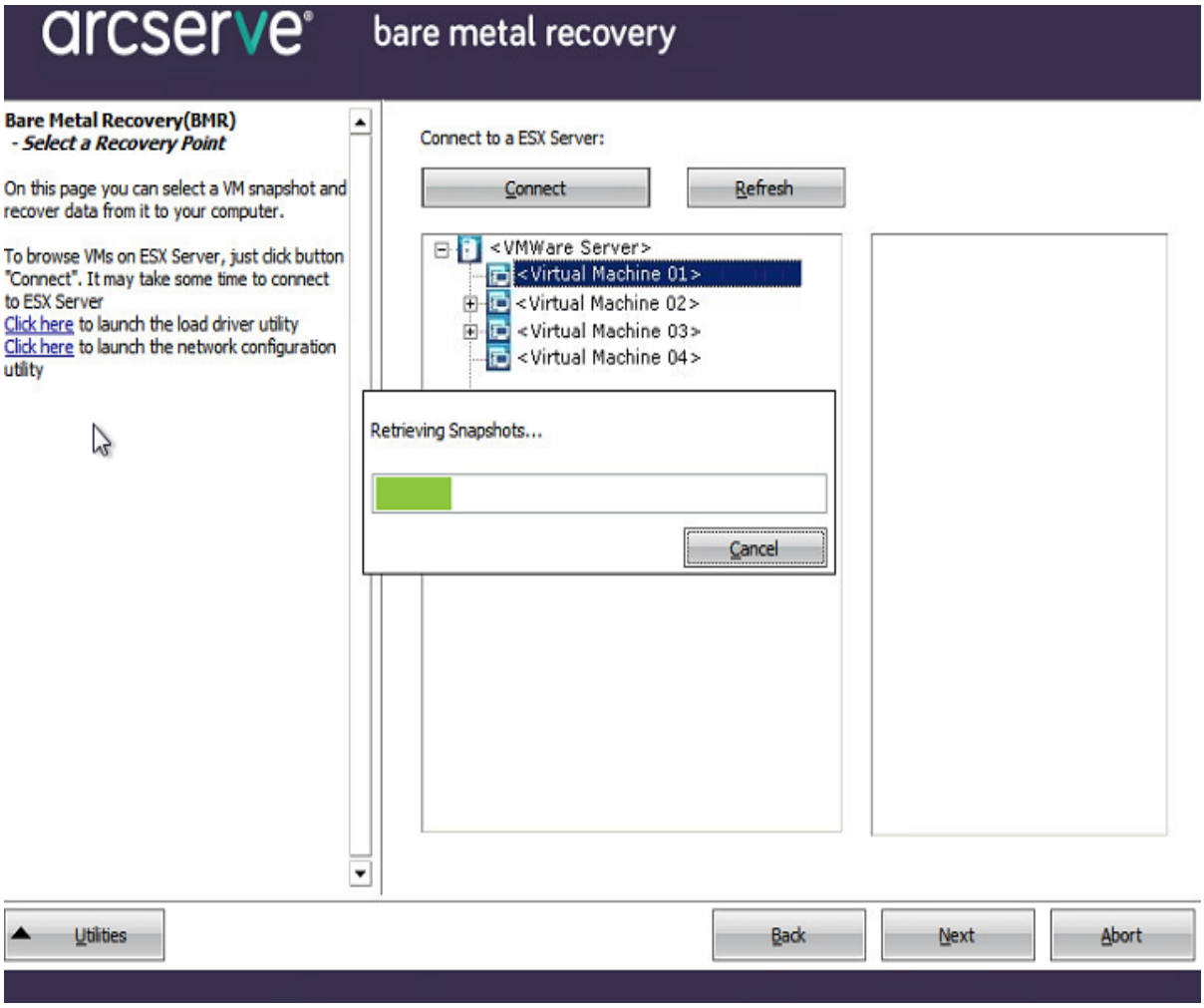
3. Immettere le informazioni per l'accesso e fare clic su **OK**.

   Nota: per gli utenti di vCenter non è necessario disporre dell'autorizzazione di amministratore a livello del server vCenter ma è sufficiente disporre di un'autorizzazione di amministratore a livello di datacenter. Inoltre, è necessario disporre delle autorizzazioni seguenti a livello di server vCenter:

   - Global, DisableMethods and EnableMethods
   - Global, License

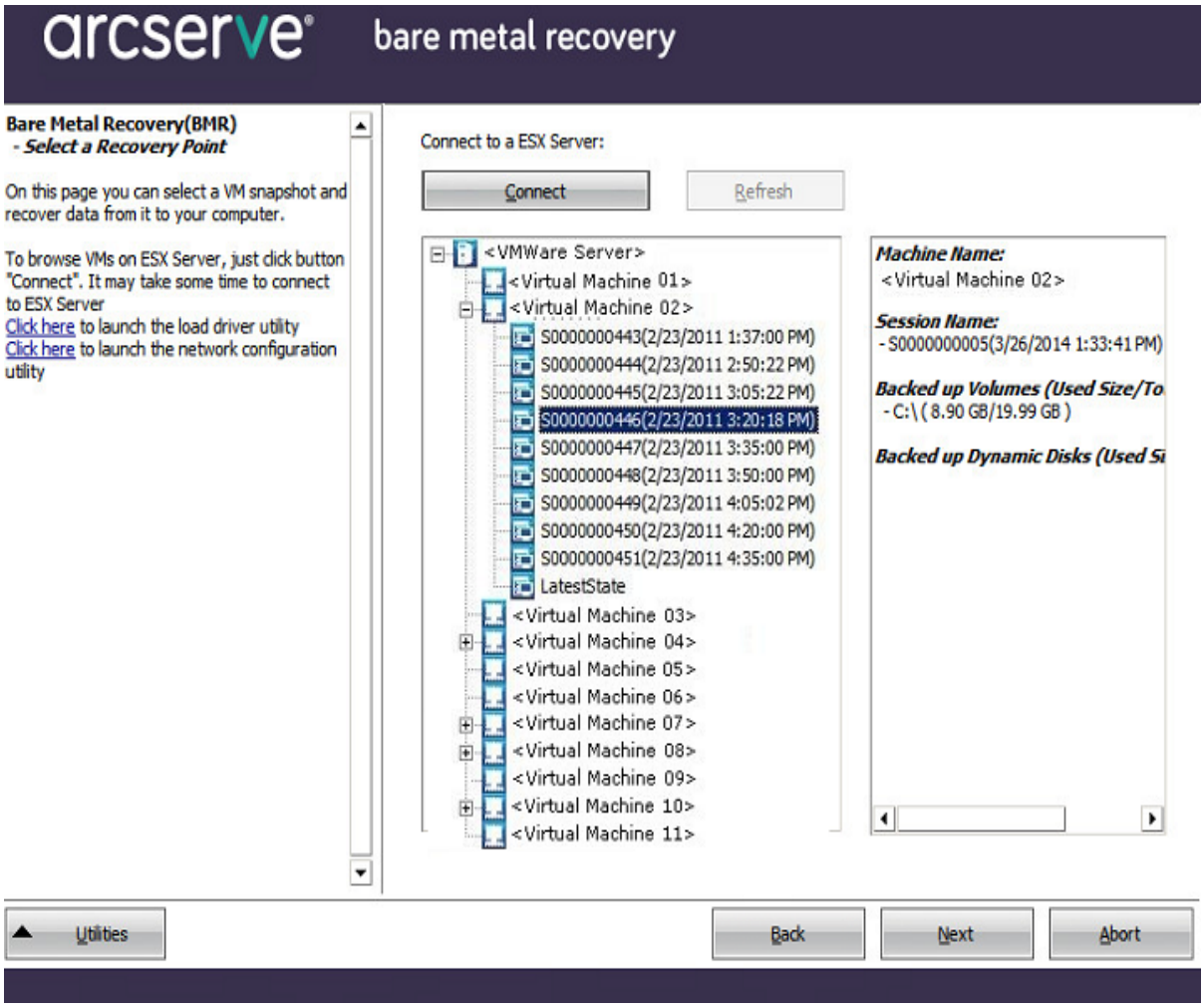
   Verrà visualizzata la schermata **Selezionare un punto di ripristino**.

   L'Agente Arcserve Unified Data Protection per Windows recupera tutte le snapshot del punto di ripristino per il server VMware selezionato e visualizza nel riquadro sinistro il server con un elenco di tutti i computer virtuali che risiedono sul server VMware selezionato.



4. Selezionare il computer virtuale contenente i punti di ripristino per l'immagine di backup.

   Verranno visualizzate le sessioni di backup (snapshot del punto di ripristino) del computer virtuale selezionato.



5. Selezionare la sessione di backup del computer virtuale (snapshot del punto di ripristino) che si desidera recuperare.

   Le informazioni relative alla snapshot del punto di ripristino selezionato (nome del computer virtuale, nome della sessione di backup, volumi di backup, dischi dinamici di backup) verranno visualizzate nel riquadro di destra.

   Dopo aver selezionato uno dei punti di ripristino presenti nell'elenco, è possibile selezionare il punto di ripristino corrispondente allo **Stato corrente** o allo **Stato più recente**.

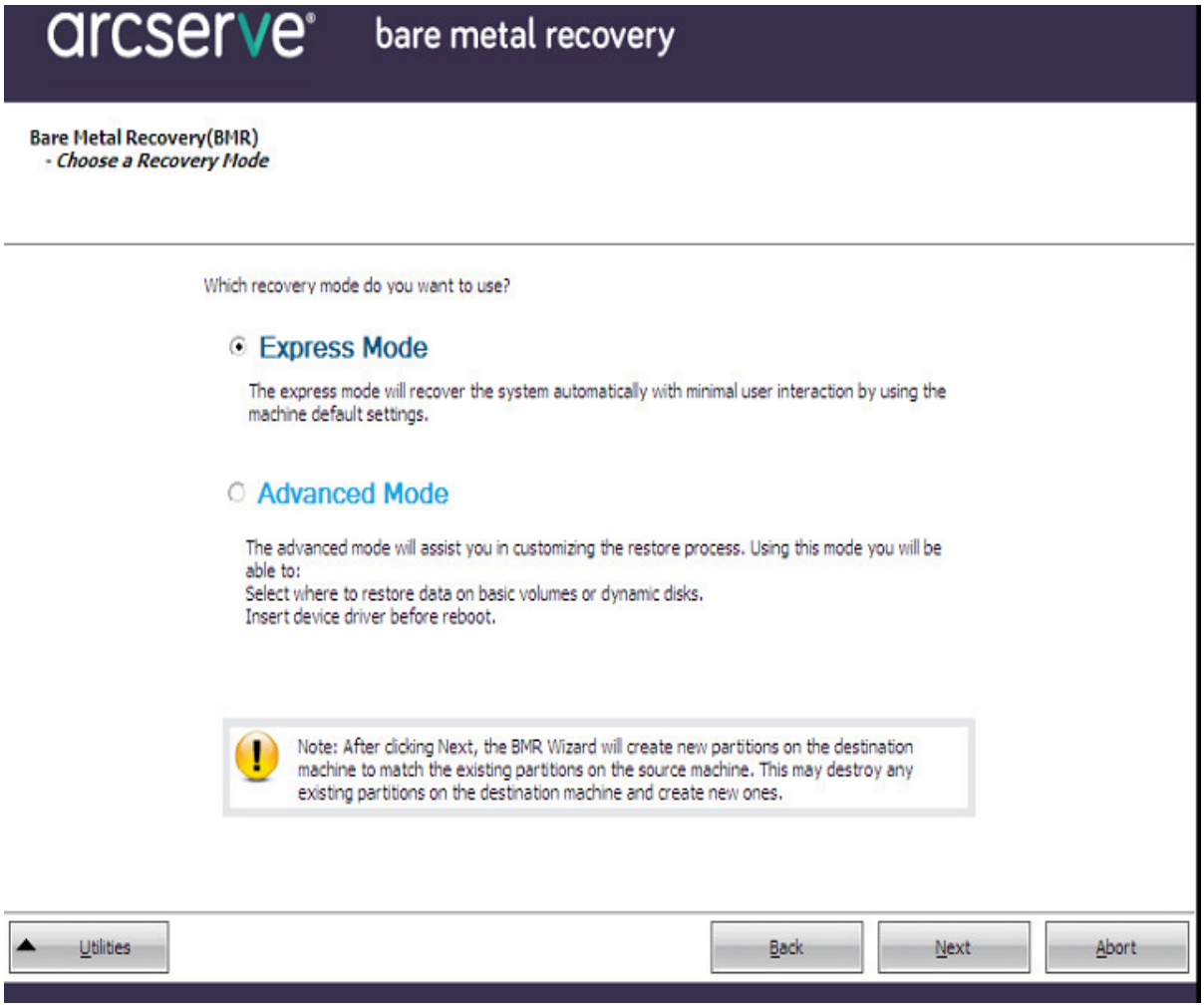
   - Se il computer virtuale utilizzato per il recupero viene acceso, verrà visualizzato lo **stato corrente** del punto di ripristino.

     Nota: Se il computer virtuale è attivato, qualsiasi modifica apportata ai dati nel computer virtuale dopo l'avvio del processo di ripristino bare metal non verrà recuperata.

   - Se il computer virtuale utilizzato per il recupero viene spento, verrà visualizzato lo **stato più recente** del punto di ripristino.

6. Verificare che il punto di ripristino selezionato sia corretto, quindi selezionare **Avanti**.

   Verrà visualizzata la scherma della procedura guidata di ripristino bare metal e le opzioni della modalità di recupero.



   Le opzioni disponibili sono **Modalità avanzata** e **Modalità rapida**.

   - Selezionare **Modalità rapida** se si desidera intervenire in modo limitato nel processo di recupero. Per ulteriori informazioni, consultare la sezione Esecuzione del ripristino bare metal in modalità rapida.
   - Selezionare **Modalità avanzata** per personalizzare il processo di recupero. Per ulteriori informazioni, consultare la sezione Esecuzione del ripristino bare metal in modalità avanzata.

   Impostazione predefinita: Modalità rapida.

Esecuzione del ripristino bare metal in modalità rapida

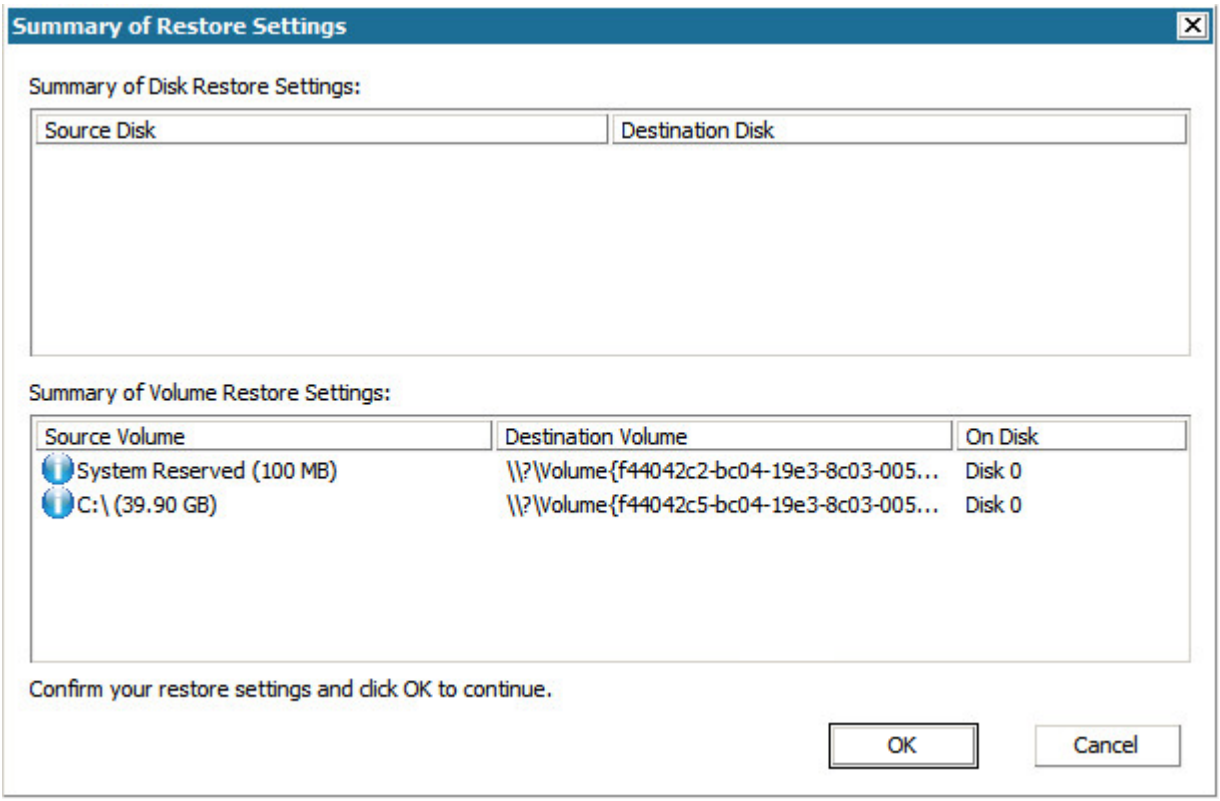
La **Modalità rapida** richiede un'interazione minima durante il processo di recupero.

Effettuare le operazioni seguenti:

1. Dalla finestra di dialogo **Selezionare una modalità di recupero**, selezionare **Modalità rapida** e fare clic su **Avanti**.

   Verrà visualizzata la schermata **Riepilogo delle impostazioni di ripristino del disco** contenente un riepilogo dei volumi da ripristinare.

   Nota: nella parte superiore della finestra Riepilogo ripristino, le lettere corrispondenti alle unità elencate nella colonna **Volume di destinazione** vengono generate automaticamente dall'Ambiente di preinstallazione di Windows (WinPE). È possibile che tali lettere di unità non corrispondano alle lettere elencate nella colonna **Volume di origine**. Tuttavia, il ripristino dei dati verrà eseguito sul volume appropriato anche se le lettere di unità sono diverse.



2. Verificare che le informazioni di riepilogo siano corrette, quindi fare clic su **OK**.

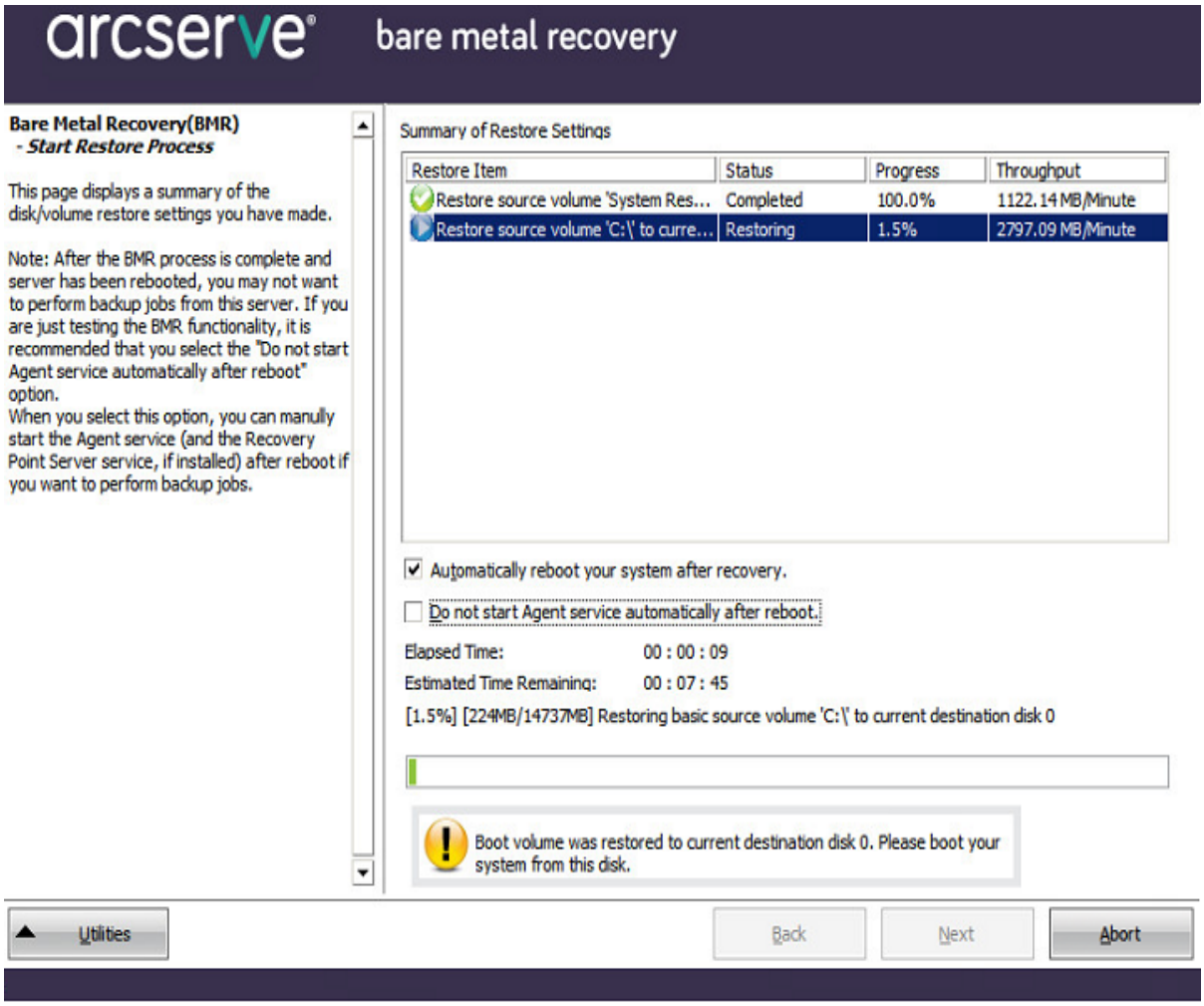
   Verrà avviato il processo di ripristino. La schermata della procedura guidata di ripristino bare metal visualizza lo stato di ripristino per ciascun volume.

- Il tempo necessario per l'esecuzione di questa operazione dipende dalle dimensioni del volume da ripristinare.
- Durante questo processo viene eseguito il ripristino blocco per blocco di tutti i dati di backup di tale punto di ripristino e viene creata una replica del computer di origine sul computer di destinazione.
- L'opzione di riavvio automatico del sistema in seguito al recupero è selezionata per impostazione predefinita. Se lo si desidera, è possibile deselezionare questa opzione ed eseguire il riavvio manuale in un secondo momento.

  Importante: se è in corso il recupero autorevole di Active Directory dopo un ripristino bare metal, è necessario deselezionare l'opzione di **riavvio automatico del sistema in seguito al ripristino**. Per ulteriori informazioni, consultare la sezione Ripristino autorevole di Active Directory dopo un ripristino bare metal.

  - Se necessario, è possibile selezionare di non avviare automaticamente il servizio Agente dopo il riavvio.
  - Se necessario, è possibile annullare o interrompere l'operazione in

qualsiasi momento.



3. Dal menu **Utilità**, è possibile accedere al **registro attività** del ripristino bare metal e utilizzare l'opzione **Salva** per salvare il registro attività.

   Per impostazione predefinita, il salvataggio del registro attività viene effettuato nella posizione seguente:

   X:\windows\system32\dr\log.

   Nota: per evitare la generazione di un errore Windows, si consiglia di non utilizzare l'opzione **Salva con nome** della finestra di dialogo del registro attività del ripristino bare metal per salvare il registro attività sul desktop o per creare una nuova cartella sul desktop.

4. Se si sta eseguendo il ripristino su hardware diversi (la scheda SCSI/FC utilizzata per la connessione ai dischi rigidi potrebbe essere stata modificata) e non viene rilevato nessun driver compatibile nel sistema originale, viene visualizzata la pagina di inserimento del driver per consentire all'utente di specificare i driver necessari per le periferiche.

È possibile individuare e selezionare i driver da inserire nel sistema ripristinato. In tal modo è possibile eseguire il ripristino su un computer con hardware diversi.

5. Una volta completato il processo di ripristino bare metal, viene visualizzata una notifica di conferma.

Esecuzione del ripristino bare metal in modalità avanzata

La **Modalità avanzata** consente di personalizzare il processo di recupero.

Effettuare le operazioni seguenti:

1. Dalla finestra di dialogo **Selezionare una modalità di recupero**, selezionare **Modalità avanzata** e fare clic su **Avanti**.

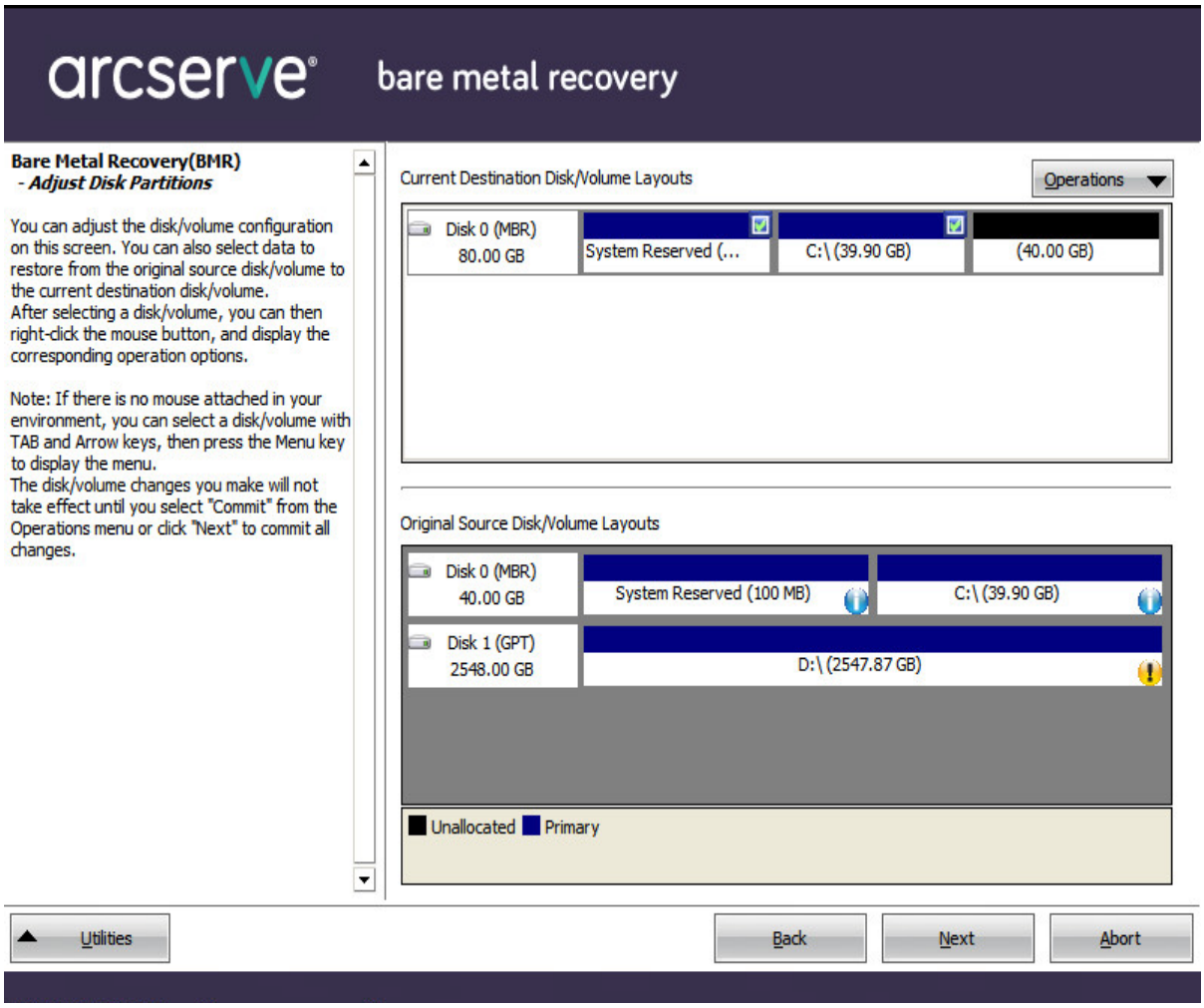
   L'utilità di ripristino bare metal esegue la ricerca del computer da recuperare e visualizza le informazioni relative alla partizione del disco corrispondente.

   Il riquadro superiore mostra la configurazione del disco presente sul computer corrente (destinazione), mentre il riquadro inferiore mostra le informazioni relative alla partizione del disco del computer originale (origine).

   Importante! Se nel riquadro inferiore il volume di origine viene contrassegnato da una X rossa, significa che tale volume contiene informazioni di sistema e che non è stato assegnato (mappato) al volume di destinazione. Il volume contenente le informazioni di sistema dovrà essere assegnato dal disco di origine al disco di destinazione e ripristinato durante il processo di ripristino bare metal. In caso contrario, non sarà possibile eseguire il riavvio.

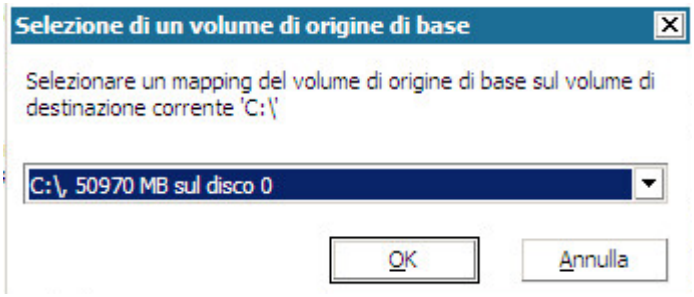
   Nota: se si esegue il ripristino bare metal del volume di sistema su un disco non configurato come disco di avvio, non sarà possibile avviare il computer in seguito al completamento del ripristino bare metal. Assicurarsi di eseguire il ripristino del volume di sistema su un disco di avvio configurato correttamente.

   Nota: se si esegue il ripristino su un altro disco/volume, la capacità del nuovo disco/volume deve essere uguale o superiore a quella del disco/volume originale. Inoltre, il ridimensionamento del disco è disponibile solo per i dischi di base e non per i dischi dinamici.



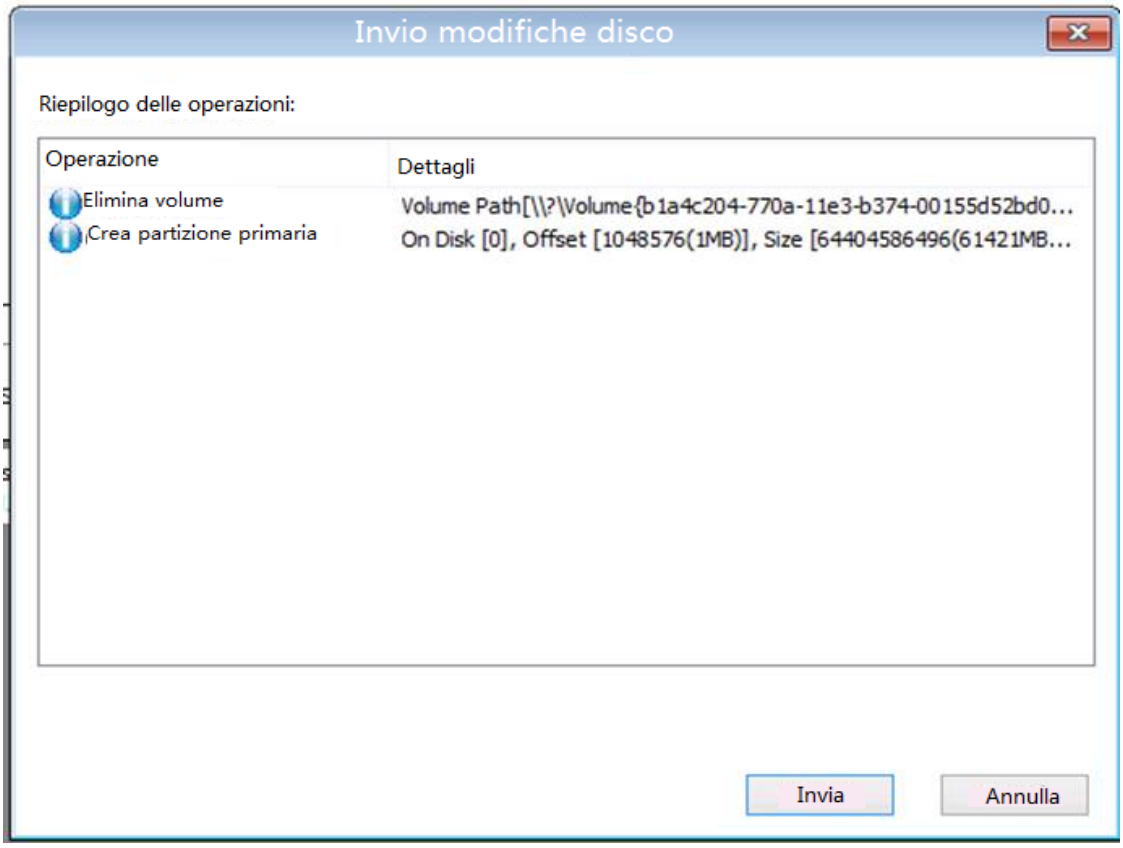
2. Se le informazioni del disco non vengono visualizzate correttamente, accedere al menu **Utilità** e verificare se sono richiesti driver mancanti.
3. Se necessario, nel riquadro del disco/volume di destinazione, è possibile fare clic sul menu a discesa **Operazioni** e visualizzare le opzioni disponibili. Per ulteriori informazioni sulle opzioni, consultare la sezione Gestione del menu delle operazioni di ripristino bare metal.
4. Per assegnare un volume di origine al volume di destinazione, fare clic su ciascun volume di destinazione e, dal menu di scelta rapida, selezionare l'opzione **Esegui mapping del volume da**.

   Verrà visualizzata la finestra di dialogo **Selezione di un volume di origine di base**.



5. Nella finestra di dialogo **Selezione di un volume di origine di base**, fare clic sul menu a discesa e selezionare il volume di origine disponibile da assegnare al volume di destinazione specificato. Fare clic su **OK**.
   - Il volume di destinazione viene contrassegnato da un'icona con il segno di spunta, a indicare che il mapping del volume di destinazione è stato eseguito.
   - Nel volume di origine, l'icona con forma di X rossa viene sostituita da un'icona verde, a indicare che il volume di origine è stato assegnato a un volume di destinazione.
6. Verificare che tutti i volumi da ripristinare e che i volumi contenenti informazioni di sistema siano assegnati a un volume di destinazione, quindi fare clic su **Avanti**.

   Verrà visualizzata la schermata Invia modifiche disco contenente un riepilogo delle operazioni selezionate. Per ciascun nuovo volume creato, vengono visualizzate le informazioni corrispondenti.



7. Verificare che le informazioni di riepilogo siano corrette, quindi fare clic su **Invia**. Se le informazioni non sono corrette, fare clic su **Annulla**.

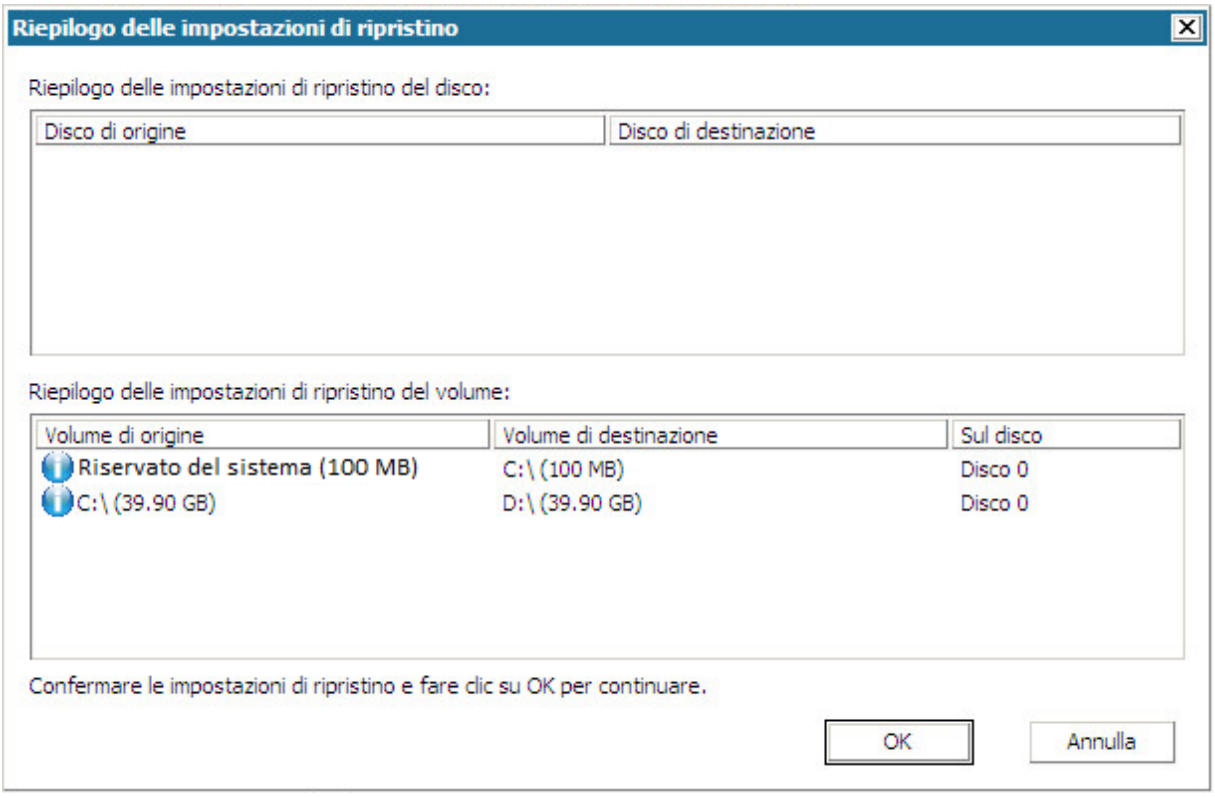
   Nota: tutte le operazioni eseguite sul disco rigido verranno implementate solo in seguito all'invio.

   I nuovi volumi vengono creati sul computer di destinazione e mappati sul computer di origine corrispondente.

8. Una volta completate le modifiche, fare clic su **OK**.

   Verrà visualizzata la schermata Riepilogo delle impostazioni di ripristino del disco contenente un riepilogo dei volumi da ripristinare.

   Nota: Nella parte superiore della pagina Riepilogo ripristino, le lettere corrispondenti alle unità elencate nella colonna Volume di destinazione vengono generate automaticamente dall'Ambiente di preinstallazione di Windows (WinPE). È possibile che tali lettere di unità non corrispondano alle lettere elencate nella colonna Volume di origine. Tuttavia, il ripristino dei dati verrà eseguito sul volume appropriato anche se le lettere di unità sono diverse.

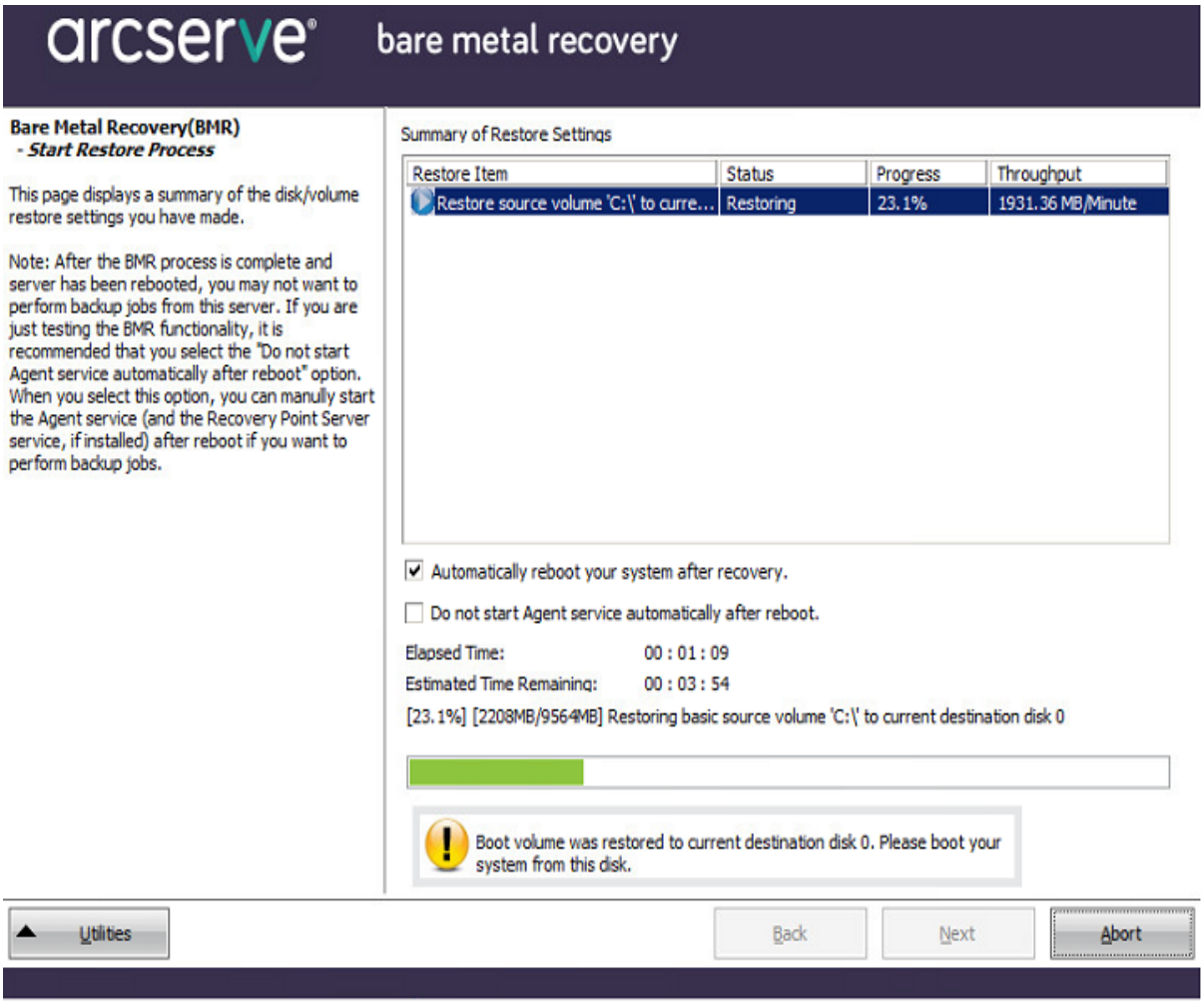


9. Verificare che le informazioni di riepilogo siano corrette, quindi fare clic su **OK**.

   Verrà avviato il processo di ripristino. La schermata della procedura guidata di ripristino bare metal visualizza lo stato di ripristino per ciascun volume.

- Il tempo necessario per l'esecuzione di questa operazione dipende dalle dimensioni del volume da ripristinare.
- Durante questo processo viene eseguito il ripristino blocco per blocco di tutti i dati di backup di tale punto di ripristino e viene creata una replica del computer di origine sul computer di destinazione.
- L'opzione di riavvio automatico del sistema in seguito al recupero è selezionata per impostazione predefinita. Se lo si desidera, è possibile deselezionare questa opzione ed eseguire il riavvio manuale in un secondo momento.

  Importante: Se è in corso il recupero autorevole di Active Directory dopo un ripristino bare metal, è necessario deselezionare l'opzione **Riavviare automaticamente il sistema dopo il recupero**. Per ulteriori informazioni, consultare la sezione Ripristino autorevole di Active Directory dopo un ripristino bare metal.
- Se necessario, è possibile selezionare di non avviare automaticamente il servizio Agente dopo il riavvio.
- Se necessario, è possibile annullare o interrompere l'operazione in qualsiasi momento.



10. Dal menu **Utilità**, è possibile accedere al **registro attività** del ripristino bare metal e utilizzare l'opzione **Salva** per salvare il registro attività.

    Per impostazione predefinita, il salvataggio del registro attività viene effettuato nella posizione seguente:

    X:\windows\system32\dr\log

    Nota: per evitare la generazione di un errore Windows, si consiglia di non utilizzare l'opzione **Salva con nome** della finestra di dialogo del registro attività del ripristino bare metal per salvare il registro attività sul desktop o per creare una nuova cartella sul desktop.

11. Se si sta eseguendo il ripristino su hardware diversi (la scheda SCSI/FC utilizzata per la connessione ai dischi rigidi potrebbe essere stata modificata) e non viene rilevato nessun driver compatibile nel sistema originale, viene visualizzata la pagina di inserimento del driver per consentire all'utente di specificare i driver necessari per le periferiche.

È possibile individuare e selezionare i driver da inserire nel sistema ripristinato. In tal modo è possibile eseguire il ripristino su un computer con hardware diversi.

12. Una volta completato il processo di ripristino bare metal, viene visualizzata una notifica di conferma.

Verifica della corretta esecuzione del ripristino bare metal

Per verificare che il ripristino bare metal sia avvenuto correttamente, eseguire le attività seguenti:

- Riavviare il sistema operativo.
- Verificare che tutti i sistemi e tutte le applicazioni funzionino correttamente.
- Verificare che tutte le impostazioni di rete siano state configurate correttamente.
- Verificare che il BIOS sia configurato per l'avvio dal disco utilizzato per il ripristino del volume di avvio.
- Quando il ripristino bare metal viene completato, occorre considerare le condizioni seguenti:
  - Il primo backup eseguito dopo il ripristino bare metal è un backup di verifica.
  - Dopo aver riavviato il computer, potrebbe essere necessario configurare manualmente le schede di rete, nel caso in cui sia stato eseguito il ripristino su hardware differenti.

    Nota: Durante il riavvio di un computer, potrebbe essere visualizzata la schermata Ripristino da errori di Windows indicante che l'arresto di Windows non è avvenuto correttamente. Se ciò si verifica, è possibile ignorare l'avviso e avviare Windows normalmente.
  - In caso di dischi dinamici, se il disco è in modalità Non in linea, è possibile modificare manualmente lo stato a In linea, accedendo all'interfaccia di gestione del disco mediante l'utilità di controllo Diskmgmt.msc.
  - In caso di dischi dinamici, se lo stato del volume è Ridondanza non riuscita, è possibile eseguire la sincronizzazione manuale dei volumi, accedendo all'interfaccia di gestione del disco mediante l'utilità di controllo Diskmgmt.msc.

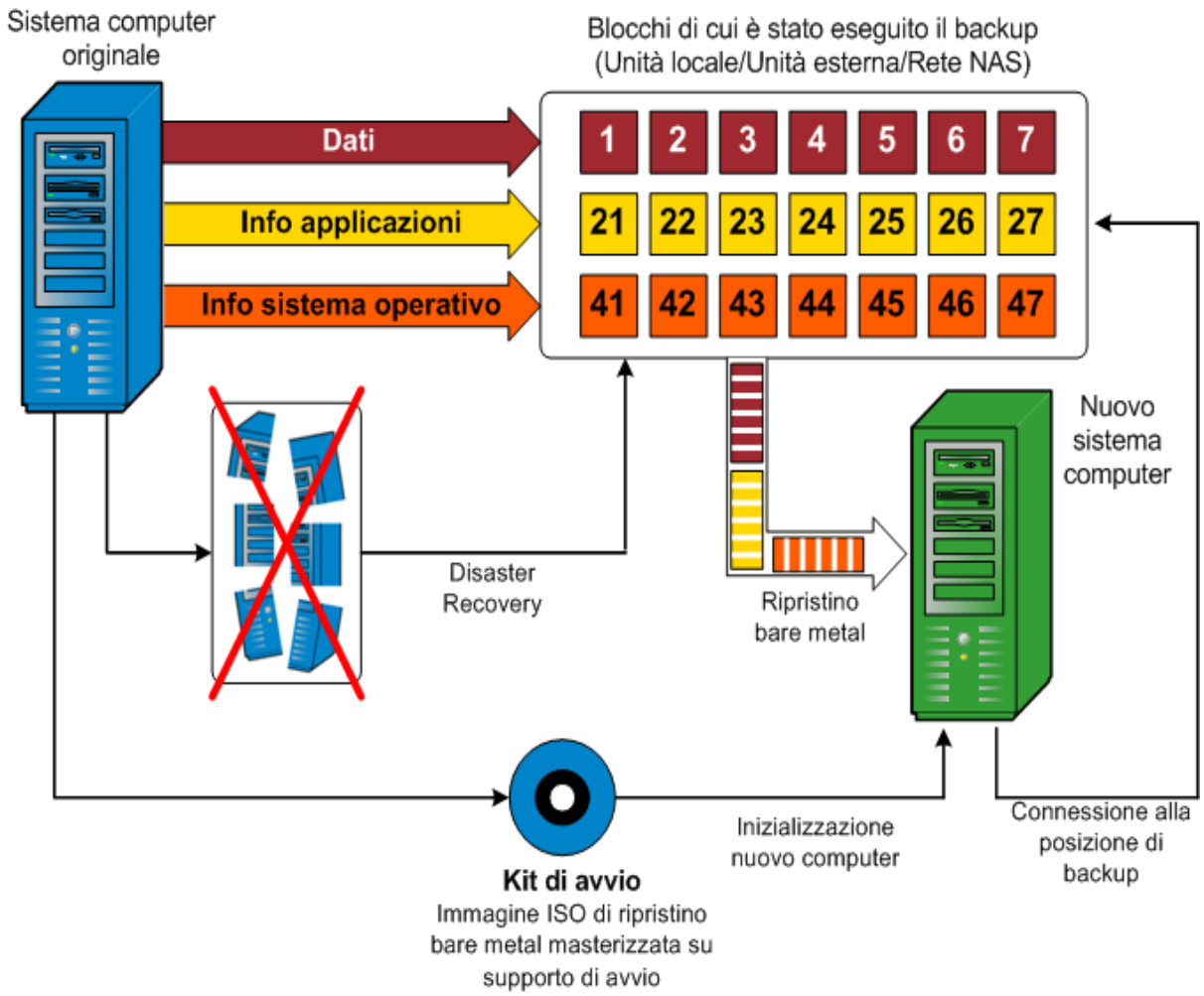
Informazioni di riferimento del ripristino bare metal

- Funzionamento del ripristino bare metal
- Sistemi operativi che supportano la conversione UEFI/BIOS
- Gestione del menu delle operazioni di ripristino bare metal

Funzionamento del ripristino bare metal

Il ripristino bare metal è il processo di ripristino di interi sistemi mediante la reinstallazione del sistema operativo, delle applicazioni software e mediante il ripristino di dati e impostazioni. Il ripristino bare metal di solito viene eseguito perché si verifica un errore nel disco rigido o perché il disco rigido è pieno e si desidera eseguire un aggiornamento (migrazione) a un'unità di dimensioni maggiori o una migrazione a un hardware più recente. È possibile eseguire un ripristino bare metal poiché durante il processo di backup a livello di blocco, l'agente Arcserve UDP (Windows) acquisisce non solo i dati, ma anche le informazioni relative al sistema operativo, alle applicazioni installate, alle impostazioni di configurazione, ai driver necessari e così via. Le informazioni necessarie per l'esecuzione di una ricostruzione completa di interi sistemi da bare metal vengono sottoposte a backup in una serie di blocchi ed archiviate nella posizione di backup.

Nota: il ripristino dei dischi dinamici viene eseguito solo a livello del disco. Se è stato eseguito il backup di dati in un volume o in un disco dinamico, non sarà possibile eseguire il ripristino di tale disco (compresi i volumi corrispondenti) durante il ripristino bare metal.



Quando si esegue un ripristino bare metal, il disco di avvio dell'agente Arcserve UDP (Windows) viene utilizzato per inizializzare il nuovo sistema e consentire l'avvio del processo di ripristino bare metal. Una volta avviato il ripristino bare metal, l'agente Arcserve UDP (Windows) richiederà di selezionare o specificare una posizione valida per il recupero dei blocchi sottoposti a backup, nonché del punto di ripristino da ripristinare. Il nuovo sistema potrebbe inoltre richiedere l'immissione di driver validi. Quando vengono fornite le informazioni di connessione e configurazione, l'agente Arcserve UDP (Windows) avvia l'estrazione dell'immagine di backup specificata dalla posizione di backup e ripristina tutti i blocchi sottoposti a backup sul nuovo sistema (i blocchi vuoti non verranno ripristinati). Una volta eseguito il ripristino completo dell'immagine bare metal sul nuovo sistema, lo stato del computer verrà ripristinato a quello dell'ultima esecuzione del backup e i backup dell'agente Arcserve UDP (Windows) potranno procedere in base alla pianificazione. (una volta completato il ripristino bare metal, il primo backup corrisponderà a Backup di verifica).

Sistemi operativi che supportano la conversione UEFI/BIOS

Se il sistema operativo del computer di origine non corrisponde al firmware del sistema, verrà richiesto se si desidera convertire il sistema UEFI in un sistema compatibile con BIOS o viceversa. La seguente tabella classifica ciascun sistema operativo e il tipo di conversione supportato:

Sistema operativo	CPU	UEFI a BIOS	BIOS a UEFI
Windows Vista (senza SP)	x86	No	No
Windows Vista (senza SP)	x64	No	No
Windows Vista SP1	x86	No	No
Windows Vista SP1	x64	Sì	Sì
Windows Server 2008	x86	No	No
Windows Server 2008	x64	Sì	Sì
Windows Server 2008 R2	x64	Sì	Sì
Windows 7	x86	No	No
Windows 7	x64	Sì	Sì
Windows 8	x86	No	No
Windows 8	x64	Sì	Sì
Windows Server 2012	x64	Sì	Sì
Windows 8.1	x86	No	No
Windows 8.1	x64	Sì	Sì
Windows 10	x86	No	No
Windows 10	x64	Sì	Sì
Windows Server 2012 R2	x64	Sì	Sì
Windows Server 2016	x64	Sì	Sì
Windows Server 2019	x64	Sì	Sì

Gestione del menu delle operazioni di ripristino bare metal

Il menu Operazioni di ripristino bare metal comprende i seguenti tre tipi di operazioni:

- Operazioni specifiche del disco
- Operazioni specifiche di volume/partizione
- Operazioni specifiche di ripristino bare metal

Operazioni specifiche del disco:

Per eseguire operazioni specifiche del disco, selezionare l'intestazione del disco e fare clic su **Operazioni**.

Pulitura disco

Questa operazione viene utilizzata per la pulitura di tutte le partizioni di un disco:

- Si tratta di un metodo alternativo per l'eliminazione di tutti i volumi di un disco. L'operazione di **pulitura disco** consente di non eliminare ogni volume singolarmente.
- Viene utilizzata per l'eliminazione di partizioni non-Windows. A causa di una limitazione di VDS, non è possibile eliminare la partizione non-Windows dall'interfaccia utente. Sarà tuttavia possibile utilizzare l'operazione per eseguire la pulitura completa.

  Nota: durante il ripristino bare metal, se il disco di destinazione dispone di partizioni non-Windows o di partizioni OEM, non sarà possibile selezionare la partizione ed eliminarla dall'interfaccia utente di ripristino bare metal. Solitamente, questo problema si verifica se è stato installato Linux/Unix sul disco di destinazione. Per risolvere il problema, eseguire una delle seguenti attività:
- Selezionare l'intestazione del disco nell'interfaccia utente di ripristino bare metal, fare clic su **Operazioni**, quindi utilizzare l'operazione **Pulitura disco** per eliminare tutte le partizioni presenti sul disco.
- Aprire un prompt dei comandi e digitare **Diskpart** per aprire la console del comando Diskpart. Digitare quindi "select disk x" (x corrisponderà al numero di disco) e "clean" per eliminare tutte le partizioni sul disco.

Converti in MBR

Questa operazione consente di convertire un disco in MBR (Master Boot Record, Record di avvio principale). L'operazione è disponibile solamente quando il disco selezionato è un disco GPT (tabella di partizione GUID) e non sono presenti volumi sul disco.

Converti in GPT

Questa operazione viene utilizzata per convertire un disco in GPT. L'operazione è disponibile solamente quando il disco selezionato è un disco MBR e non sono presenti volumi sul disco.

Converti in disco di base

Questa operazione viene utilizzata per convertire un disco in un disco di base. L'operazione è disponibile solamente quando il disco selezionato è un disco dinamico e non sono presenti volumi sul disco.

Converti in disco dinamico

Questa operazione viene utilizzata per convertire un disco in un disco dinamico. L'operazione è disponibile soltanto quando il disco selezionato è un disco di base.

Disco in linea

Questa operazione viene utilizzata per rendere un disco in linea. L'operazione è disponibile soltanto quando il disco selezionato è in stato Non in linea.

Proprietà disco

Questa operazione viene utilizzata per visualizzare proprietà del disco dettagliate. L'operazione è sempre disponibile. Quando viene selezionata, verrà visualizzata la finestra di dialogo **Proprietà disco**.

Operazioni specifiche di volume/partizione:

Per eseguire operazioni di volume/partizione, selezionare l'area di testo del disco, quindi fare clic su **Operazioni**. Questo menu consente di creare nuove partizioni corrispondenti alle partizioni di disco del volume di origine.

Crea partizione primaria

Questa operazione consente di creare una partizione su un disco di base. È disponibile solamente quando l'area selezionata è uno spazio su disco non allocato.

Crea partizione logica

Questa operazione consente di creare una partizione logica su un disco MBR di base. È disponibile solamente quando l'area selezionata è una partizione estesa.

Crea partizione estesa

Questa operazione viene utilizzata per creare una partizione estesa su un disco MBR di base. È disponibile solamente quando il disco è un disco MBR e l'area selezionata è uno spazio su disco non allocato.

Crea partizione di sistema riservato

Questa operazione consente di creare la partizione di sistema riservato su un sistema firmware BIOS e genera una relazione di mapping con la partizione di sistema EFI di origine. L'operazione è disponibile soltanto quando viene eseguito il ripristino di un sistema UEFI in un sistema BIOS.

Nota: se precedentemente è stata eseguita una conversione da UEFI a un sistema compatibile con BIOS, utilizzare l'opzione Crea partizione di sistema riservato per il ridimensionamento del disco di destinazione.

Crea partizione del sistema EFI

Questa operazione viene utilizzata per creare la partizione di sistema EFI su un disco GPT di base. È disponibile solamente quando il firmware del computer di destinazione è UEFI e il disco selezionato è un disco GPT di base.

Nota: se precedentemente è stata eseguita la conversione da BIOS a un sistema compatibile con UEFI, utilizzare l'opzione Crea partizione del sistema EFI per il ridimensionamento del disco di destinazione.

Nota: i sistemi che supportano UEFI richiedono che la partizione di avvio sia anche presente su un disco GPT (Tabella di partizione GUID). Se si utilizza un disco MBR (record di avvio principale), è necessario eseguire la conversione del disco in un disco GPT, quindi utilizzare l'operazione Crea partizione del sistema EFI per il ridimensionamento del disco.

Ridimensiona volume

Questa operazione consente di ridimensionare un volume. Si tratta di un metodo alternativo di Windows Estendi volume/Riduci volume. È disponibile solamente quando l'area selezionata è una partizione di disco valida.

Elimina volume

Questa operazione consente di eliminare un volume. È disponibile solamente quando l'area selezionata è un volume valido.

Elimina partizione estesa

Questa operazione viene utilizzata per eliminare la partizione estesa. È disponibile solamente quando l'area selezionata è una partizione estesa.

Proprietà volume

Questa operazione viene utilizzata per visualizzare le proprietà del volume dettagliate. Quando viene selezionata questa operazione, viene visualizzata la finestra di dialogo **Proprietà volume**.

Operazioni specifiche di ripristino bare metal:

Queste operazioni sono specifiche del ripristino bare metal. Per eseguire operazioni di ripristino bare metal, selezionare l'intestazione del disco o l'area di testo del disco, quindi fare clic su **Operazioni**.

Esegui mapping del disco da

Questa operazione viene utilizzata per stabilire una relazione di mapping tra i dischi dinamici di origine e di destinazione. L'opzione è disponibile soltanto quando il disco selezionato è un disco dinamico.

Nota: quando viene eseguito il mapping su un altro disco, la capacità di ciascun volume di destinazione mappato deve essere uguale o superiore alla capacità del volume di origine corrispondente.

Esegui mapping del volume da

Questa operazione viene utilizzata per stabilire una relazione di mapping tra i volumi di base di origine e di destinazione. L'opzione è disponibile soltanto quando il volume selezionato è un volume di base.

Nota: quando viene eseguito il mapping su un altro disco, la capacità di ciascun volume di destinazione mappato deve essere uguale o superiore alla capacità del volume di origine corrispondente.

Conferma

Questa operazione è sempre disponibile. Tutte le operazioni vengono memorizzate nella cache e non modificano i dischi di destinazione fino alla selezione dell'operazione **Conferma**.

Reimposta

Questa operazione è sempre disponibile. L'operazione **Reimposta** viene utilizzata per abbandonare le operazioni e ripristinare il layout del disco sullo stato predefinito. Viene così eseguita la pulitura di tutte le operazioni memorizzate nella cache. Per reimpostazione si intende ricaricare le informazioni di layout del disco di origine e di destinazione dal file di configurazione e dal sistema operativo corrente, annullando le modifiche apportate dall'utente alle informazioni di layout del disco.

Risoluzione dei problemi relativi al ripristino bare metal

Quando viene rilevato un problema, l'agente Arcserve UDP (Windows) genera un messaggio che consente di identificare e risolvere il problema. Questi messaggi sono contenuti nel **Registro attività** dell'agente Arcserve UDP (Windows). Per accedere a questo registro, utilizzare l'opzione **Visualizza registri** dell'interfaccia utente della pagina principale. Inoltre, in caso di un'azione non corretta, l'agente Arcserve UDP (Windows) visualizza solitamente un messaggio popup che consente all'utente di identificare e risolvere rapidamente il problema.

- Velocità effettiva bassa durante il ripristino bare metal
- I volumi dinamici non sono riconosciuti dal sistema operativo dopo il ripristino bare metal.
- Impossibile eseguire il riavvio del computer virtuale Hyper-V in seguito al ripristino bare metal
- Impossibile eseguire il riavvio del computer virtuale VMware in seguito al ripristino bare metal
- Impossibile avviare il server dopo avere eseguito un ripristino bare metal.
- Errore di invio del processo di ripristino bare metal al Recovery Point Server

Velocità effettiva bassa durante il ripristino bare metal

Questo problema potrebbe essere causato dai controller SATA con AHCI abilitato.

Durante il ripristino bare metal, l'agente Arcserve UDP (Windows) installa i driver per le periferiche sconosciute critiche. Se la periferica dispone già dei driver installati, l'agente Arcserve UDP (Windows) non aggiornerà nuovamente il driver. Windows 7PE contiene già i driver necessari per alcune periferiche, tuttavia, tali driver potrebbero non essere i più indicati e rallentare il processo di ripristino bare metal.

Per risolvere il problema, completare una delle seguenti attività:

- Verificare se la cartella di pool dei driver contiene i driver del disco più recenti. In tal caso, se si sta eseguendo il ripristino sul computer originale, installare il nuovo driver contenuto nella cartella di pool dei driver. In caso di ripristino in un computer alternativo, scaricare i driver del disco più recenti da Internet, e caricarli prima di avviare il recupero dei dati. Per caricare il driver, utilizzare l'utilità drvload.exe, fornita con Windows PE.
- Modificare la modalità operativa della periferica da AHCI (Advanced Host Controller Interface) alla modalità di compatibilità. La modalità di compatibilità consente di ottenere una velocità effettiva superiore.

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Volumi dinamici non riconosciuti dal sistema operativo dopo il ripristino bare metal

Per mantenere lo stato coerente dei dischi dinamici, il sistema operativo Windows esegue la sincronizzazione automatica dei metadati della Gestione dischi logici (LDM) su ciascun disco dinamico. Quando si esegue il ripristino bare metal di un disco dinamico e il disco viene messo in linea, i metadati LDM del disco vengono aggiornati automaticamente dal sistema operativo. In seguito a questa operazione, è possibile che il sistema operativo non sia in grado di riconoscere il disco dinamico che risulta mancante dopo il riavvio del computer.

Per risolvere il problema, quando si esegue il ripristino bare metal con più dischi dinamici, non eseguire operazioni di disco prima della procedura BMR (quali pulizia, eliminazione del volume, e così via).

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Impossibile eseguire il riavvio del computer virtuale Hyper-V in seguito al ripristino bare metal

Se è stato eseguito il ripristino bare metal su un computer Hyper-V costituito da più dischi collegati a un controller IDE (Integrated Drive Electronics) e non è possibile eseguire il riavvio del server, eseguire la seguente procedura per la risoluzione del problema:

1. Verificare che il disco contenente il volume di sistema corrisponda al disco master.

   La BIOS Hyper-V esegue la ricerca del volume di sistema sul disco principale (disco 1) connesso al canale principale. Se il volume di sistema non viene individuato sul disco principale, non sarà possibile eseguire il riavvio del computer virtuale.

   Nota: Verificare che il disco contenente il volume di sistema sia connesso a un controller di IDE. Impossibile riavviare Hyper-V da un disco SCSI.

2. Se necessario, modificare le impostazioni Hyper-V, per connettere il disco contenente il volume di sistema al canale principale IDE e riavviare nuovamente il computer virtuale.

   Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Impossibile eseguire il riavvio del computer virtuale VMware in seguito al ripristino bare metal

Se è stato eseguito il ripristino bare metal su un computer VMware costituito da più dischi connessi a un controller IDE (Integrated Drive Electronics) o a una scheda SCSI e non è possibile eseguire il riavvio del server, attenersi alla seguente procedura per la risoluzione del problema:

1. Verificare che il disco contenente il volume di sistema corrisponda al disco master.

   La BIOS VMware esegue la ricerca del volume di sistema sul disco principale (disco 0) connesso al canale principale. Se il volume di sistema non viene individuato sul disco principale, non sarà possibile eseguire il riavvio del computer virtuale.

2. Se necessario, modificare le impostazioni del computer VMware, per connettere il disco contenente il volume di sistema al canale master di IDE e riavviare nuovamente il computer virtuale.

3. Se si tratta di un disco SCSI, verificare che il disco contenente il volume di avvio sia il primo disco ad eseguire la connessione alla scheda SCSI. In caso contrario, assegnare il disco di avvio dal BIOS VMware.

4. Verificare che il disco contenente il volume di avvio sia incluso negli 8 dischi precedenti, in quanto il BIOS VMware è in grado di individuare un numero massimo di 8 dischi durante l'avvio. Se il disco contenente i volumi di sistema connessi alla scheda SCSI è preceduto da più di 7 dischi, non sarà possibile eseguire l'avvio del computer virtuale.

   Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Impossibile avviare il server dopo avere eseguito un ripristino bare metal.

Sintomo

Se il computer di origine è un server Active Directory su cui è in esecuzione un ripristino bare metal verso un computer fisico con hardware differente o un computer virtuale su un server Hyper-v, il server non si avvia e viene visualizzata una schermata blu con il messaggio seguente:

STOP: c00002e2 Directory Services could not start because of the following error: a device attached to the system is not functioning. Stato di errore: 0xc0000001.

Soluzione

Riavviare il sistema nell'ambiente PE di ripristino bare metal, rinominare tutti i file *.log nella cartella C:\Windows\NTDS e riavviare il sistema. Ad esempio, rinominare il file edb.log in edb.log.old e riavviare il sistema.

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Errore di invio del processo di ripristino bare metal al Recovery Point Server

È supportato soltanto un processo di ripristino bare metal per l'esecuzione di un ripristino dallo stesso server RPS per lo stesso nodo (backup agente o backup basato su host). L'operazione è controllata dal monitoraggio del processo del server RPS.

Se il computer su cui è in esecuzione il processo di ripristino bare metal viene interrotto o riavviato in maniera imprevista, il monitoraggio del processo sul lato server RPS attenderà 10 minuti per poi scadere. In questi 10 minuti non sarà possibile avviare un altro ripristino bare metal per lo stesso nodo dallo stesso server RPS.

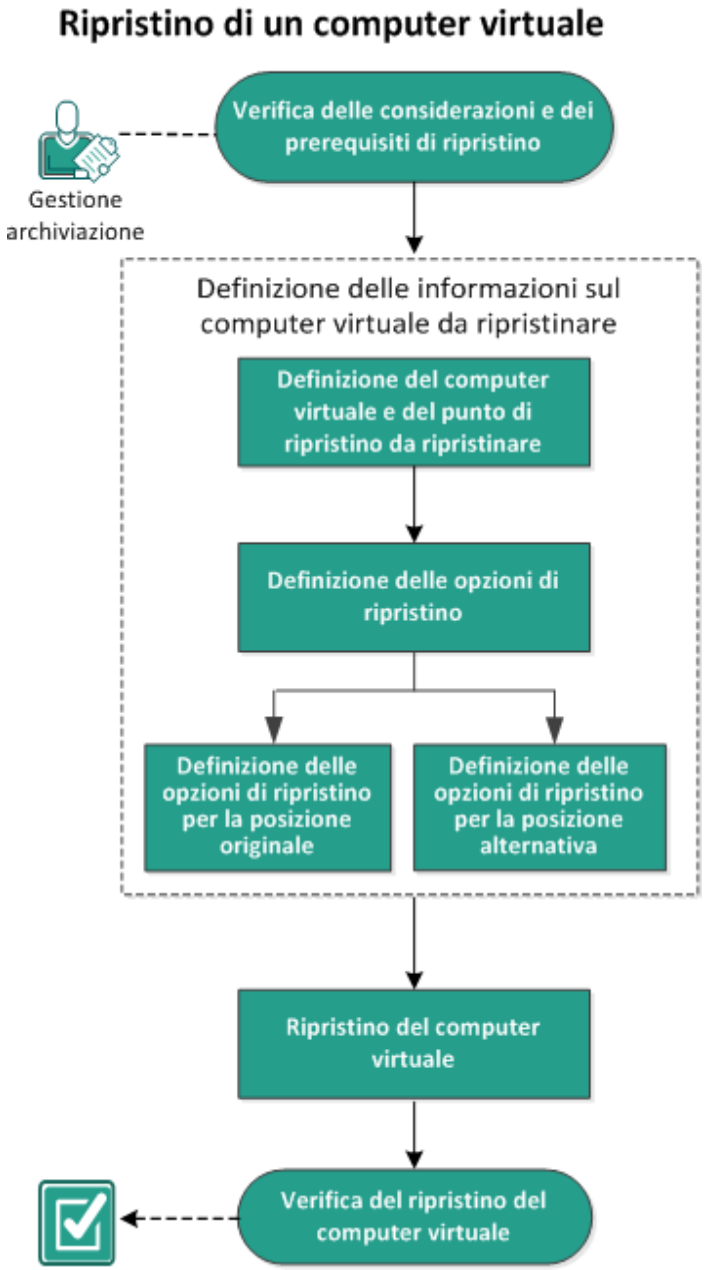
Se il ripristino bare metal viene interrotto dall'interfaccia utente di ripristino bare metal, il problema non si verifica.

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Ripristino di un computer virtuale

Arcserve UDP consente di utilizzare l'opzione **Recupera computer virtuale** per ripristinare un computer virtuale di cui in precedenza è stato eseguito il backup senza agente basato su host. Questo metodo permette di ripristinare l'intero computer virtuale nella posizione originale o in una posizione ESX o Hyper-V alternativa. È possibile individuare i punti di ripristino disponibili per il computer virtuale da una visualizzazione di calendario e selezionare il punto da ripristinare.

Il diagramma seguente mostra il processo di ripristino da un computer virtuale:



Completare le attività seguenti per ripristinare un computer virtuale:

1. Verifica delle considerazioni e dei prerequisiti di ripristino
2. Definizione delle informazioni sul computer virtuale da ripristinare
    a. Definizione del computer virtuale e del punto di ripristino da ripristinare
    b. Definizione delle opzioni di ripristino
        - Definizione delle opzioni di ripristino per la posizione originale
        - Definizione delle opzioni di ripristino per la posizione alternativa
3. Ripristino del computer virtuale
4. Verifica del ripristino del computer virtuale

Verifica delle considerazioni e dei prerequisiti di ripristino

Verificare i seguenti prerequisiti prima di procedere al ripristino:

- Si dispone di punto di ripristino valido da cui eseguire il ripristino.
- È necessario disporre di un server Virtual Center/ESX o Hyper-V valido e accessibile per il ripristino del computer virtuale.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Verificare le seguenti considerazioni sul ripristino:

- Se la destinazione di recupero del computer virtuale è Windows Server 2008 R2, il computer virtuale del backup di origine non dovrà contenere dischi VHDx, i quali non sono supportati dal server Hyper-V (Windows Server 2008 R2).
- Se la destinazione di recupero del computer virtuale è Windows Server 2008 R2 o Windows 2012, il tipo di sistema secondario del computer virtuale del backup di origine non dovrà essere Generazione 2 (funzionalità introdotta con Windows Server 2012 R2) e non sarà supportato sul server Hyper-V (Windows Server 2012/2008 R2).

Definizione delle informazioni sul computer virtuale da ripristinare

È possibile eseguire il ripristino di un intero computer virtuale da un punto di ripristino.

Il processo interessato nel ripristino del computer virtuale è il seguente:

1. Definizione del computer virtuale e del punto di ripristino da ripristinare
2. Definizione delle opzioni di ripristino
   - Definizione delle opzioni di ripristino per la posizione originale
   - Definizione delle opzioni di ripristino per la posizione alternativa

Definizione del computer virtuale e del punto di ripristino da ripristinare

Utilizzare l'opzione **Recupera computer virtuale** per ripristinare un computer virtuale di cui è già stato eseguito il backup. Questo metodo consente di creare in modo rapido e uniforme un computer virtuale da un punto di ripristino di Arcserve UDP su un server ESX o Hyper-V. Il computer virtuale recuperato può quindi essere avviato per completare il processo di ripristino.

Effettuare le operazioni seguenti:

1. Accedere alla finestra di dialogo per la selezione del metodo di ripristino in uno dei modi seguenti:

   Da Arcserve UDP:

   a. Accedere ad Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

      Nota: Viene effettuato automaticamente l'accesso al nodo agente e la finestra di dialogo per la selezione del metodo di ripristino viene visualizzata dal nodo agente.

   Dall'agente Arcserve UDP (Windows):

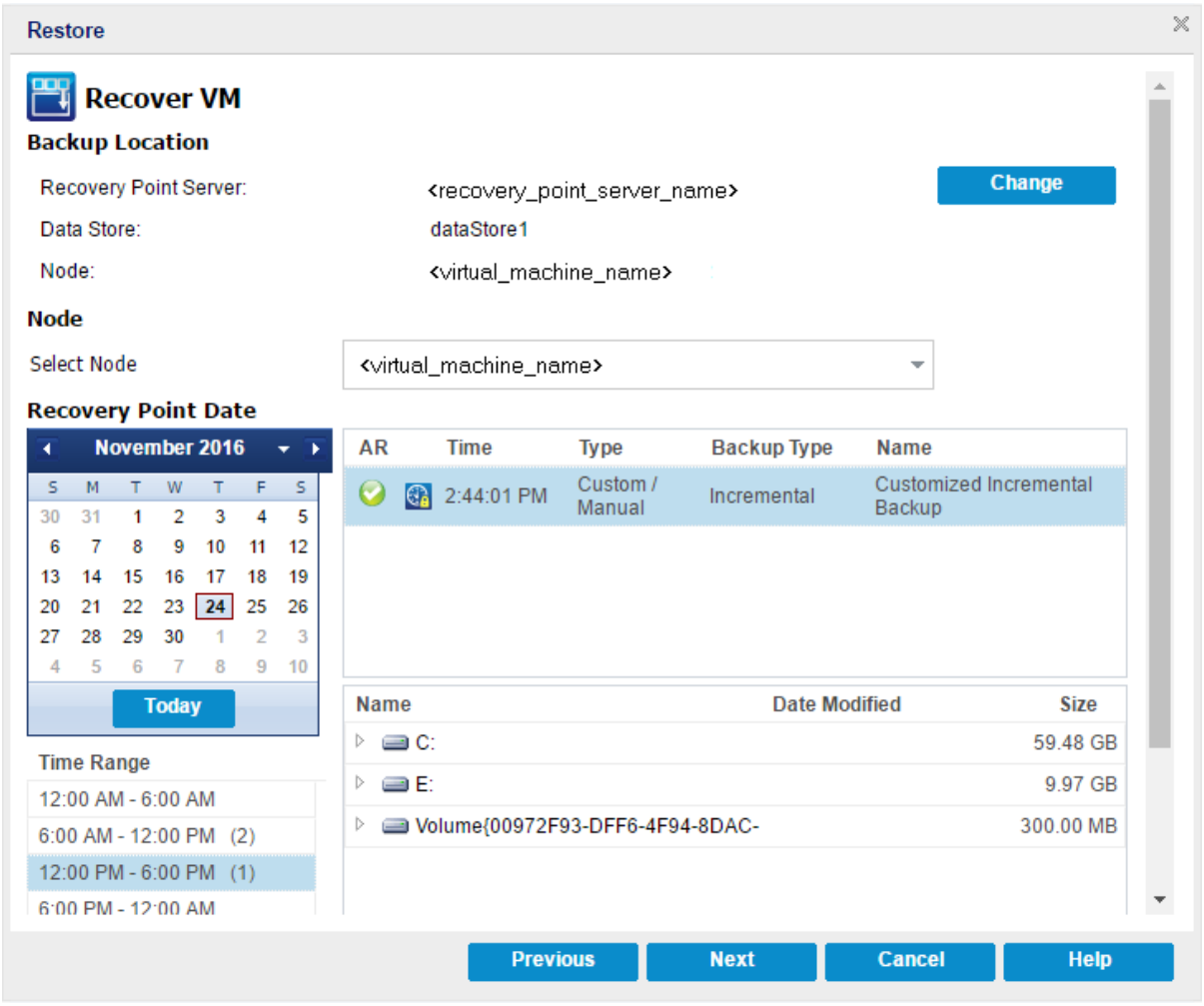
   a. Accedere all'agente Arcserve UDP (Windows).

   b. Dalla pagina principale selezionare **Ripristino**.

   Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

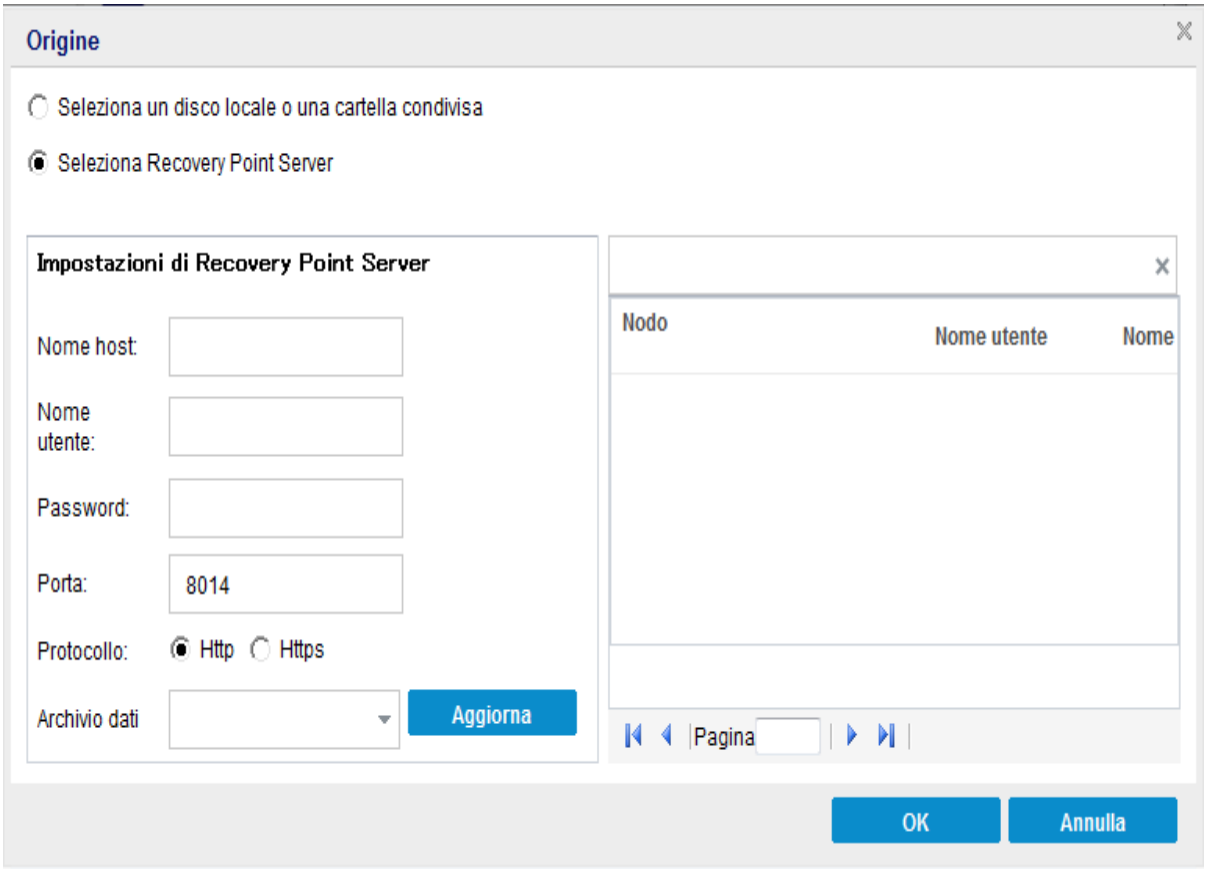
2. Fare clic sull'opzione **Recupera computer virtuale**.

   Viene visualizzata la finestra di dialogo **Recupera computer virtuale**.



3. Fare clic su **Modifica** per modificare la posizione di backup.

   Viene visualizzata la finestra di dialogo **Origine**. È possibile selezionare la posizione di backup in questa finestra di dialogo.



4. Selezionare una delle seguenti opzioni:

   Selezione di un disco locale o una cartella condivisa

   a. Specificare o accedere al percorso di archiviazione delle immagini di backup e selezionare l'origine di backup appropriata.

      Per verificare la connessione al percorso specificato, fare clic sulla freccia verde. Se necessario, immettere le credenziali Nome utente e Password per poter accedere alla posizione di origine.

      Viene visualizzata la finestra di dialogo **Selezionare la posizione di backup**.

   b. Selezionare la cartella di archiviazione dei punti di ripristino e fare clic su **OK**.

      La finestra di dialogo **Selezionare la posizione di backup viene chiusa** e la posizione di backup viene visualizzata nella finestra di dialogo **Origine**.

   c. Fare clic su **OK**.

   I punti di ripristino sono elencati nella finestra di dialogo **Recupera computer virtuale**.

   Selezione di un Recovery Point Server

a. Specificare i dettagli dell'impostazione Recovery Point Server e fare clic su **Aggiorna**.

   Tutti i nodi(agenti/computer virtuali) vengono elencati nella colonna Nodo della finestra di dialogo **Origine.**

b. Selezionare il nodo (agente/computer virtuale) dall'elenco visualizzato e fare clic su **OK**.

   I punti di ripristino sono elencati nella finestra di dialogo **Recupera computer virtuale**.

5. Dal menu a discesa **Computer virtuale**, selezionare il computer virtuale da ripristinare.

   Viene mostrata la visualizzazione di calendario con tutte le date contenenti punti di ripristino per l'origine di backup specificata evidenziate in verde.

6. Selezionare la data corrispondente all'immagine del computer virtuale da ripristinare.

   Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito e al nome del backup.

7. Selezionare un punto di ripristino da ripristinare.

   Viene visualizzato il contenuto di backup (incluse tutte le applicazioni) per il punto di ripristino selezionato. Durante il ripristino di un computer virtuale, viene eseguito il ripristino dell'intero sistema. Di conseguenza, sarà possibile visualizzare, ma non selezionare, singoli volumi, cartelle o file del computer virtuale selezionato.

   Nota: l'icona di orologio con il simbolo di lucchetto indica che il punto di ripristino contiene informazioni crittografate e che potrebbe richiedere una password per il ripristino.

8. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Opzioni di ripristino**.

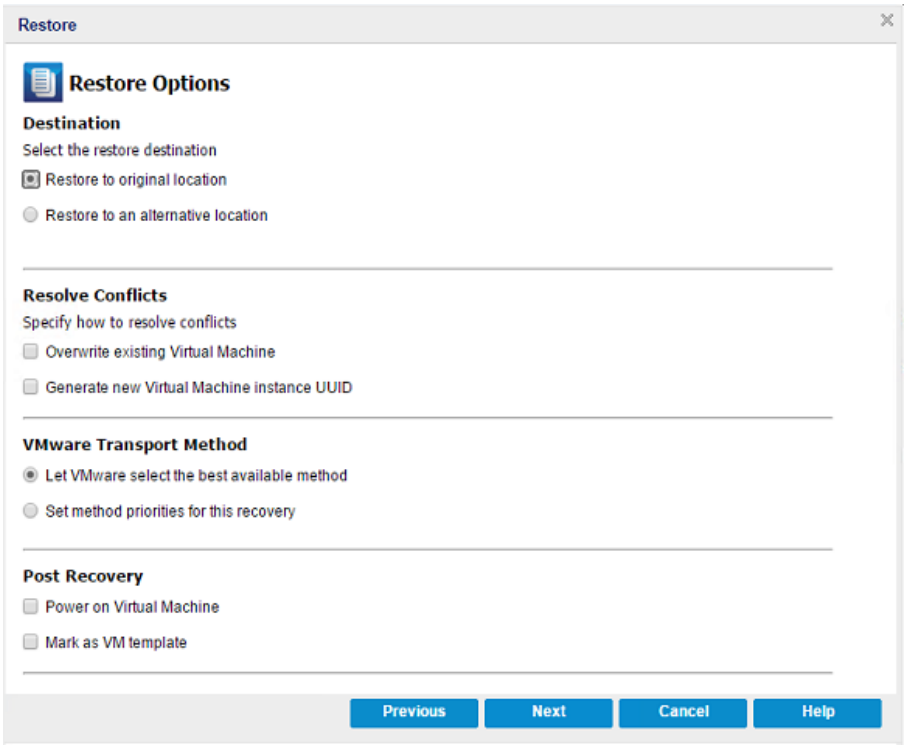
   Vengono specificati il computer virtuale e il punto di ripristino da ripristinare.

Definizione delle opzioni di ripristino

Dopo avere specificato il computer virtuale e il punto di ripristino da ripristinare, definire le opzioni di ripristino per l'immagine del computer virtuale selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo Opzioni di ripristino, selezionare la destinazione di ripristino.



Le opzioni di destinazione disponibili sono:

Ripristina in posizione originale

Esegue il ripristino del computer virtuale nella posizione originale in cui è stata acquisita l'immagine di backup. Questa opzione è selezionata per impostazione predefinita.

Per ulteriori informazioni, consultare la sezione Definizione delle opzioni di ripristino per la posizione originale.

Ripristina in una posizione alternativa

Esegue il ripristino del computer virtuale in un percorso diverso da quello in cui è stata acquisita l'immagine di backup.

Per ulteriori informazioni, consultare la sezione Definizione delle opzioni di ripristino per la posizione alternativa.

2. (Facoltativo) Selezionare la casella di controllo **Utilizzare la rete del server RPS selezionata per il ripristino del traffico**, quindi procedere come segue:
    a. Per abilitare la comunicazione tra il server proxy Windows e il Recovery Point Server, selezionare la rete CIDR dall'elenco a discesa.
    b. Per definire i vincoli di SMB Multichannel in modo che i dati vengano trasferiti solo tramite la rete selezionata, selezionare la casella di controllo **Usa l'ethernet apposita se il computer corrente abilita SMB Multichannel**.

        Note:

        - Per impostazione predefinita, questa opzione non è disponibile. Per attivare questa opzione, creare la stringa *UseDedicatedEthernet* nel seguente percorso, quindi impostare il valore di registro su 1:

            SOFTWARE\Arcserve\Unified Data Protection\Engine
        - Quando si esegue un processo di ripristino dalla pagina Nodi, creare una chiave di registro sul proxy di backup.
        - Quando si esegue un processo di ripristino dall'agente normale utilizzando la sessione di backup RPS, creare una chiave di registro sull'agente normale.
3. (Facoltativo) Selezionare la casella di controllo **Utilizzare la rete del server RPS selezionata per il ripristino del traffico**, quindi procedere come segue:
    a. Per abilitare la comunicazione tra il server proxy Windows e l'Hypervisor, selezionare la rete CIDR dall'elenco a discesa.
    b. Per definire i vincoli di SMB Multichannel in modo che i dati vengano trasferiti solo tramite la rete selezionata, selezionare la casella di controllo **Usa l'ethernet apposita se il computer corrente abilita SMB Multichannel**.

        Note:

        - Per impostazione predefinita, questa opzione non è disponibile. Per attivare questa opzione, creare la stringa *UseDedicatedEthernet* nel seguente percorso, quindi impostare il valore di registro su 1:

            SOFTWARE\Arcserve\Unified Data Protection\Engine
        - Quando si esegue un processo di ripristino dalla pagina Nodi, creare una chiave di registro sul proxy di backup.
        - Quando si esegue un processo di ripristino dall'agente normale utilizzando la sessione di backup RPS, creare una chiave di registro sull'agente normale.

4. Specificare le opzioni Risoluzione conflitti che verranno eseguite da Arcserve UDP in caso di conflitti durante il processo di ripristino

   Sovrascrivi il computer virtuale esistente

   Questa opzione consente di specificare se sovrascrivere il computer virtuale esistente. Per impostazione predefinita, l'opzione di sovrascrittura non è selezionata.

   Nota: Per l'opzione Sovrascrivi il computer virtuale esistente, con "computer virtuale esistente" si intende un computer virtuale con lo stesso nome e contenuto nello stesso host ESXi (per il computer virtuale VMware), oppure un computer virtuale con lo stesso nome e lo stesso UUID di istanza contenuto nello stesso host Hyper-V (per il computer virtuale Hyper-V). Se è presente un computer virtuale con lo stesso nome ma che risiede in un host ESXi diverso (compreso nello stesso vCenter), non sarà possibile utilizzare l'opzione di sovrascrittura. In questo caso, l'interfaccia utente grafica del computer virtuale rileva quel computer virtuale e mostra un messaggio di errore. Impedisce inoltre all'utente di procedere, in modo che il computer virtuale non venga sovrascritto per errore. Per risolvere il problema, è necessario rinominare il computer virtuale esistente oppure utilizzare l'opzione Ripristina in posizione alternativa, quindi specificare un nome di computer virtuale diverso.

   - Se si seleziona questa opzione, il processo di ripristino sovrascriverà (sostituirà) le immagini esistenti del computer virtuale contenute nella destinazione di ripristino specificata. L'immagine del computer virtuale verrà ripristinata dai file di backup indipendentemente dalla sua presenza sulla destinazione di ripristino.
   - Se non si seleziona questa opzione, l'interfaccia utente grafica di recupero del computer virtuale mostra un messaggio di errore e impedisce all'utente di proseguire se il computer virtuale originale è ancora presente nella posizione originale. Per risolvere il problema, è necessario rinominare il computer virtuale esistente oppure utilizzare l'opzione Ripristina in posizione alternativa, quindi specificare un nome di computer virtuale diverso.

   Generate new Virtual Machine instance UUID (Genera nuovo UUID istanza del computer virtuale)

   Questa opzione consiste di specificare se si desidera generare un nuovo UUID istanza per il computer virtuale ripristinato o conservare l'UUID dell'istanza originale.

   Nota: se non si seleziona questa opzione, l'UUID di istanza originale viene impostato sul computer virtuale ripristinato. Tuttavia, nel caso in cui il server vCenter/ESXi di destinazione o l'host Hyper-V dispongano già di un computer

virtuale con lo stesso UUID dell'istanza, verrà invece utilizzato il nuovo UUID e verrà visualizzato un messaggio di avviso nel registro attività del processo di ripristino del computer virtuale.

5. Specificare l'opzione Post-recupero.

   Attiva computer virtuale

   Specificare se avviare il computer virtuale al termine del processo di ripristino. Per impostazione predefinita, questa opzione non è selezionata.

   Contrassegna come modello del computer virtuale (disponibile solo per computer virtuale VMware)

   Selezionare se convertire il computer virtuale ripristinato in modello. Se il nodo di origine è un computer virtuale in fase di backup, questa opzione non è selezionata per impostazione predefinita. Se il nodo di origine è un modello in fase di backup, questa opzione è selezionata per impostazione predefinita.

   Le opzioni di ripristino vengono definite per il ripristino di un computer virtuale.

Definizione delle opzioni di ripristino per la posizione originale

Durante il processo di configurazione per il recupero di un computer virtuale, è necessario selezionare la posizione in cui di desidera ripristinare il computer virtuale. Le opzioni disponibili sono **Ripristina in posizione originale** e **Ripristina in posizione alternativa**.

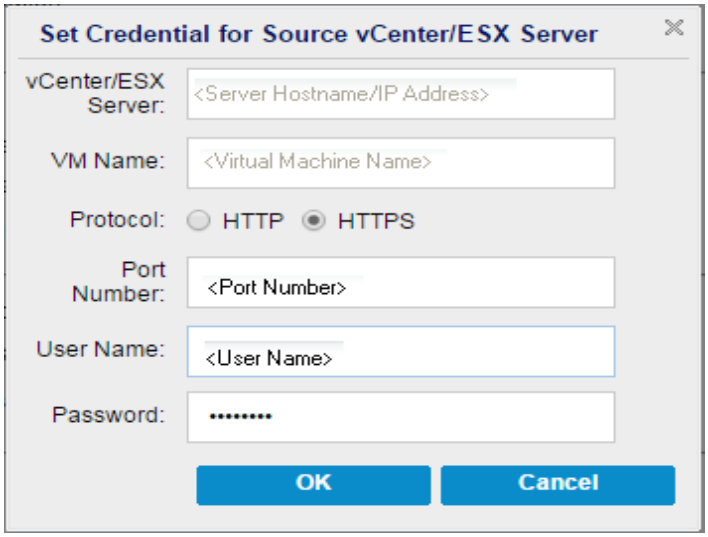
La presente procedura descrive il ripristino di un computer virtuale nella posizione originale.

Effettuare le operazioni seguenti:

1. Dalla finestra di dialogo **Opzioni di ripristino**, dopo aver specificato le opzioni **Risoluzione dei conflitti** e **Post-recupero**, selezionare l'opzione **Ripristina in posizione originale**, quindi fare clic su **Avanti**.

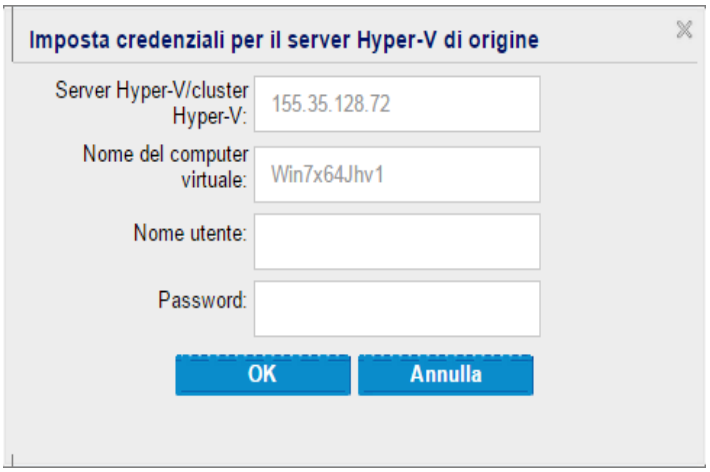
   Verrà visualizzata la finestra di dialogo corrispondente per VMware o Hyper-V.

   - Per VMware verrà visualizzata la finestra di dialogo **Imposta credenziali per il server vCenter/ESX di origine**.



   - Per Hyper-V verrà visualizzata la finestra di dialogo **Imposta credenziali per**

il server Hyper-V di origine.



2. Specificare le credenziali di accesso al computer virtuale.
   - Per VMware, completare i campi seguenti.

     Server vCenter/ESX

     Visualizza il nome host o l'indirizzo IP del sistema server vCenter o ESX di destinazione.

     Nota: Non è possibile modificare questo campo. È possibile visualizzare soltanto i dettagli.

     Nome computer virtuale

     Mostra il nome del computer virtuale di cui si sta eseguendo il ripristino.

     Nota: Non è possibile modificare questo campo. È possibile visualizzare soltanto i dettagli.

     Protocollo

     Specifica il protocollo da utilizzare per la comunicazione con il server di destinazione. Le opzioni disponibili sono HTTP e HTTPS.

     Numero porta

     Specifica la porta da utilizzare per il trasferimento dei dati tra il server di origine e la destinazione.

     Impostazione predefinita: 443.

     Nome utente

     Specifica il nome dell'utente che dispone dei diritti di accesso al server vCenter/ESX su cui ripristinare il computer virtuale.

     Password

     Consente di specificare la password corrispondente al nome utente.

- Per Hyper-V, completare i campi seguenti.

  Server Hyper-V/cluster Hyper-V

  Mostra il nome host o l'indirizzo IP del sistema server o cluster Hyper-V di destinazione.

  Nota: Non è possibile modificare questo campo. È possibile visualizzare soltanto i dettagli.

  Nome computer virtuale

  Mostra il nome del computer virtuale di cui si sta eseguendo il ripristino.

  Nota: Non è possibile modificare questo campo. È possibile visualizzare soltanto i dettagli.

  Nome utente

  Specifica il nome dell'utente che dispone dei diritti di accesso al server Hyper-V su cui ripristinare il computer virtuale. Per un computer virtuale cluster Hyper-V, specificare l'account di dominio con privilegi amministrativi sul cluster.

  Password

  Consente di specificare la password corrispondente al nome utente.

3. Fare clic su **OK**.

   Verrà visualizzata la finestra di dialogo **Riepilogo di ripristino**.

   Vengono definite le opzioni di ripristino per la posizione originale.

Definizione delle opzioni di ripristino per la posizione alternativa

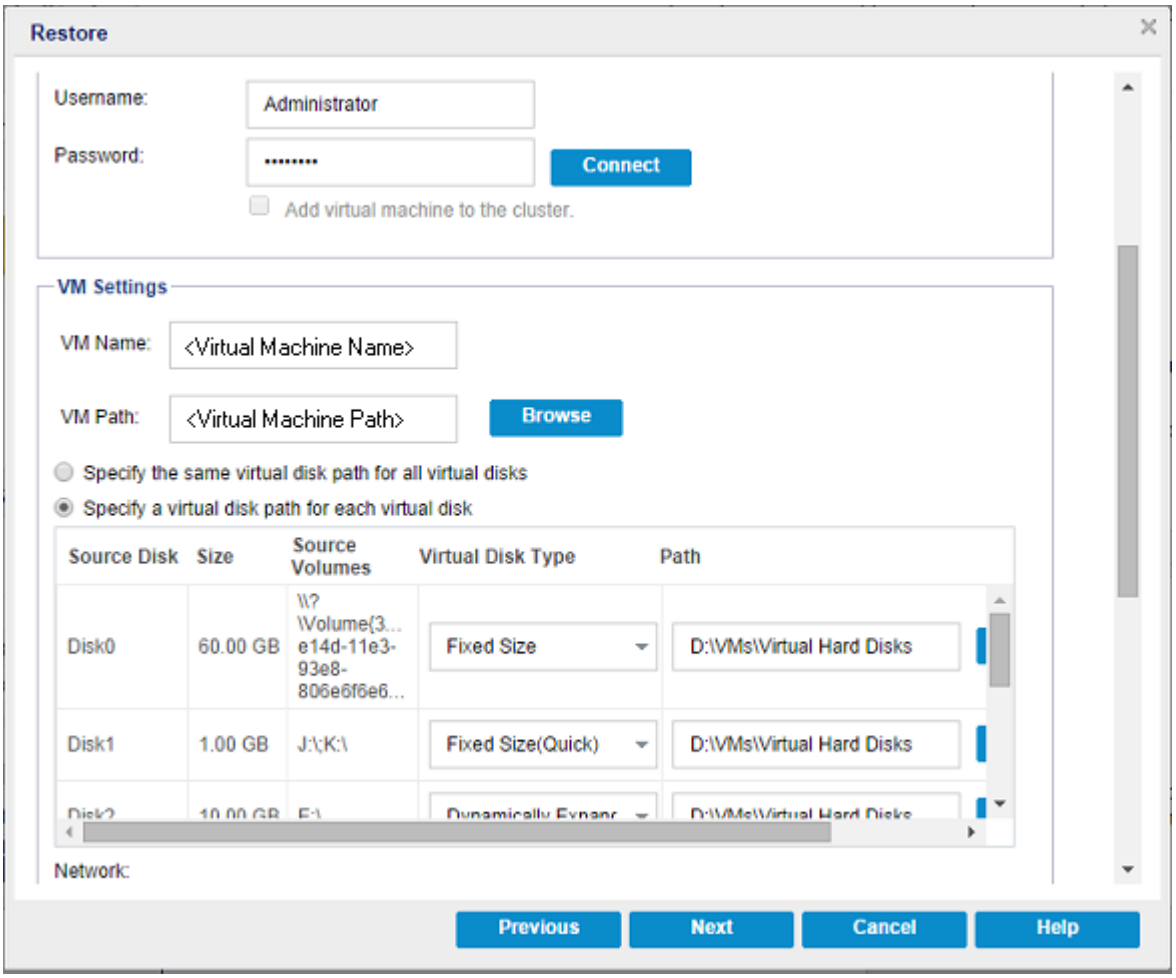
Durante il processo di configurazione del computer virtuale di ripristino, è necessario specificare la posizione di archiviazione del computer virtuale di cui è stato eseguito il recupero. Le opzioni disponibili sono **Ripristina in posizione originale** e **Ripristina in posizione alternativa**.

La presente procedura descrive il procedimento di ripristino di un computer virtuale in una posizione alternativa o un archivio dati differente.

Effettuare le operazioni seguenti:

1. Dalla finestra di dialogo **Opzioni di ripristino**, dopo aver specificato le opzioni **Risoluzione dei conflitti** e **Post-recupero**, selezionare l'opzione **Ripristina in posizione alternativa**.
   - Per VMware, la finestra di dialogo **Opzioni di ripristino** verrà espansa per visualizzare ulteriori opzioni di ripristino in posizione alternativa.
   - Per Hyper-V, la finestra di dialogo **Opzioni di ripristino** verrà espansa per visualizzare ulteriori opzioni di ripristino in posizione alternativa.

   Se si seleziona l'opzione **Specificare un percorso per ogni disco virtuale**, viene visualizzata la finestra di dialogo seguente:



2. Specificare le informazioni relative al server corrispondenti.
   - Per VMware, completare i campi seguenti:

     Server vCenter/ESX

     Specifica il nome host o l'indirizzo IP del sistema server vCenter o ESX di destinazione.

     Nome utente

     Specifica il nome dell'utente che dispone dei diritti di accesso al server vCenter/ESX su cui ripristinare il computer virtuale.

     Password

     Consente di specificare la password corrispondente al nome utente.

     Protocollo

     Specifica il protocollo da utilizzare per la comunicazione con il server di destinazione. Le opzioni disponibili sono HTTP e HTTPS.

     Valore predefinito: HTTPS.

Nota: VMware Virtual Disk Development Kit (VDDK) 6.x.x è integrato in Arcserve UDP versione 6.5. Tuttavia, VDDK 6.x.x non supporta il protocollo HTTP. Verificare che sia selezionato HTTPS salvo quando si sostituisce manualmente la versione VDDK 6.x.x integrata con un'altra.

Numero porta

Specifica la porta da utilizzare per il trasferimento dei dati tra il server di origine e la destinazione.

Valore predefinito: 443

- Per Hyper-V, completare i campi seguenti:

Server Hyper-V

Visualizza il nome host o l'indirizzo IP del sistema server Hyper-V di destinazione.

Nome utente

Specifica il nome dell'utente che dispone dei diritti di accesso al server Hyper-V su cui ripristinare il computer virtuale. Per un computer virtuale cluster Hyper-V, specificare l'account di dominio con privilegi amministrativi sul cluster.

Password

Consente di specificare la password corrispondente al nome utente.

Aggiungi computer virtuale al cluster

Selezionare l'opzione se si desidera aggiungere il computer virtuale ripristinato da Arcserve UDP al cluster. Valutare le seguenti opzioni:

- Se si fornisce il nome del nodo cluster come il nome di server Hyper-V, la casella di controllo è disabilitata e selezionata per impostazione predefinita. Di conseguenza, il computer virtuale viene aggiunto automaticamente al cluster.
- Se si fornisce il nome host di un server Hyper-V compreso nel cluster, la casella di controllo è abilitata ed è possibile selezionare di aggiungere il computer virtuale al cluster.
- Se si fornisce il nome host di un server Hyper-V standalone non compreso nel cluster, la casella di controllo è disabilitata e deselezionata.

3. Dopo aver specificato le informazioni relative al server vCenter/ESX o al server Hyper-V, fare clic sul pulsante **Connetti a questo server vCenter/ESX** o sul pulsante **Connetti a questo server Hyper-V**.

Se le informazioni per l'accesso al server alternativo sono corrette, verrà abilitato il campo **Impostazioni del computer virtuale**.

4. Specificare le impostazioni del **computer virtuale**.
   - Per VMware, completare i campi seguenti:

     Nome computer virtuale

     Specifica il nome del computer virtuale di cui si sta eseguendo il ripristino.

     Server ESX

     Specifica il server ESX di destinazione. Nel menu a discesa sarà disponibile un elenco di tutti i server ESX associati al server vCenter.

     Pool di risorse

     Seleziona il **pool di risorse** o il **pool vApp** da utilizzare per il ripristino del computer virtuale.

     Nota: un pool di risorse è una raccolta configurata di CPU e di risorse di memoria. Un pool vApp è una raccolta di uno o più computer virtuali che può essere gestita come un singolo oggetto.

     Impostazione predefinita: vuoto.

     Fare clic sul pulsante **Sfoglia pool di risorse** per visualizzare la finestra di dialogo **Selezionare un pool di risorse.** Questa finestra di dialogo contiene un elenco di tutti i pool di risorse e i pool vApp disponibili per il server ESX di destinazione. Selezionare il pool da utilizzare per il ripristino del computer virtuale. È possibile lasciare vuoto il campo se non si desidera assegnare un pool di risorse o un pool vApp per il ripristino di questo computer virtuale.



Criterio di archiviazione

Specificare il criterio di archiviazione del computer virtuale applicato al computer virtuale principale del computer virtuale ripristinato. Selezionare Archivio dati predefinito se non si desidera applicare il criterio di archiviazione del computer virtuale.

Nota: se è possibile visualizzare soltanto i valori predefiniti dell'archivio dati ma sono presenti altri criteri di archiviazione in vCenter, l'account utilizzato per stabilire la connessione a vCenter non dispone di privilegi sufficienti per ottenere il criterio di archiviazione da vCenter. Verificare che l'account disponga dei privilegi di visualizzazione a livello di profilo per vCenter.

Archivio dati del computer virtuale

Specificare l'archivio dati di destinazione per il computer virtuale principale ripristinato.

Nota: per impostazione predefinita, vengono elencati soltanto gli archivi dati compatibili con i criteri di archiviazione elencati selezionati. Se si desidera visualizzare tutti gli archivi dati, deselezionare la casella di controllo **Mostra solo archivi dati compatibili per il criterio di archiviazione selezionato** contenuto nella tabella Archivio dati su disco.

Archivio dati su disco

Specificare il tipo di disco virtuale, il criterio di archiviazione e l'archivio dati di destinazione per ciascun disco virtuale del computer virtuale.

- Tipo di disco virtuale: selezionare una delle seguenti opzioni: Thin, Thick Lazy azzerato o Thick Eager azzerato.
- Criterio di archiviazione: selezionare un criterio di archiviazione del computer virtuale applicato al disco virtuale. Selezionare Archivio dati predefinito se non si desidera applicare il criterio di archiviazione del computer virtuale.
- Archivio dati di destinazione: selezionare l'archivio dati in cui è stato ripristinato il disco virtuale.

Nota: per impostazione predefinita, vengono elencati soltanto gli archivi dati compatibili con i criteri di archiviazione selezionati. Se si desidera visualizzare tutti gli archivi dati, deselezionare la casella di controllo **Mostra solo archivi dati compatibili per il criterio di archiviazione selezionato** contenuto nella tabella Archivio dati su disco.

Rete

Specifica i dettagli di configurazione dello switch standard vSphere/switch distribuito vSphere.

- Per Hyper-V, completare i campi seguenti.

Nome computer virtuale

Specifica il nome del computer virtuale di cui si sta eseguendo il ripristino.

Percorso computer virtuale

Specifica il percorso di destinazione (sul server Hyper-V) su cui salvare il file di configurazione del computer virtuale Hyper-V. La cartella predefinita del file di configurazione del computer virtuale per il server Hyper-V viene visualizzata per impostazione predefinita. È possibile modificare il percorso direttamente nel campo oppure fare clic su **Sfoglia** per selezionarne uno.

Nota: In caso di ripristino del computer virtuale in un cluster Hyper-V, se si desidera eseguire la migrazione del computer virtuale nei nodi del cluster, specificare il volume condiviso cluster (CSV) per il percorso del computer virtuale e il percorso del disco virtuale.

Specificare lo stesso percorso per tutti i dischi virtuali

Specificare un percorso (sul server Hyper-V) su cui salvare tutti i dischi virtuali del computer virtuale. La cartella predefinita del file di disco del

computer virtuale per il server Hyper-V viene visualizzata per impostazione predefinita. È possibile modificare il percorso direttamente nel campo oppure fare clic su **Sfoglia** per selezionarne uno.

Nota: In caso di ripristino del computer virtuale in un cluster Hyper-V, se si desidera eseguire la migrazione del computer virtuale nei nodi del cluster, specificare il volume condiviso cluster (CSV) per il percorso del computer virtuale e il percorso del disco virtuale.

Specificare un percorso per ogni disco virtuale

Specificare un percorso (sul server Hyper-V) per ogni disco virtuale del computer virtuale. La cartella predefinita del file di disco del computer virtuale per il server Hyper-V viene visualizzata per impostazione predefinita. È possibile modificare il percorso direttamente nel campo oppure fare clic su **Sfoglia** per selezionarne uno. Per assegnare il tipo di disco virtuale, selezionare una delle opzioni seguenti: Dimensione fissa, Dimensione fissa (Quick), Espansione dinamica e Mantieni come disco di origine.

Note:

- In caso di ripristino del computer virtuale in un cluster Hyper-V, se si desidera eseguire la migrazione del computer virtuale nei nodi del cluster, specificare il volume condiviso cluster (CSV) per il percorso del computer virtuale e il percorso del disco virtuale.
- Non utilizzare l'opzione Dimensione fissa (Quick) salvo quando si è certi di non aver salvato in precedenza informazioni sensibili sulla periferica di archiviazione in cui risiede il file del disco virtuale.

Dimensione fissa (Quick)

Con questa opzione è possibile ripristinare il disco di dimensione fissa in modo più rapido. Non è necessario azzerare i blocchi di disco inutilizzati in fase di ripristino del disco. Tuttavia, è possibile che alcuni frammenti dei dati originali restino nell'archiviazione sottostante. Questa situazione comporta il rischio di perdite delle informazioni. Dopo aver montato il disco nel computer virtuale, l'utente del computer virtuale può utilizzare alcuni strumenti di disco per analizzare i dati grezzi nel disco e ottenere i dati originali sulla periferica di archiviazione del server Hyper-V in cui risiede il file del disco virtuale.

Rete

Specifica i dettagli di configurazione di rete per il computer virtuale.

5. Fare clic su **OK**.

Verrà visualizzata la finestra di dialogo **Riepilogo di ripristino**.

Vengono definite le opzioni di ripristino per la posizione alternativa.

Ripristino del computer virtuale

Il **Riepilogo ripristino** consente di verificare tutte le opzioni di ripristino definite e, se necessario, di modificarle.

Nella finestra di dialogo **Riepilogo ripristino**, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.

- Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
- Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

Verrà eseguito il ripristino del computer virtuale.

Verifica del ripristino del computer virtuale

Dopo il completamento del processo di ripristino, verificare che il computer virtuale sia stato ripristinato nella destinazione specificata.

Effettuare le operazioni seguenti:

1. Accedere alla destinazione di ripristino specificata.

   Ad esempio, se si sceglie di ripristinare il computer virtuale nella destinazione di ripristino come posizione originale, accedere al server Center/ESX o Hyper-V originale e controllare se il computer virtuale è presente.

   Se si sceglie di ripristinare il computer virtuale nella posizione alternativa, accedere al server Center/ESX o Hyper-V alternativo fornito nelle opzioni di ripristino e controllare se il computer virtuale è presente.

2. Verificare che il computer virtuale sia stato ripristinato.

   Il ripristino del computer virtuale è avvenuto correttamente.

Ripristino di SQL Filestream

La presente sezione descrive i seguenti argomenti:

Applicazione della patch T00002266

Questa sezione fornisce informazioni su come applicare la patch T00002266.

Prima di installare la patch *T00002266*, assicurarsi di disporre del file *SqlRestore.ini* in *C:\Programmi\Arcserve\Unified Data Protection\Engine\Configuration* per eseguire il ripristino.

Per installare la patch, procedere come segue:

1. Scaricare ed estrarre il file **T00002266.zip**.
2. Per eseguire l'installazione, fare clic sul file **T00002266.exe**.

Per aprire e modificare il file SqlRestore.ini, procedere come segue:

1. Sul computer di origine, accedere al percorso seguente:

   C:\Programmi\Arcserve\Unified Data Protection\Engine\Configuration
2. Aprire il file *SqlRestore.ini* in un editor di testo e includere le seguenti informazioni:

   RestoreInstanceName = {nome dell'istanza di destinazione di SQLServer}

   MDF-restore-folder = {posizione del file MDF}

   LDF-restore-folder = {posizione del file LDF}

   NDF-restore-folder = {posizione del file NDF}

   FILESTREAM-restore-folder = {posizione del file FileStreams}
3. In base alla posizione in cui si desidera ripristinare i database, modificare il contenuto incluso tra parentesi graffe con le posizioni delle cartelle.

   Ad esempio, sostituire:

   MDF-restore-folder = {posizione del file MDF}

   con

   MDF-restore-folder = C:\Rest\MDF1

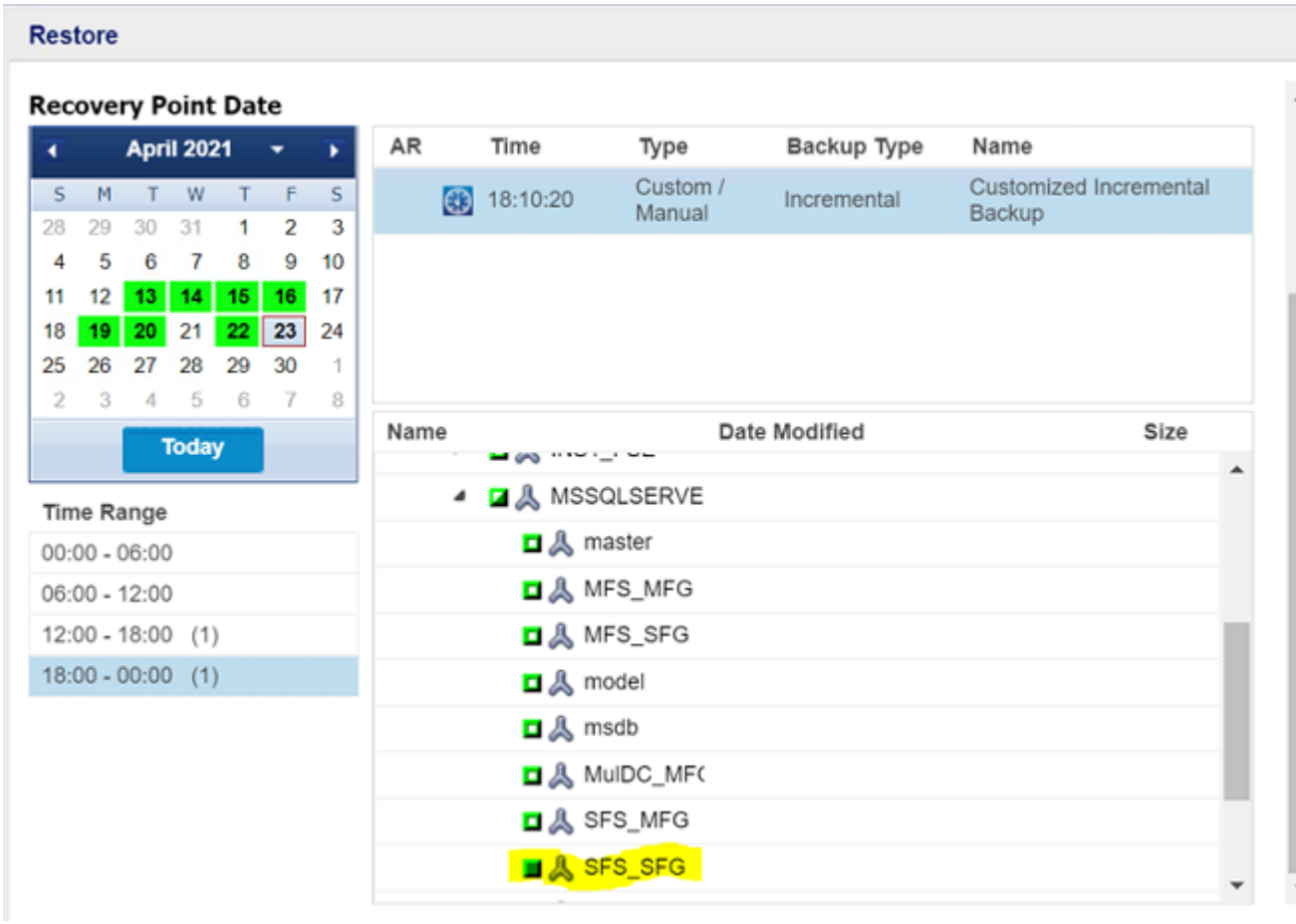
   Nota: il contenuto incluso tra parentesi graffe indica i segnaposto per il nome e le posizioni. Le parentesi non sono necessarie quando si utilizzano i dati effettivi.
4. Eseguire il ripristino per un database SQL in base alle proprie esigenze.

Ripristino del database SQL nella posizione originale

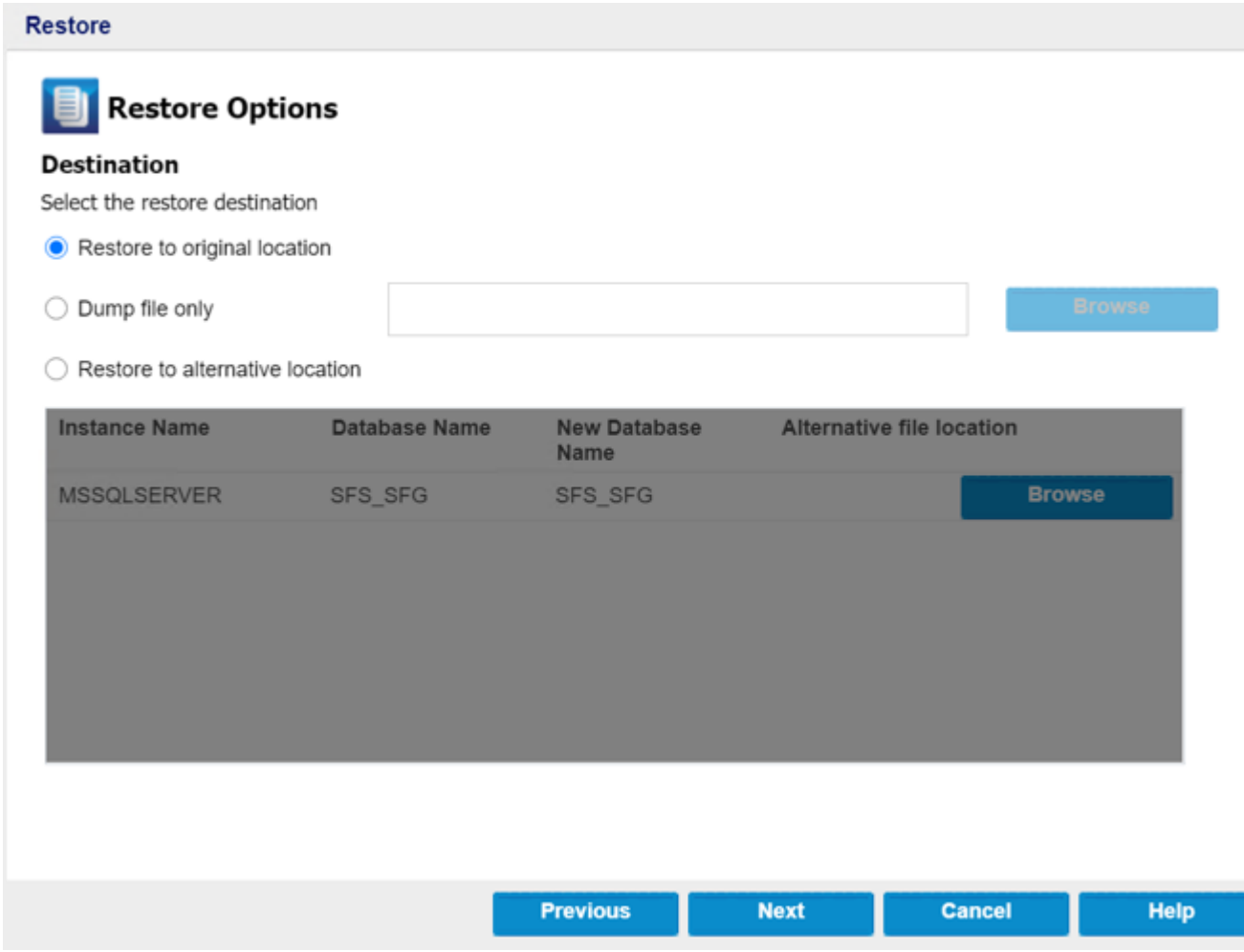
In questa sezione vengono fornite informazioni su come ripristinare il database SQL con Filestream abilitato in una posizione originale.

Effettuare le operazioni seguenti:

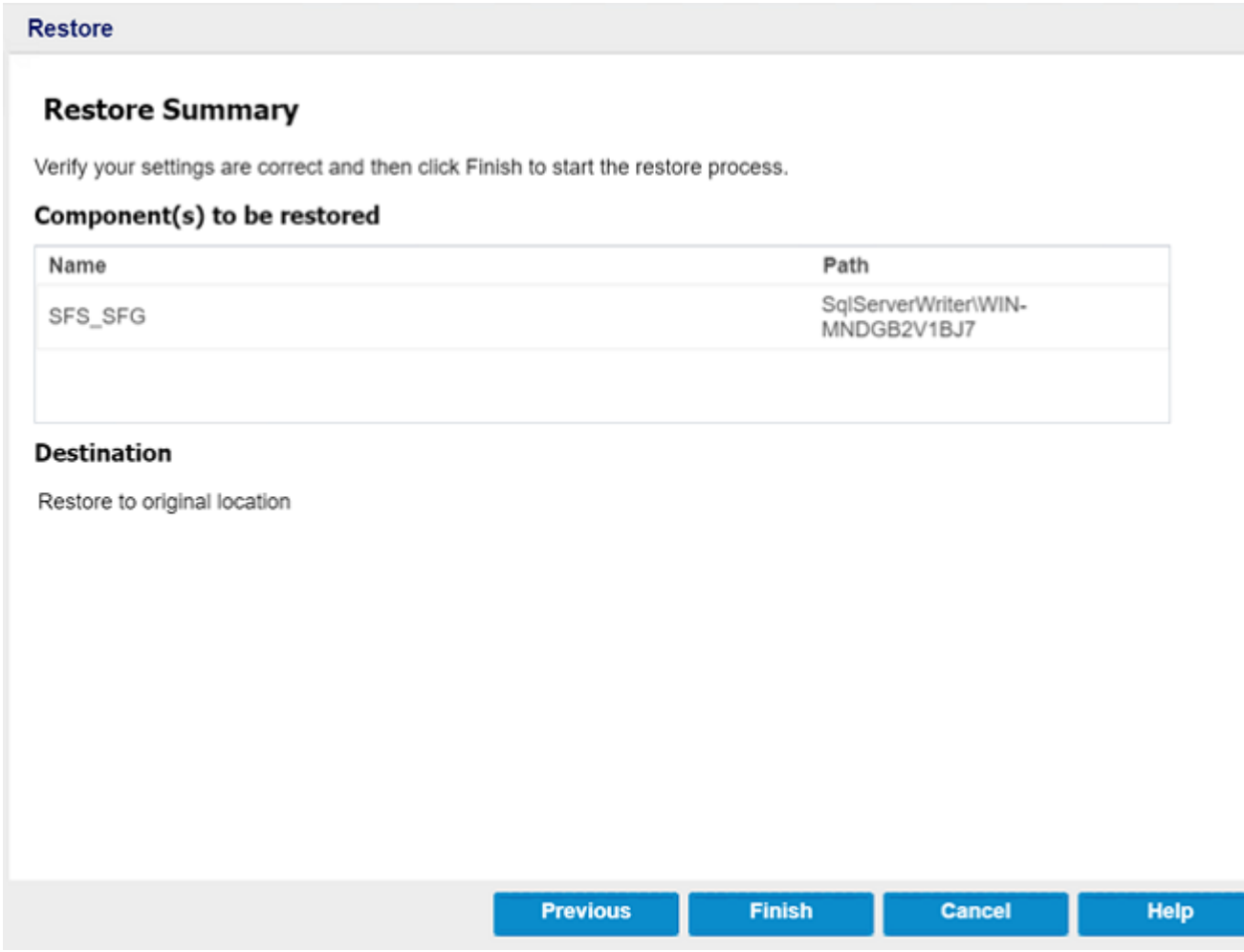
1. Dalla schermata Ripristino, selezionare la data del punto di ripristino, l'intervallo di tempo e il database SQL, quindi fare clic su **Avanti**.



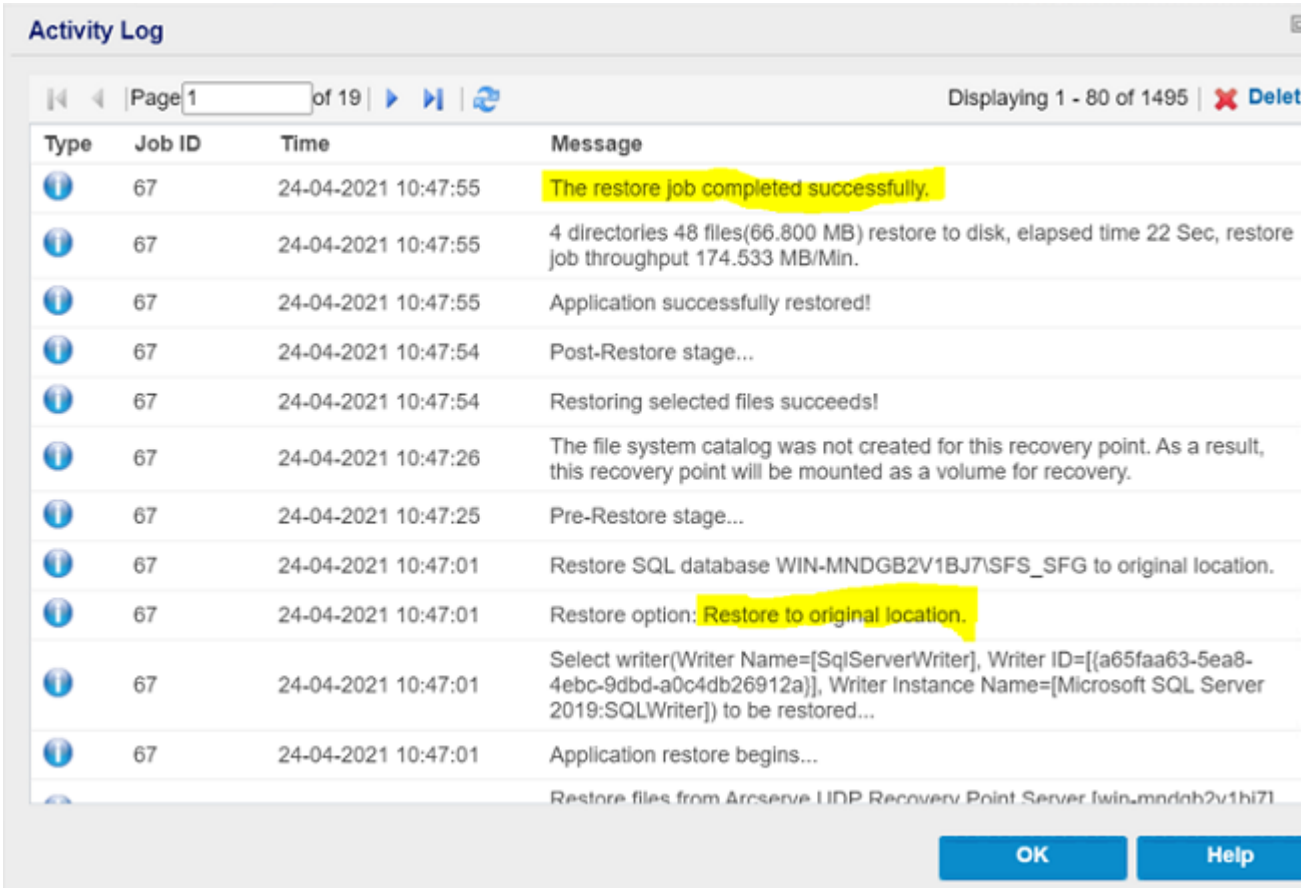
2. Dalla schermata Opzioni di ripristino, in Destinazione selezionare **Ripristina in posizione originale**, quindi fare clic sul pulsante **Sfoglia** per selezionare l'istanza.



3. Selezionare l'istanza, quindi fare clic su **Avanti**.
4. Verificare che le impostazioni siano corrette, quindi fare clic su **Fine** per avviare il processo di ripristino nella posizione originale.



Visualizzare i registri attività per verificare che lo stato del ripristino sia stato eseguito correttamente.



Ripristino del database SQL su un'istanza alternativa dello stesso server

In questa sezione vengono fornite informazioni su come ripristinare il database SQL con Filestream abilitato su un'istanza alternativa del database abilitato per File-stream in cui entrambe le istanze si trovano sullo stesso server SQL.

Effettuare le operazioni seguenti:

1. Per modificare il nome dell'istanza, aprire il file **SqlRestore.ini**, quindi modificare il file **RestoreInstanceName**.

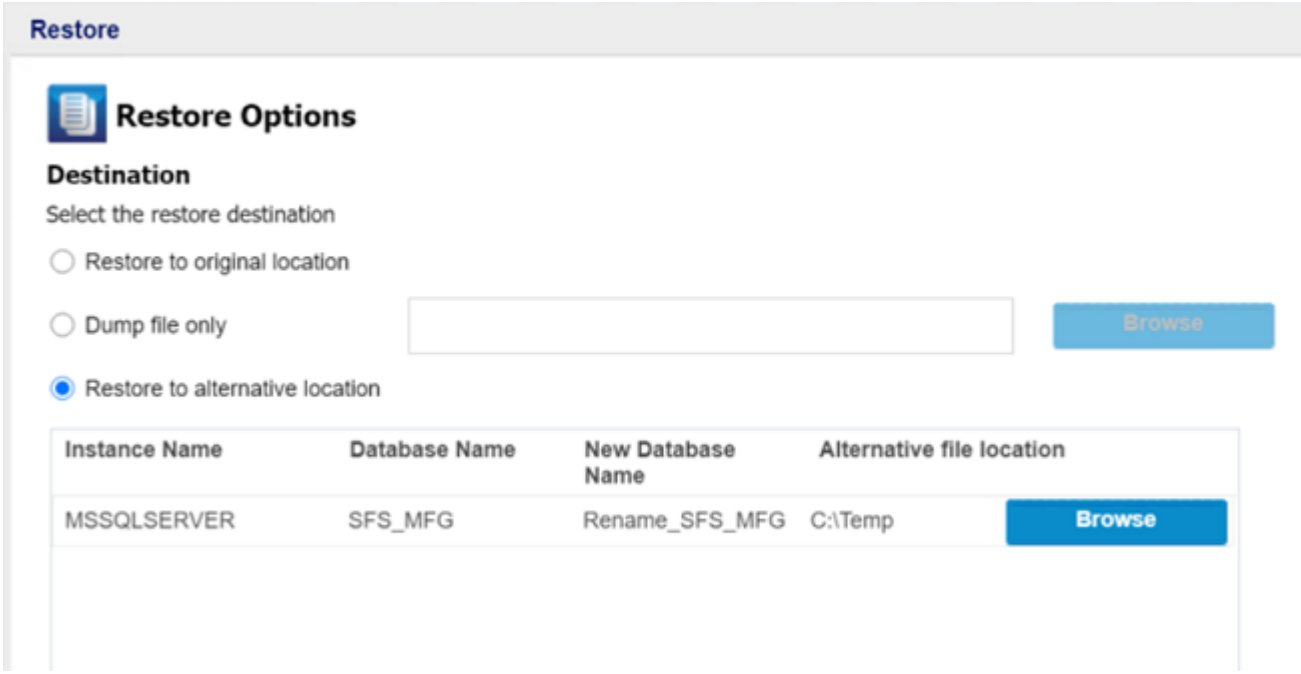
   Ad esempio, modificare il nome dell'istanza da *WIN-MNDGB2V1BJ7\MSSQLSERVER* a *WIN-MNDGB2V1BJ7\INS1_FSE*.

   Nota: WIN-MNDGB2V1BJ7 indica il server SQL.



Nota: è possibile specificare il campo *RestoreInstanceName* anche senza SQL Server. Ad esempio, *RestoreInstanceName = INS1_FSE*.

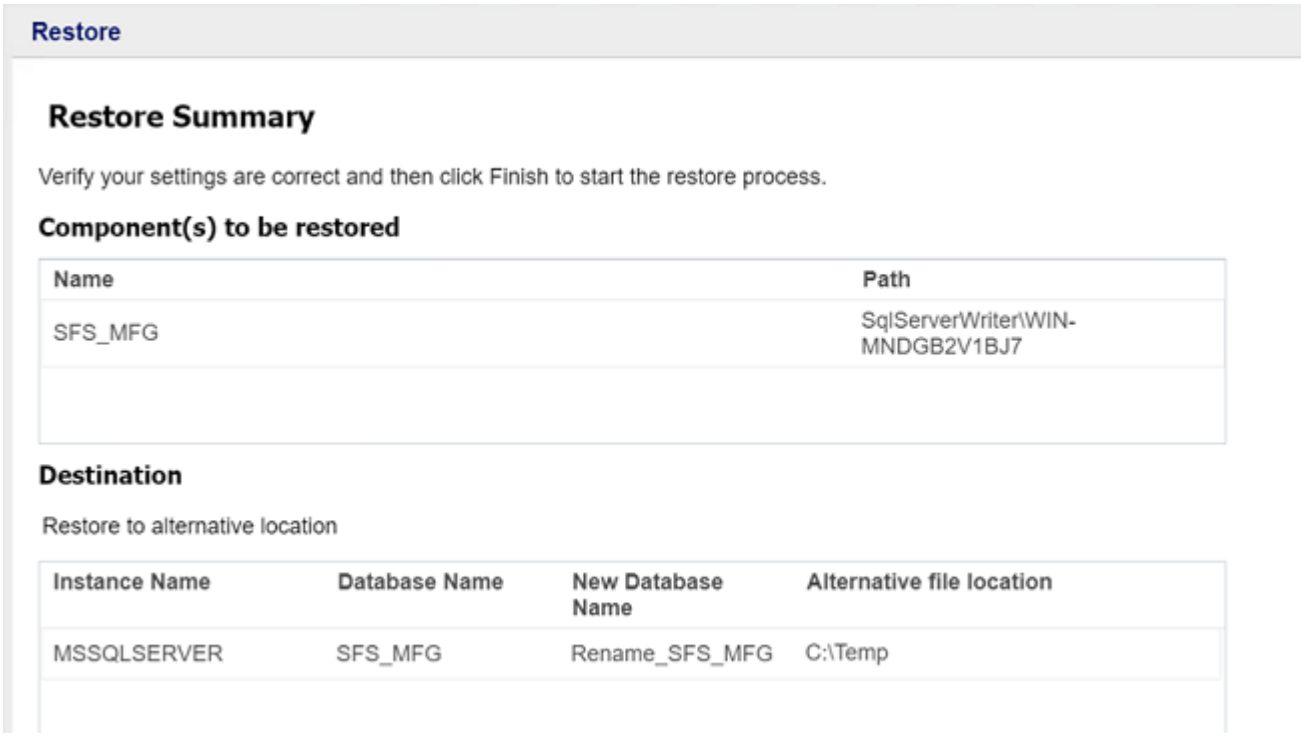
2. Nell'agente, nella pagina Ripristino, selezionare il database che si desidera ripristinare, quindi fare clic su **Avanti**.
3. Nella schermata Opzioni di ripristino, selezionare **Ripristina in posizione alternativa** e ricercare l'istanza.



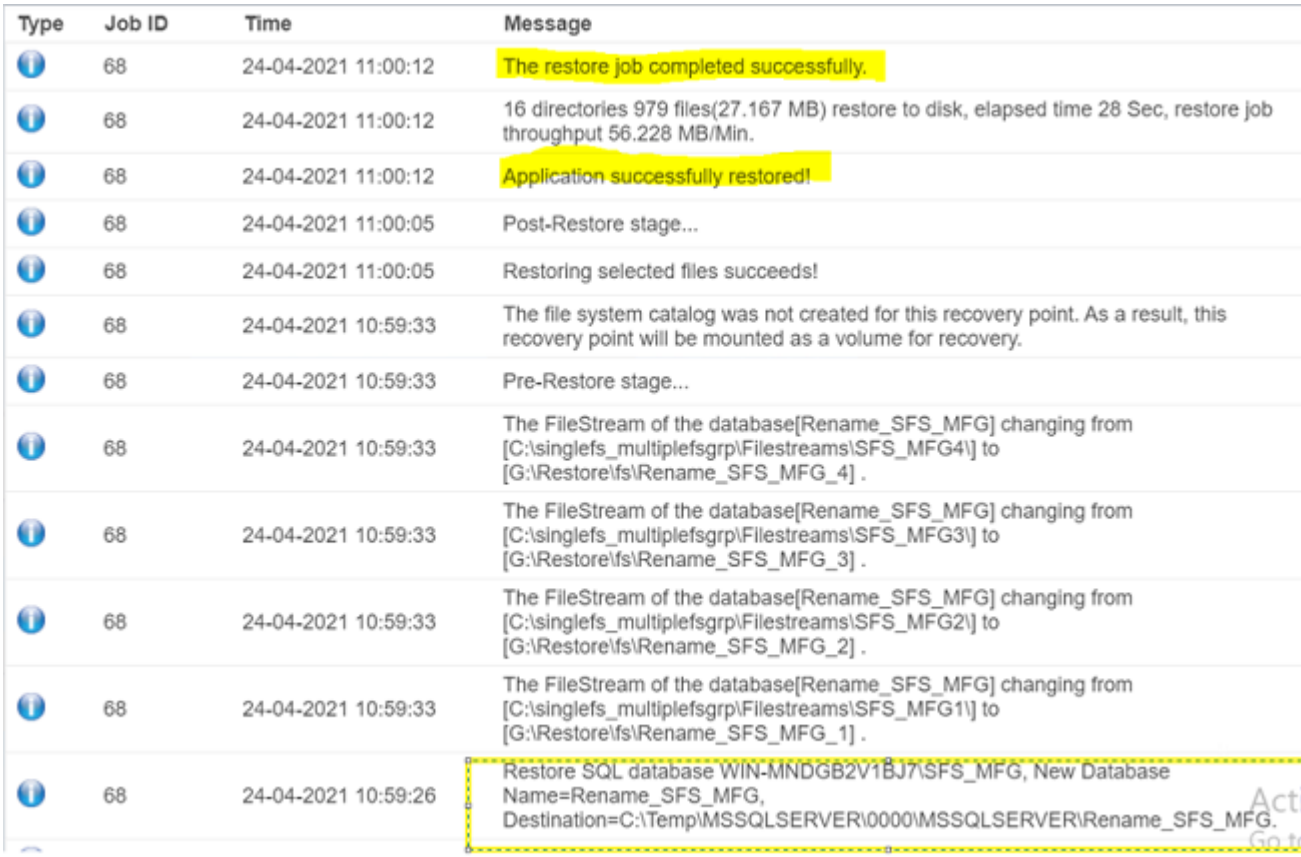
Per rinominare il nome del database, fare clic sull'area di testo **Nuovo nome database** e digitare il nuovo nome. Ad esempio, *SFS_MFG* viene rinominato *Rename_SFS_MFG*.

Nota: in Posizione file alternativa è selezionata una cartella temporanea. Questa posizione consente di elaborare il ripristino dei file nella posizione definita nel file SqlRestore.ini.

4. Verificare che le impostazioni siano corrette, quindi fare clic su **Fine** per avviare il processo di ripristino.

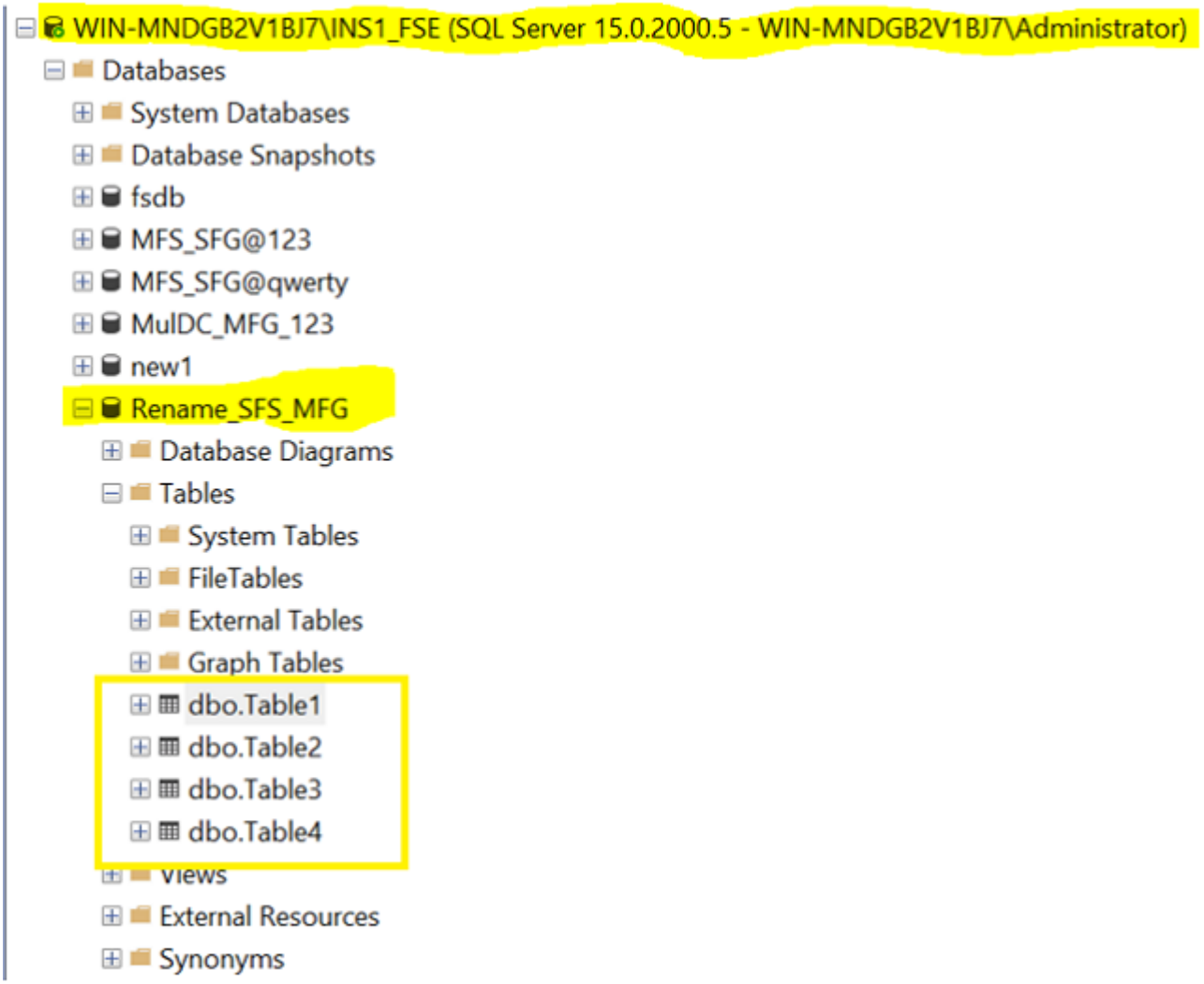


Il registro attività visualizza lo stato del ripristino insieme alla ride-nominazione del database.

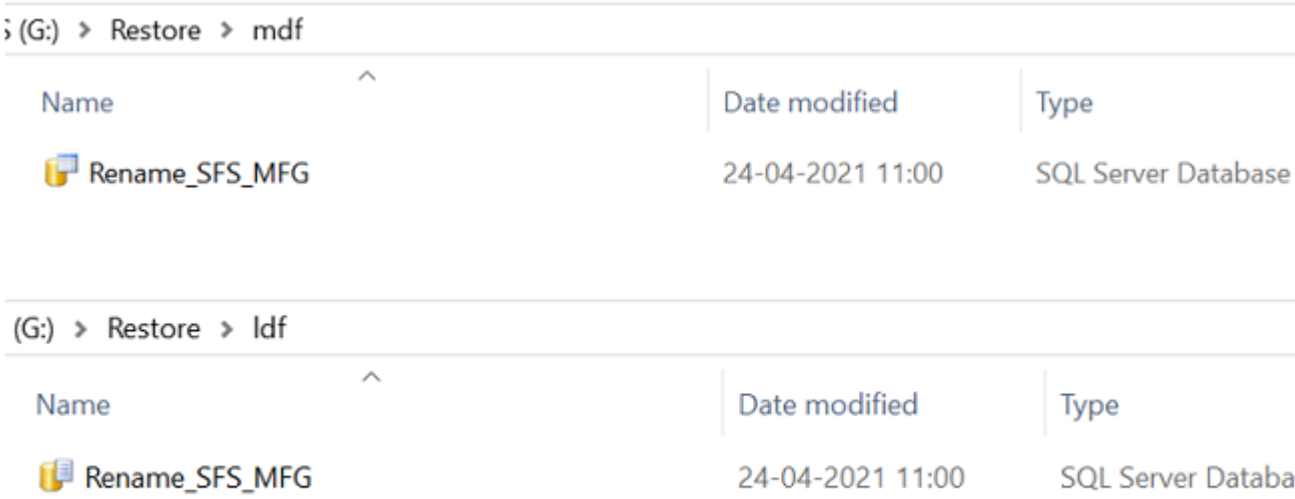


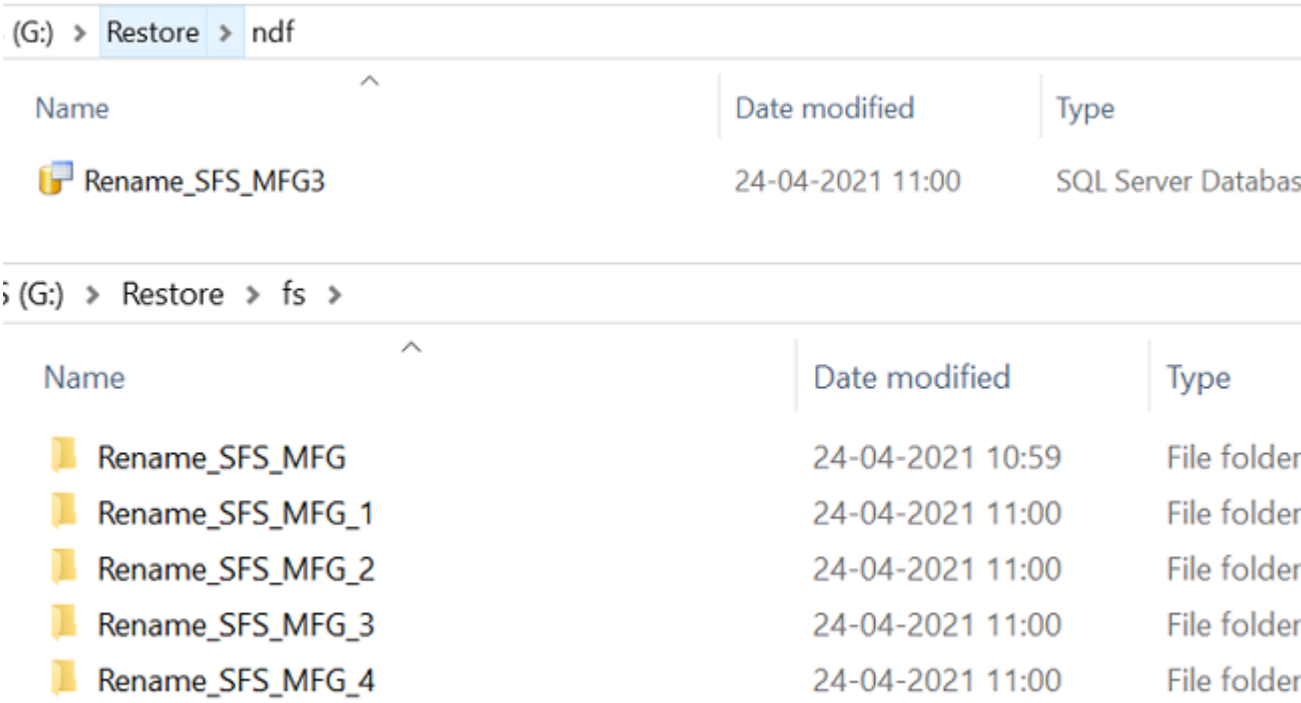
Type	Job ID	Time	Message
	68	24-04-2021 11:00:12	The restore job completed successfully.
	68	24-04-2021 11:00:12	16 directories 979 files(27.167 MB) restore to disk, elapsed time 28 Sec, restore job throughput 56.228 MB/Min.
	68	24-04-2021 11:00:12	Application successfully restored!
	68	24-04-2021 11:00:05	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.

Le modifiche apportate al nome dell'istanza e del database vengono applicate anche a SQL Management Studio.



In base a quanto definito nel file SqlRestore.ini, i file LDF, MDF e Filestream sono archiviati nelle rispettive cartelle.



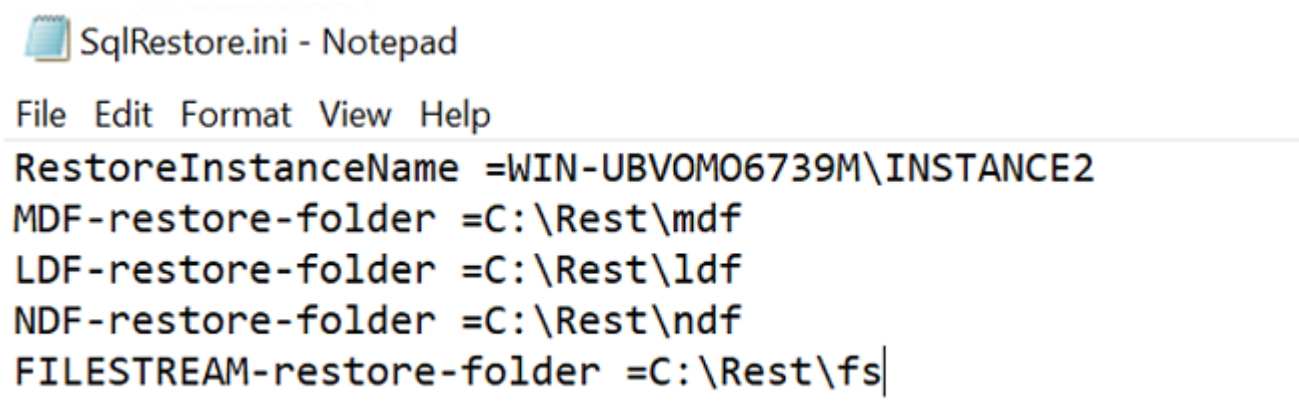


Ripristino del database SQL su un'istanza alternativa di un server diverso

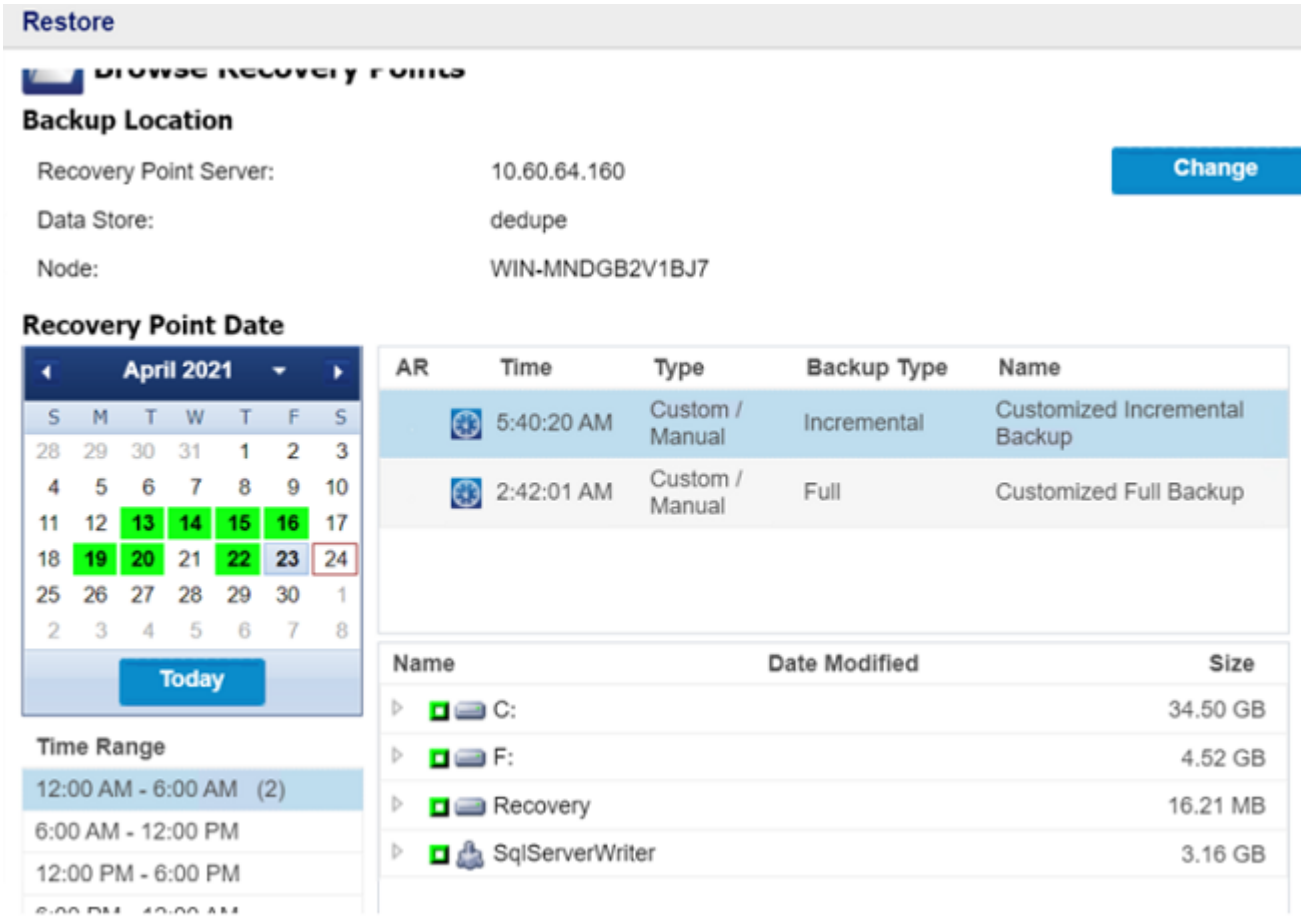
In questa sezione vengono fornite informazioni su come ripristinare il database SQL con Filestream abilitato su un'istanza alternativa del database abilitato per Filestream in cui entrambe le istanze si trovano su un server SQL diverso. Ad esempio, se il database si trova nel server di origine WIN-MNDGB2V1BJ7 e nell'istanza di origine MSSQLSERVER, è possibile ripristinarlo sul server di destinazione WIN-UBVOMO6739M e sull'istanza di destinazione INSTANCE2.

Effettuare le operazioni seguenti:

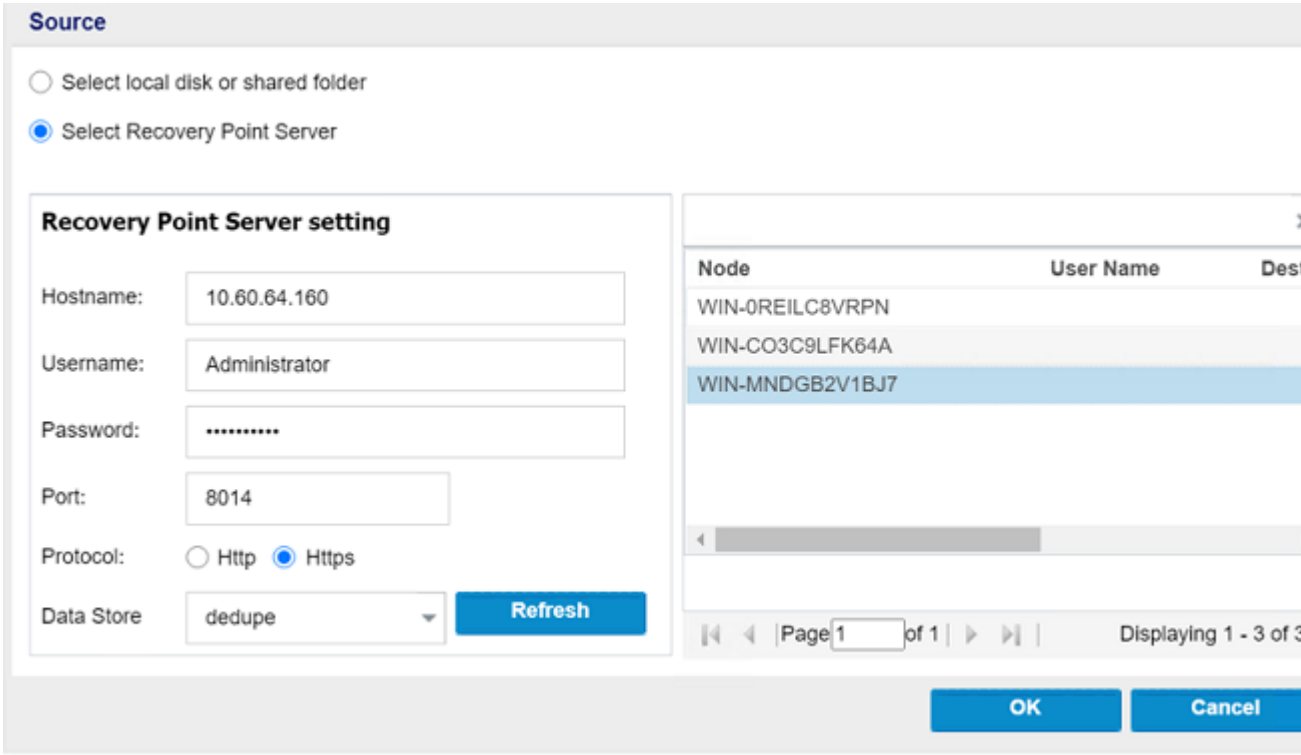
1. Per ripristinare il database sul server alternativo (WIN-UBVOMO6739M) e sull'istanza (INSTANCE2), modificare il file SqlRestore.ini.



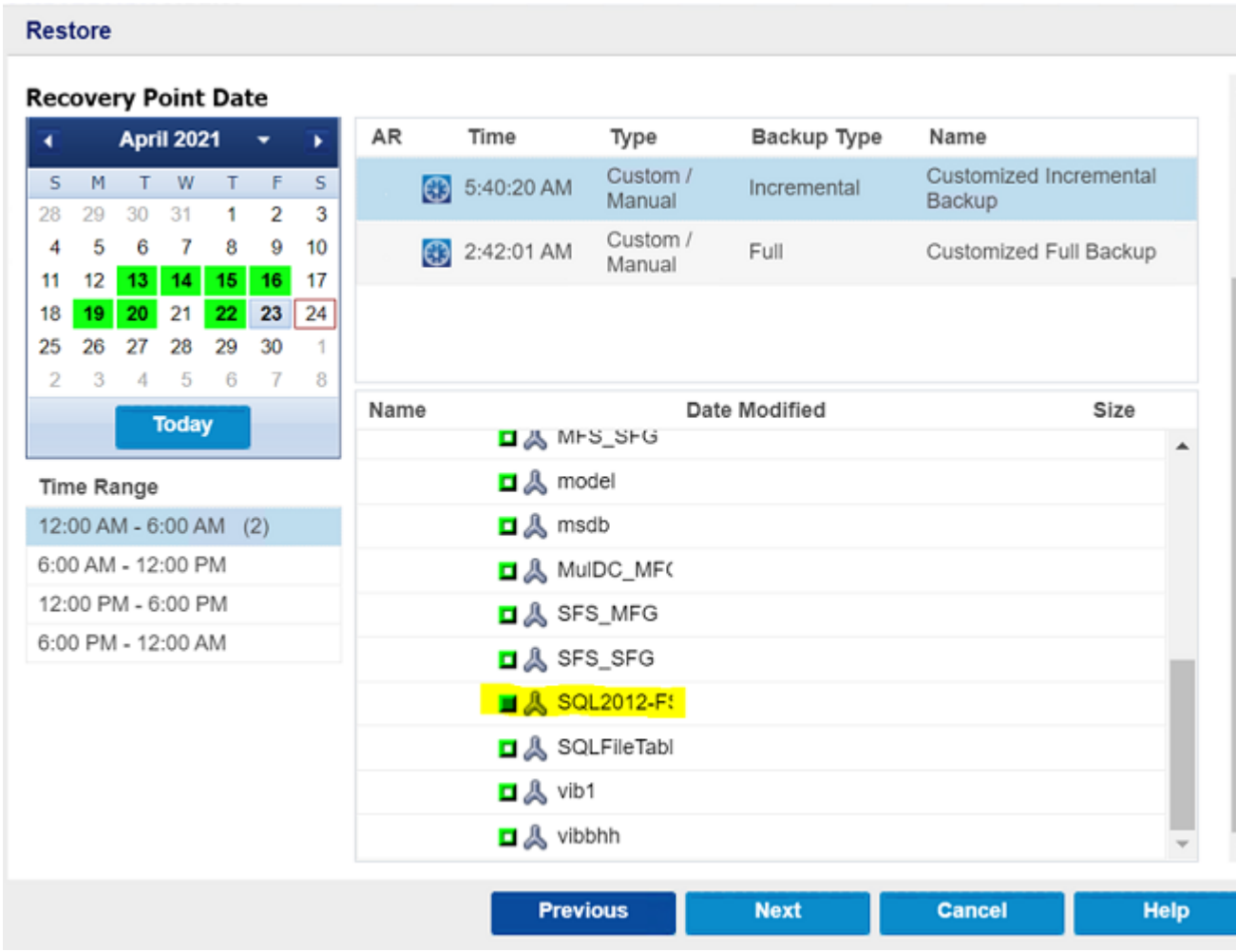
2. Per modificare la posizione del Recovery Point Server (RPS) per il ripristino dei server e delle istanze su un server alternativo, fare clic sul pulsante **Modifica**, quindi fornire i dettagli del nuovo server RPS.



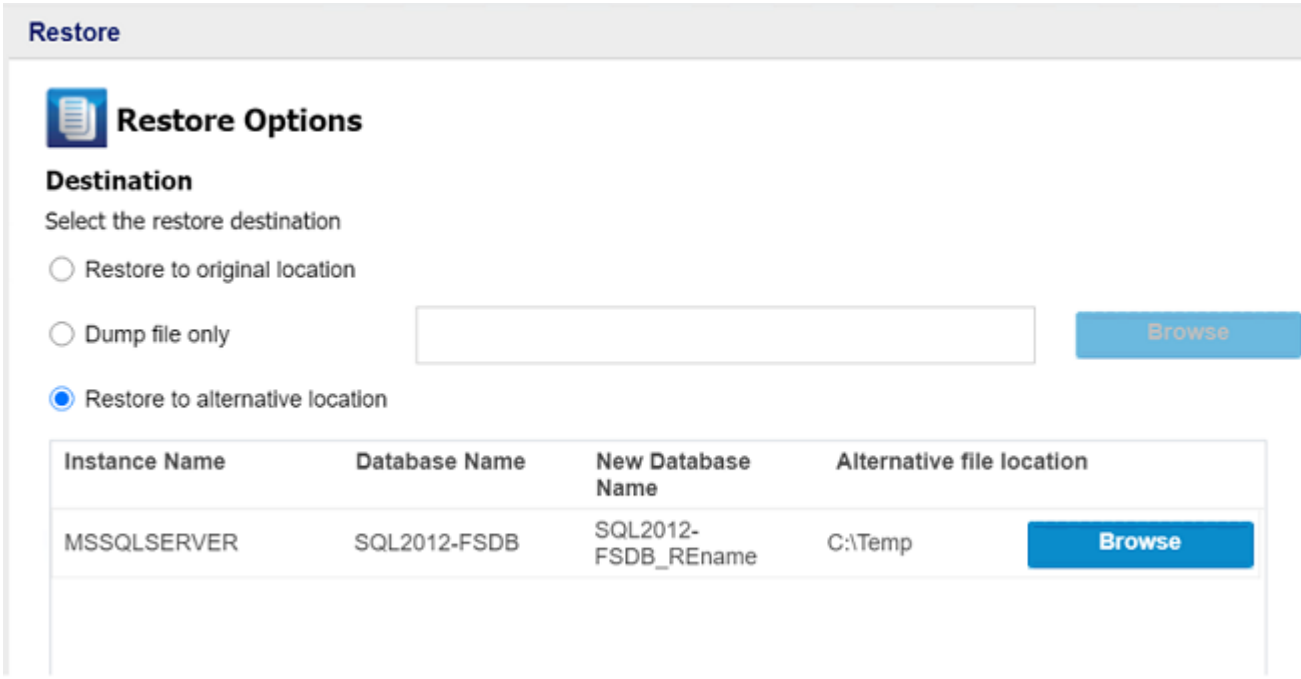
3. Per selezionare il server RPS di origine, fare clic su **Seleziona server del punto di ripristino**, selezionare il server di origine (WIN-MNDGB2V1BJ7), quindi fare clic su **OK**.



4. Per eseguire il ripristino su un server alternativo, selezionare il database (SQL2012-FSDB), quindi fare clic su **Avanti**.



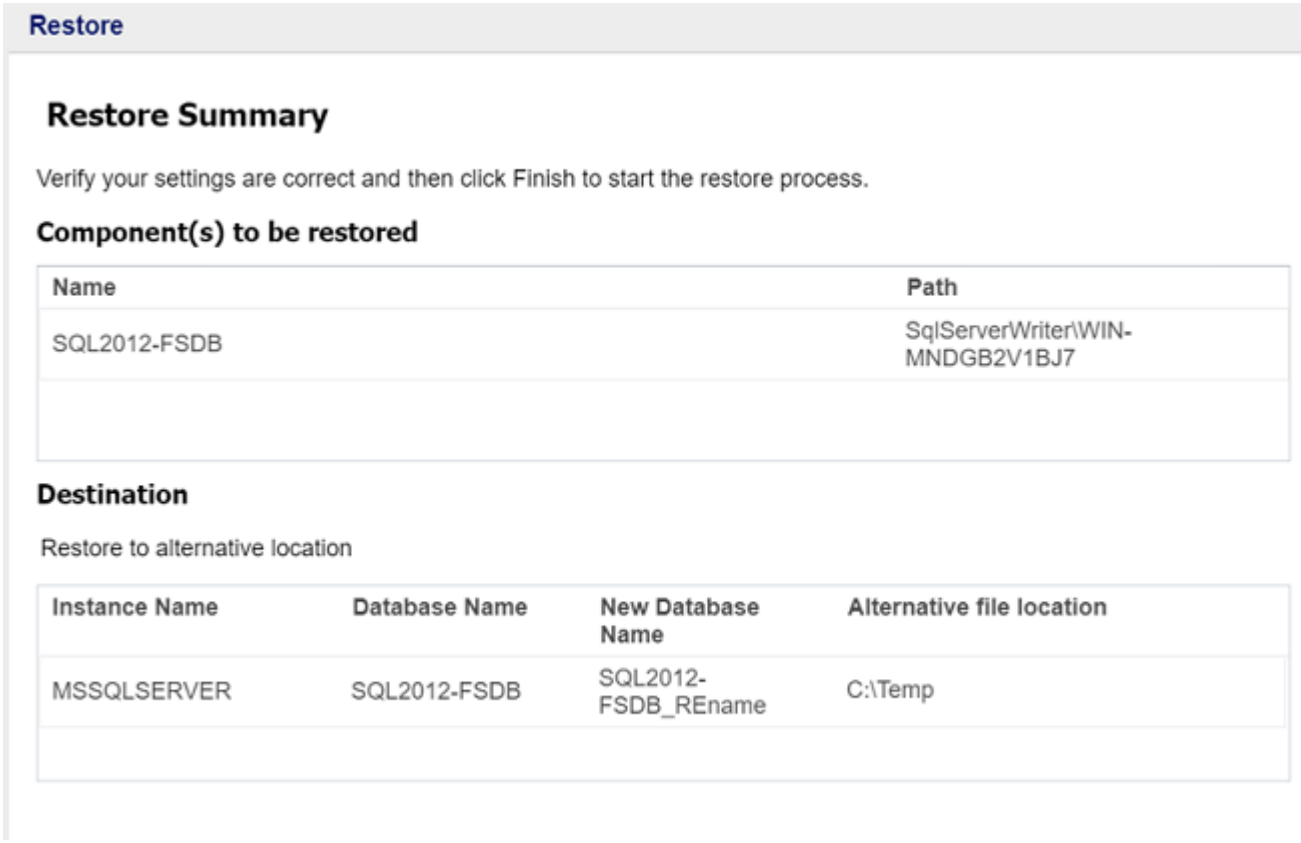
5. Nella schermata Opzioni di ripristino, selezionare **Ripristina in posizione alternativa** e ricercare l'istanza.



Per rinominare il nome del database, fare clic sull'area di testo **Nuovo nome database** e digitare il nuovo nome. Ad esempio, SQL2012-FSDB viene rinominato SQL2012-FSDB-REname.

Nota: in Posizione file alternativa è selezionata una cartella temporanea. Questa posizione consente di elaborare il ripristino dei file nella posizione definita nel file SqlRestore.ini.

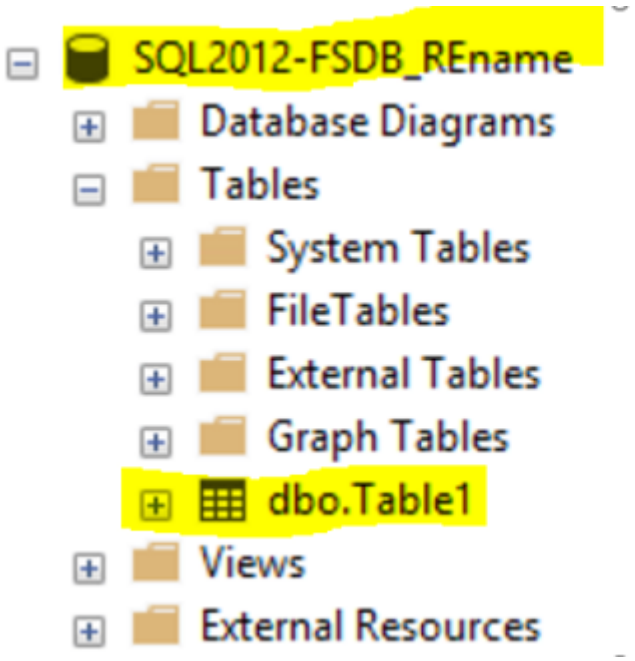
6. Verificare che le impostazioni siano corrette, quindi fare clic su **Fine** per avviare il processo di ripristino.



Il registro attività visualizza lo stato del ripristino insieme alla ride-nominazione del database.

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.

La modifica del nome del database viene riprodotta in SQL Management Studio.



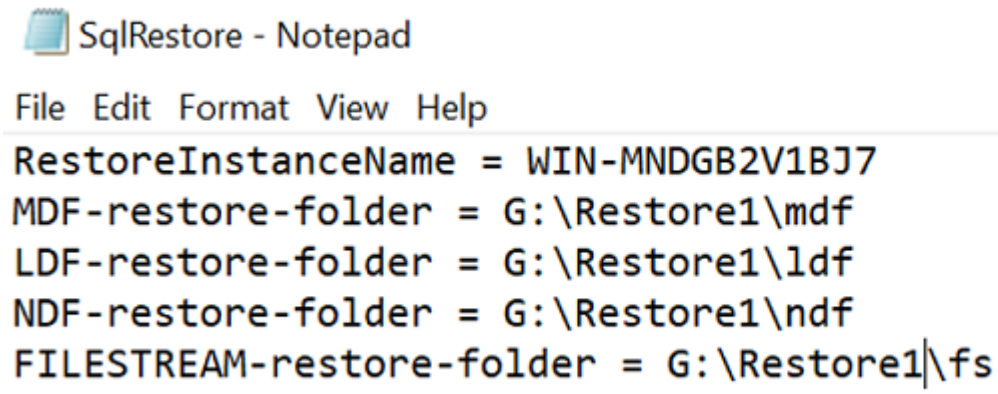
Ripristino del database SQL in una posizione alternativa della stessa istanza

In questa sezione vengono fornite informazioni su come ripristinare il database SQL con il flusso di file attivato in una posizione alternativa ma sulla stessa istanza durante la ridenominazione del database.

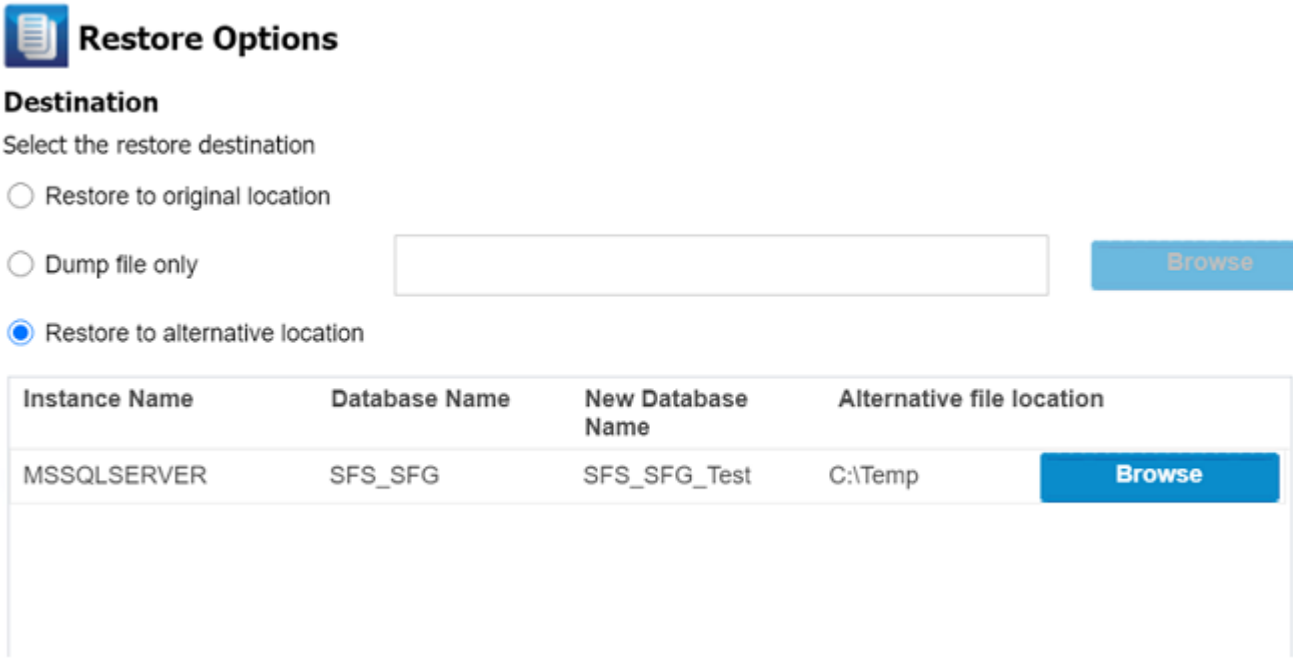
Effettuare le operazioni seguenti:

1. Per modificare il database di ripristino in una posizione alternativa, aprire il file SqlRestore.ini, quindi modificare le posizioni della cartella in base alle proprie esigenze.

   Ad esempio, modificare le posizioni della cartella da *C:\singlefs_singlefsgrp\SFS_SFG1* a *G:\Restore1\fs1*.



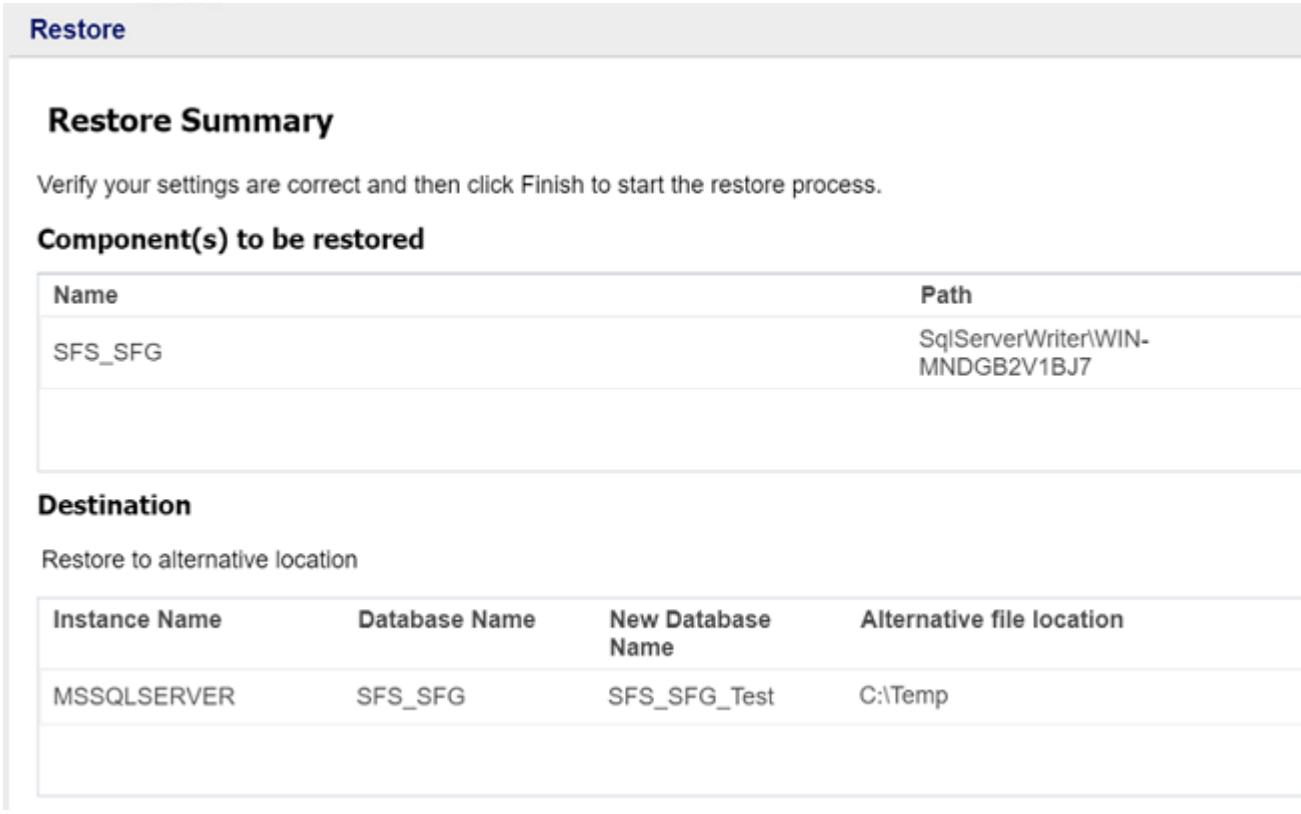
2. Nell'agente, nella pagina Ripristino, selezionare il database che si desidera ripristinare, quindi fare clic su **Avanti**.
3. Nella schermata Opzioni di ripristino, selezionare **Ripristina in posizione alternativa** e ricercare l'istanza.



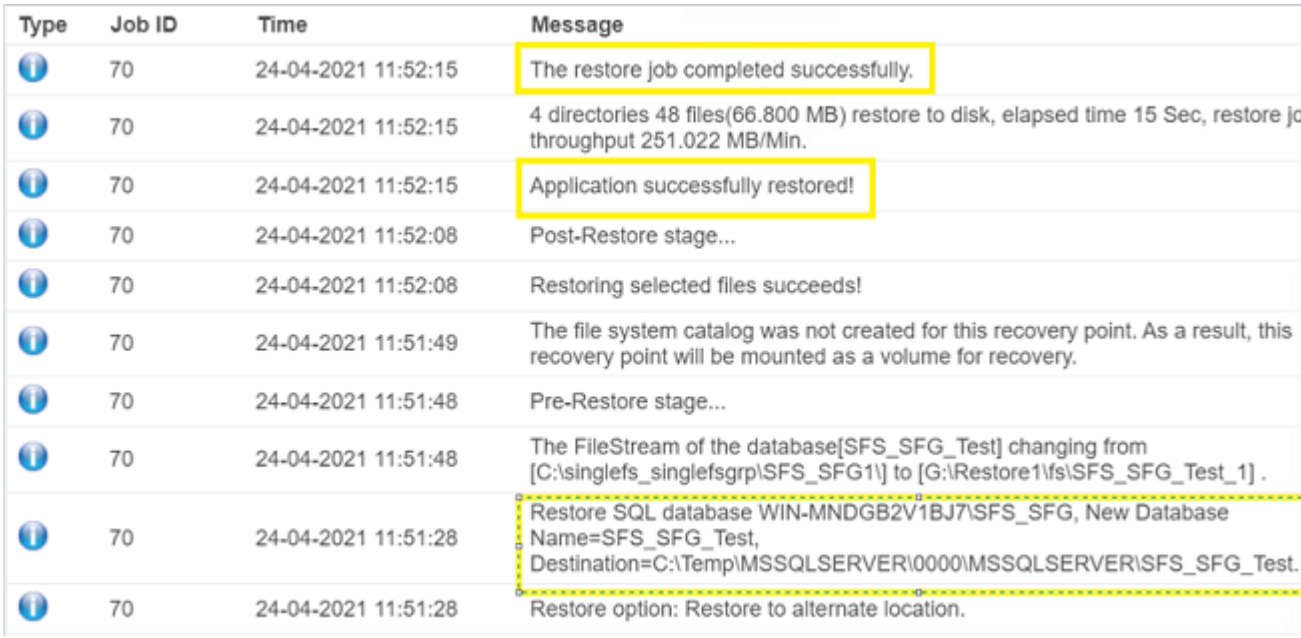
Per rinominare il nome del database, fare clic sull'area di testo **Nuovo nome database** e digitare il nuovo nome. Ad esempio, *SFS_SFG* viene rinominato *SFS_SFG_Test*.

Nota: in Posizione file alternativa è selezionata una cartella temporanea. Questa posizione consente di elaborare il ripristino dei file nella posizione definita nel file SqlRestore.ini.

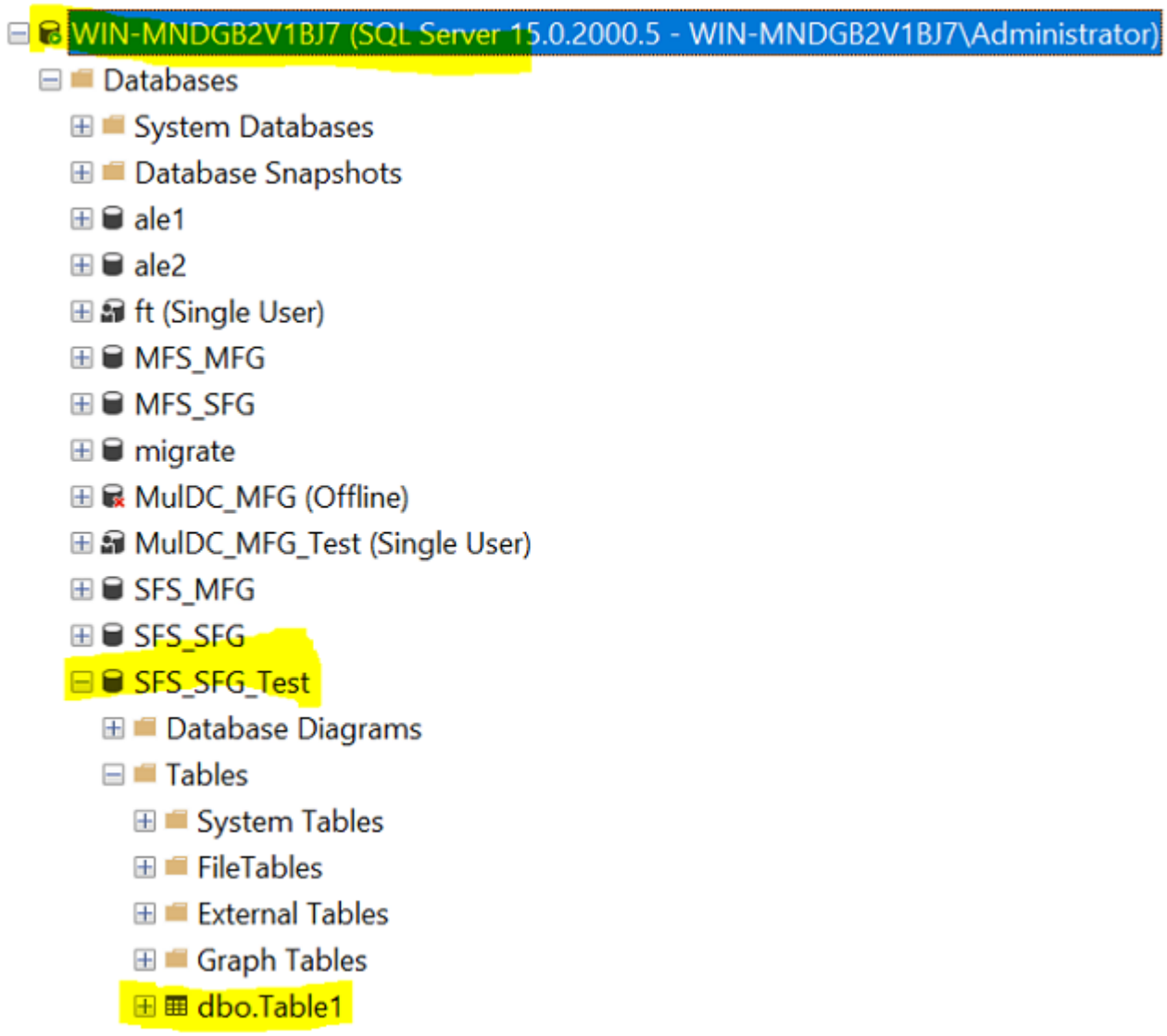
4. Verificare che le impostazioni siano corrette, quindi fare clic su **Fine** per avviare il processo di ripristino.



Il registro attività visualizza lo stato del ripristino insieme alla ride-nominazione del database.



La modifica del nome del database viene riprodotta in SQL Management Studio.

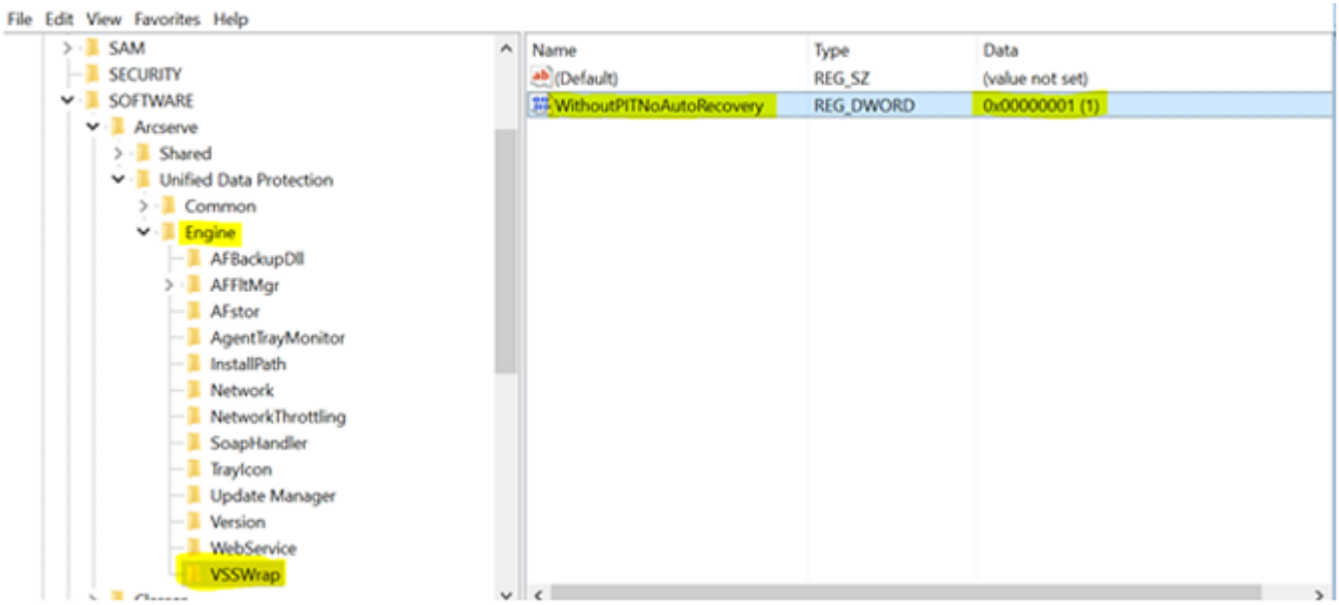


Modalità di ripristino tramite chiave di registro

In questa sezione vengono fornite informazioni su come utilizzare la modalità di ripristino mediante la chiave di registro. Questo metodo consente di ripristinare il database abilitato per Filestream nell'istanza alternativa (INS1_FSE).

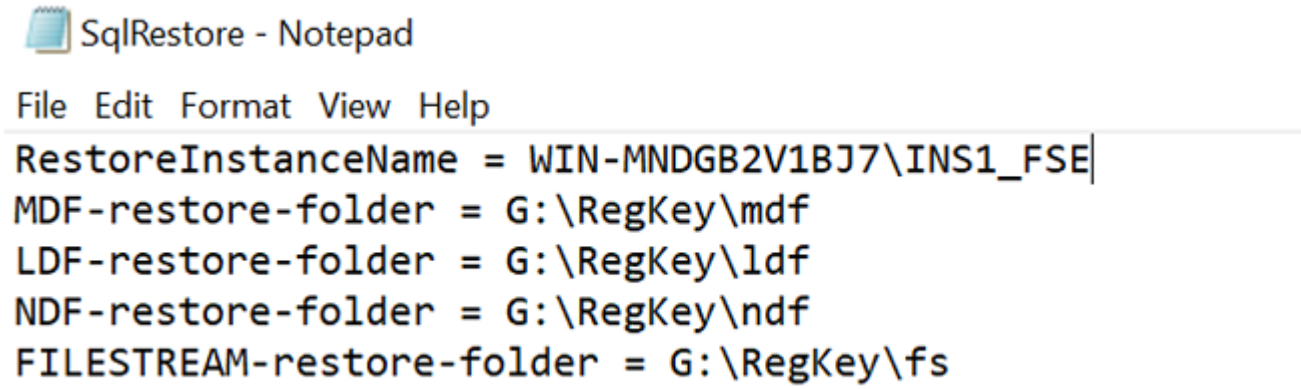
Una volta completato il backup, aggiungere la chiave di registro nella cartella VSSWrap con il valore DWORD a 32 bit: *WithoutPITNoAutoRecovery* e impostare il valore su 1.

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\VSSWrap\

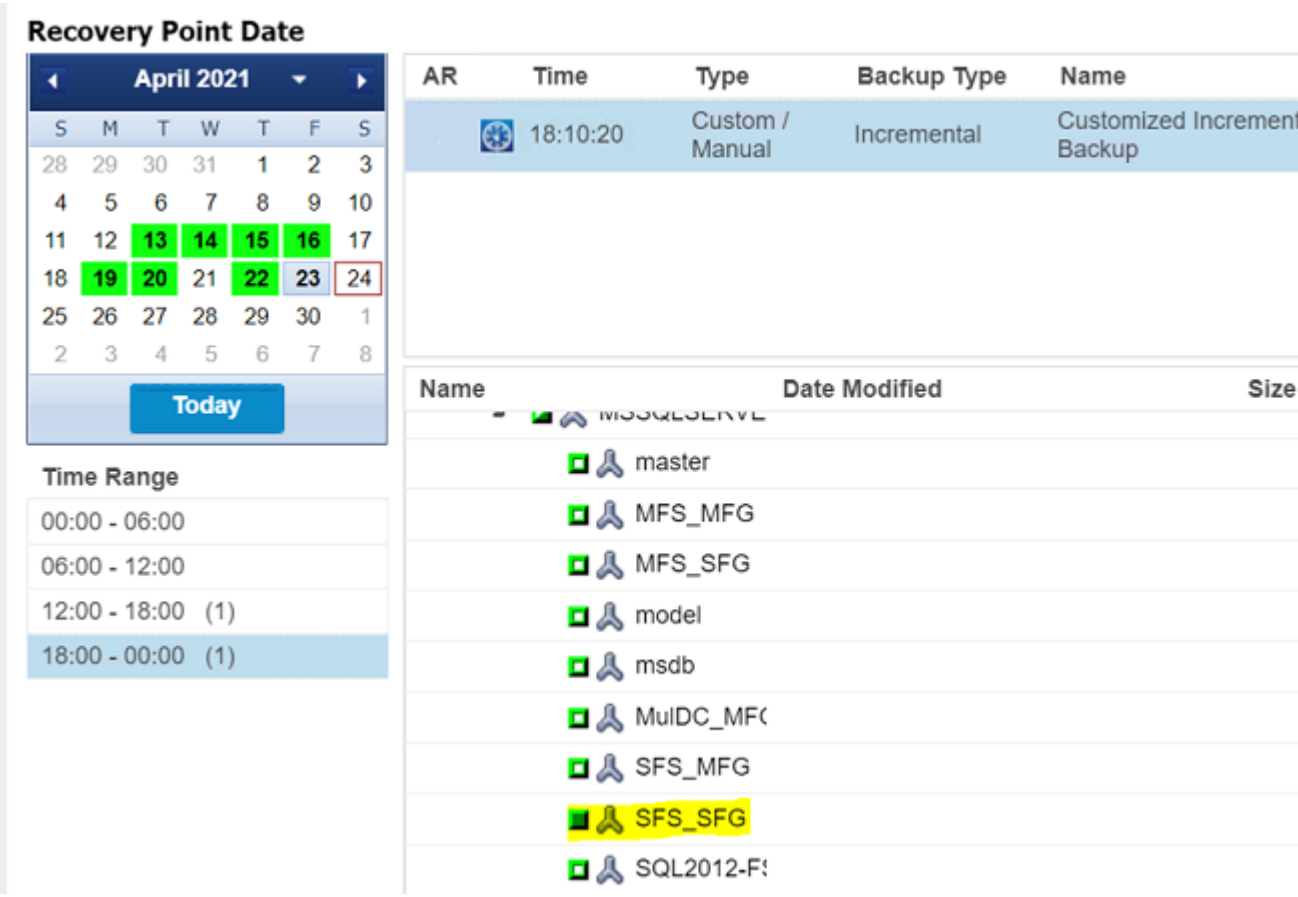


Effettuare le operazioni seguenti:

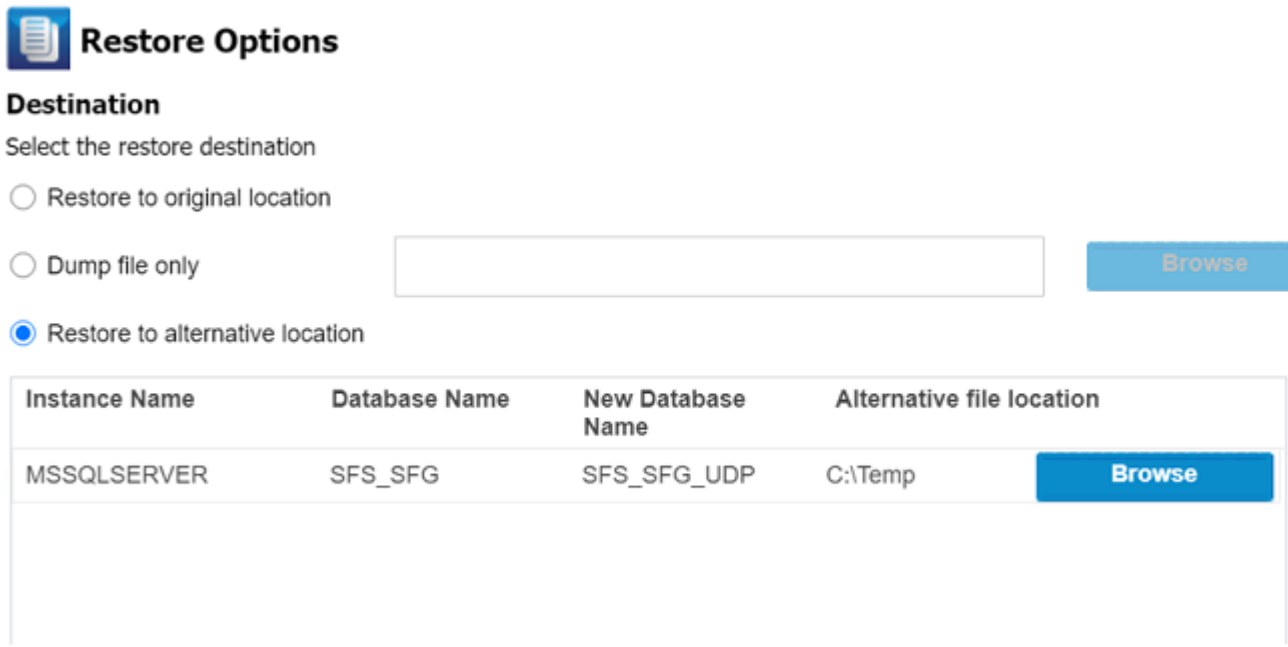
1. Per ripristinare il database in un'istanza alternativa, aprire il file SqlRestore.ini e modificare le posizioni della cartella in base alle proprie esigenze.



2. Nell'agente, nella pagina Ripristino, selezionare il database che si desidera ripristinare, quindi fare clic su **Avanti**.



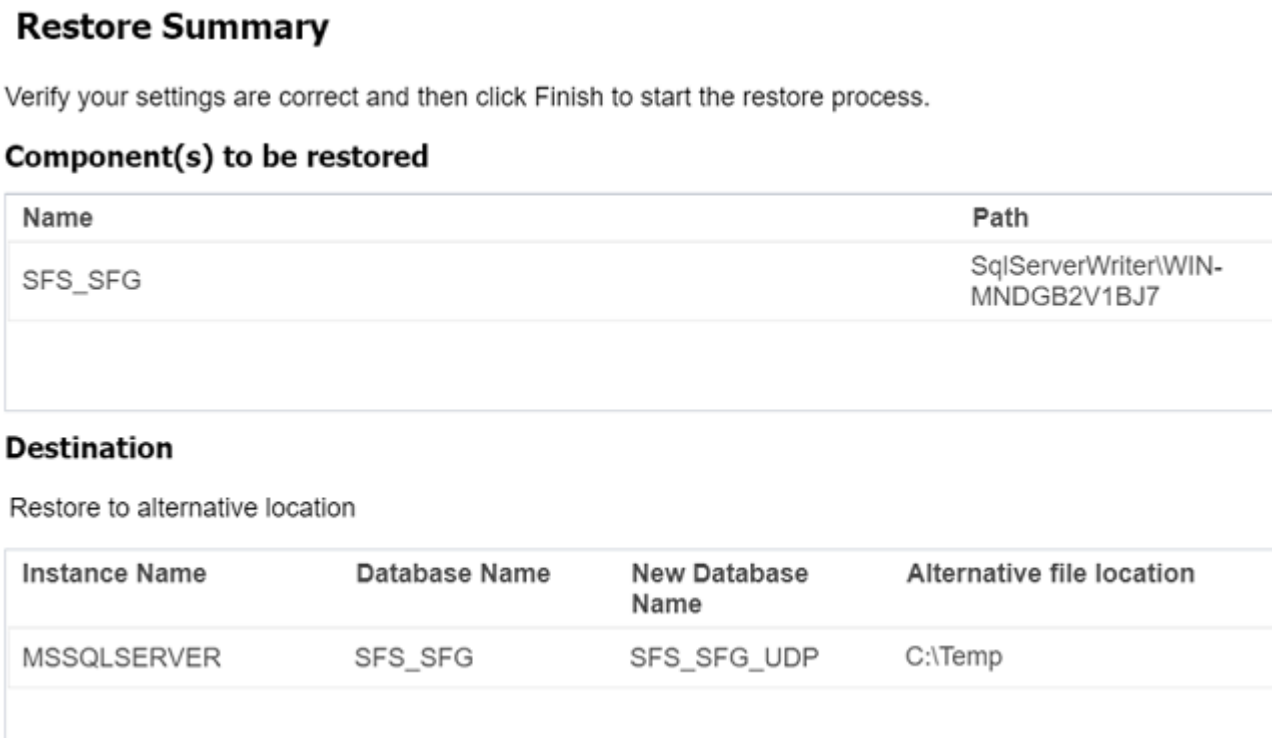
3. Nella schermata Opzioni di ripristino, selezionare **Ripristina in posizione alternativa** e ricercare l'istanza.



Per rinominare il nome del database, fare clic sull'area di testo **Nuovo nome database** e digitare il nuovo nome. Ad esempio, *SFS_SFG* viene rinominato *SFS_SFG_UDP*.

Nota: in Posizione file alternativa è selezionata una cartella temporanea. Questa posizione consente di elaborare il ripristino dei file nella posizione definita nel file SqlRestore.ini.

4. Verificare che le impostazioni siano corrette, quindi fare clic su **Fine** per avviare il processo di ripristino.



Restore Summary

Verify your settings are correct and then click Finish to start the restore process.

Component(s) to be restored

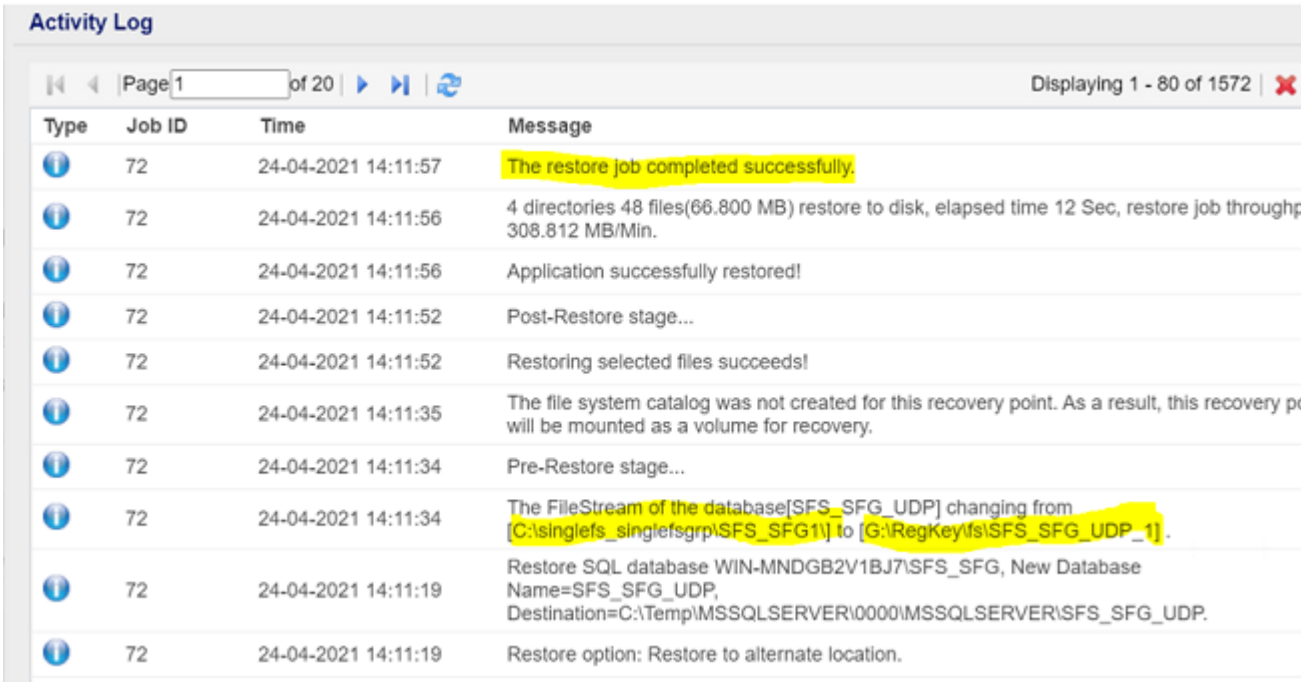
Name	Path
SFS_SFG	SqlServerWriter\WIN-MNDGB2V1BJ7

Destination

Restore to alternative location

Instance Name	Database Name	New Database Name	Alternative file location
MSSQLSERVER	SFS_SFG	SFS_SFG_UDP	C:\Temp

Il registro attività visualizza lo stato del ripristino insieme alla ride-nominazione del database.



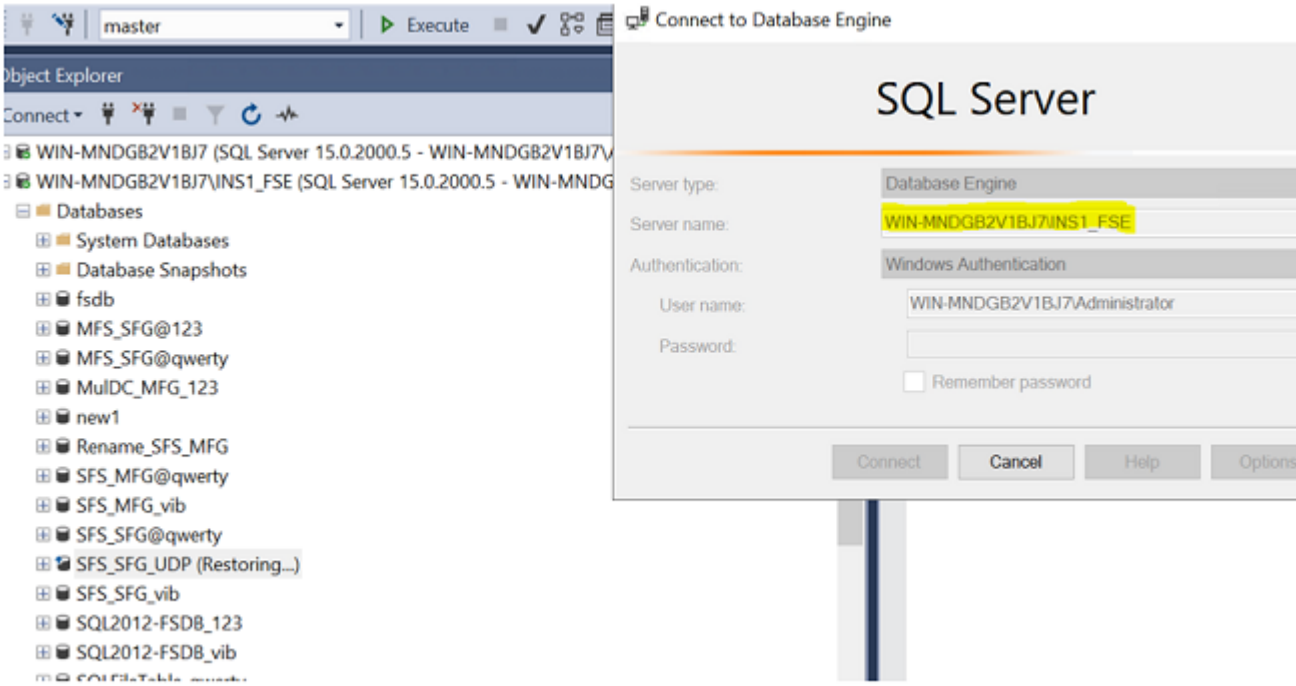
In alcuni casi, il database viene comunque visualizzato come in fase di ripristino anche dopo il completamento del processo.



Per rimuovere il database dalla modalità di ripristino, procedere come segue:

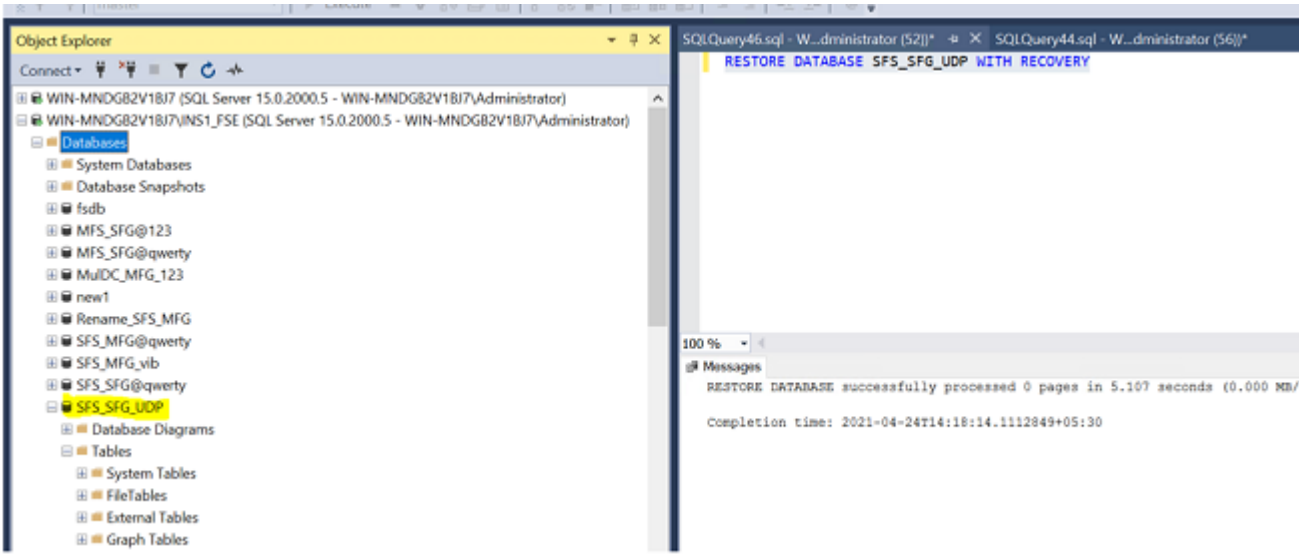
1. Fare clic con il pulsante destro del mouse sul database, quindi selezionare **Nuova query**.

   La finestra viene visualizzata e si connette all'istanza ripristinata.



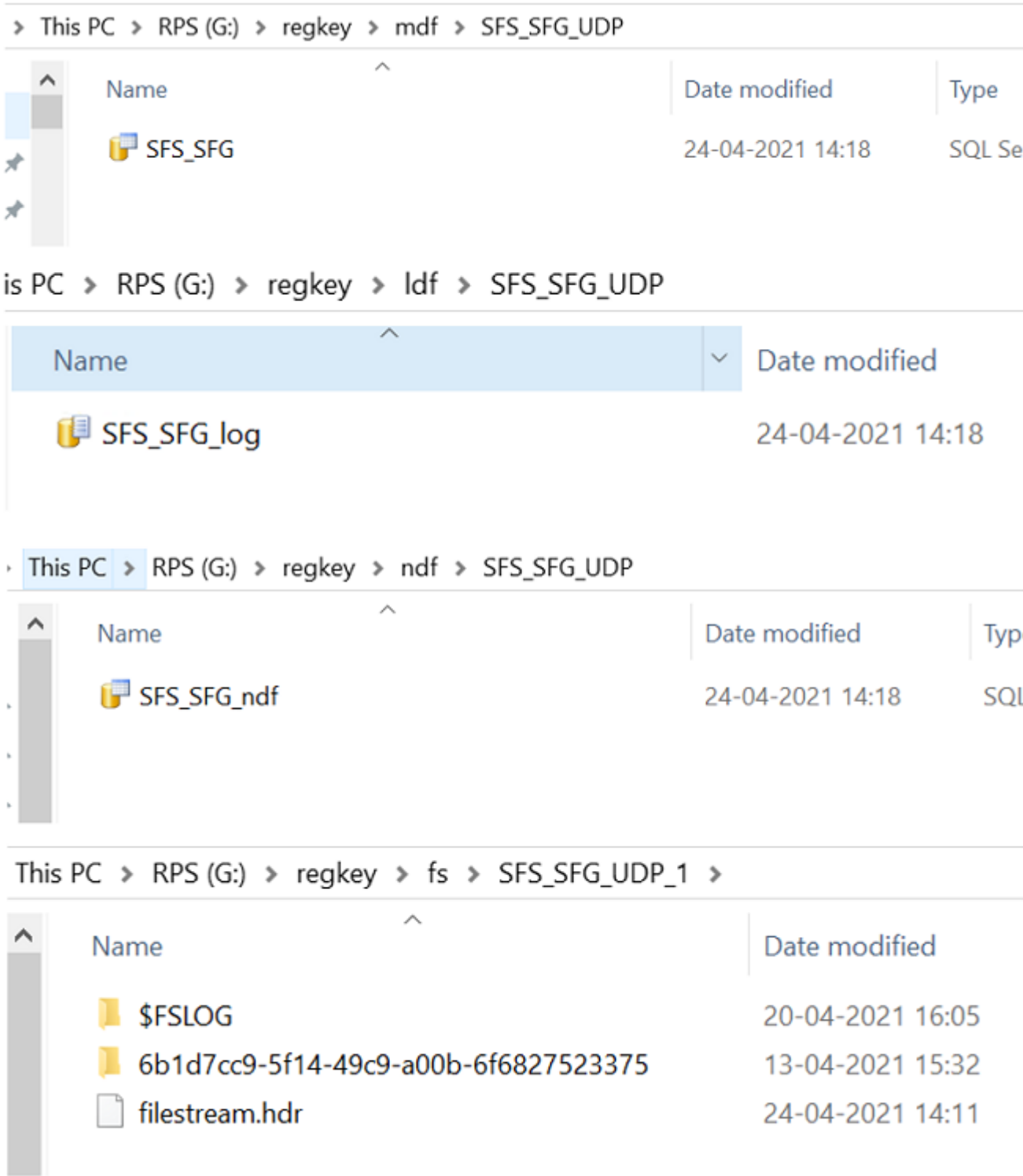
2. Nella finestra della query, eseguire la seguente query.

   RESTORE DATABASE [DATABASE NAME] WITH RECOVERY



   La modalità di ripristino viene rimossa dal database.

   Nota: se la ridenominazione di un file di database non viene eseguita correttamente durante l'utilizzo del Registro di sistema, la cartella principale visualizza il nuovo nome. Tuttavia, i file di database come MDF, NDF e LDF visualizzano il nome del database originale.


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

Uso dell'utilità Exchange Granular Restore (GRT)

In questa sezione verranno trattati i seguenti argomenti sull'utilità Exchange Granular Restore (GRT):

Introduzione

Verifica delle considerazioni e dei prerequisiti

Ripristino dei dati di Microsoft Exchange mediante l'utilità Exchange Granular Restore (GRT)

Introduzione

L'utilità Exchange Granular Restore viene utilizzata per il ripristino degli oggetti di posta e non di posta di Microsoft Exchange. L'utilità include la possibilità di inserimento di elementi, ad esempio messaggi di posta elettronica, da database non in linea (*. EDB) e file di registro nei database originali attivi di Exchange, nonché di estrazione di dati granulari in file Personal Storage (.pst).

Questa utilità include i seguenti vantaggi fondamentali:

- Supporta elementi non di posta elettronica (ad esempio, calendari, contatti, attività) e cartelle pubbliche.
- È in grado di funzionare anche con solo un file di database. I registri non sono obbligatori, ma garantiscono la disponibilità di dati ancora più recenti per il ripristino.
- Non è necessario generare un catalogo poiché ripristina direttamente la posta dal punto di ripristino montato.
- Richiede una quantità minima di tempo per il ripristino di un elemento di livello della casella di posta da un database o da una casella di posta utente di qualsiasi dimensione.
- Supporta le opzioni della riga di comando per l'elaborazione di più database.

Nota: Per ulteriori informazioni sulle specifiche e sulle altre funzionalità supportate, consultare la Guida per l'utente di Exchange Granular Restore (esr.pdf).

Verifica delle considerazioni e dei prerequisiti

Verificare i seguenti prerequisiti prima di procedere al ripristino:

- L'utilità Exchange Granular Restore è disponibile al percorso seguente:

  Lo strumento è installato con l'agente Arcserve UDP nella directory seguente:

  ```
  X:\Programmi\Arcserve\Unified Data Protection\Engine\Exchange GRT
  ```

  Nota: Lo strumento è installato con l'agente Arcserve UDP.

- Il processo di ripristino è impostato per l'esecuzione dal computer di Exchange o dal computer proxy HBBU.

  Nota: Per eseguire il processo di ripristino da un altro computer, cercare il punto di ripristino dalla destinazione di backup.

- Ai fini del processo di ripristino vengono identificati il nome del database, il nome del server, il percorso del database (.edb) e i file di registro dell'utente.

  Per l'identificazione occorre utilizzare Exchange Management Console (EMC), il pannello di controllo di Exchange (ECP) o Exchange Management Shell.

  Esempio:

  ```
  Get-Mailbox -identity "username" | fl Database
  ```

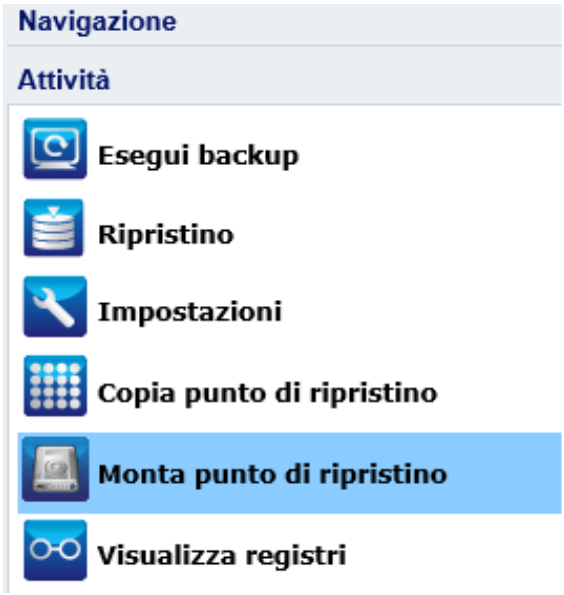
  ```
  Get-MailboxDatabase -identity "Databasename" | fl Name, Server, EdbFilePath,LogFolderPath
  ```

Ripristino dei dati di Microsoft Exchange mediante l'utilità Exchange Granular Restore (GRT)

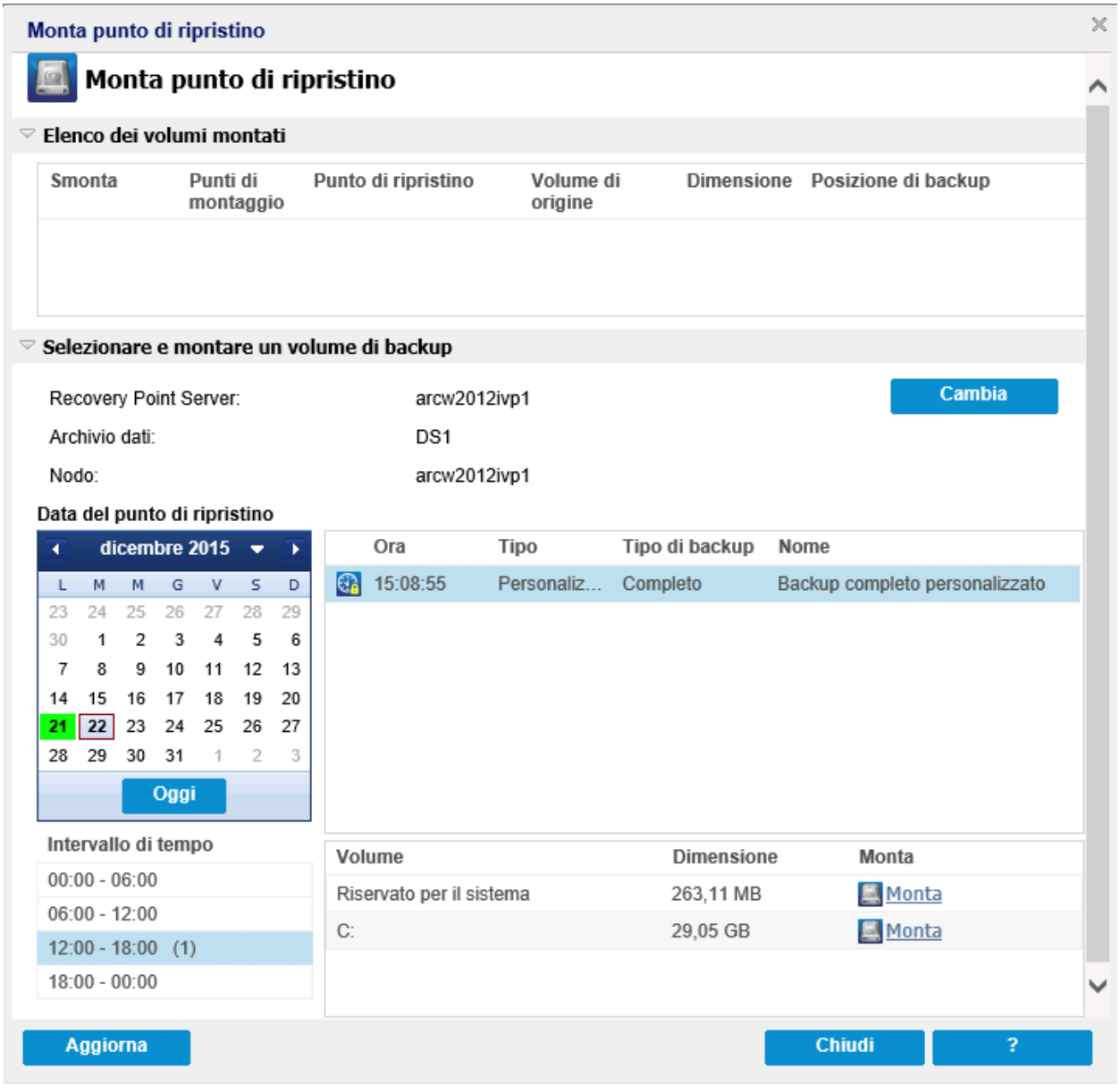
Prima di iniziare, verificare gli eventuali prerequisiti e considerazioni.

Per ripristinare elementi della casella di posta di Microsoft Exchange mediante l'utilità Exchange Granular Restore, completare le attività seguenti:

1. Dalla console dell'agente Arcserve UDP, selezionare l'attività Monta punto di ripristino (scelta consigliata) o ripristinare il database di Exchange nell'unità locale. Verrà visualizzata la finestra di dialogo Monta punto di ripristino.

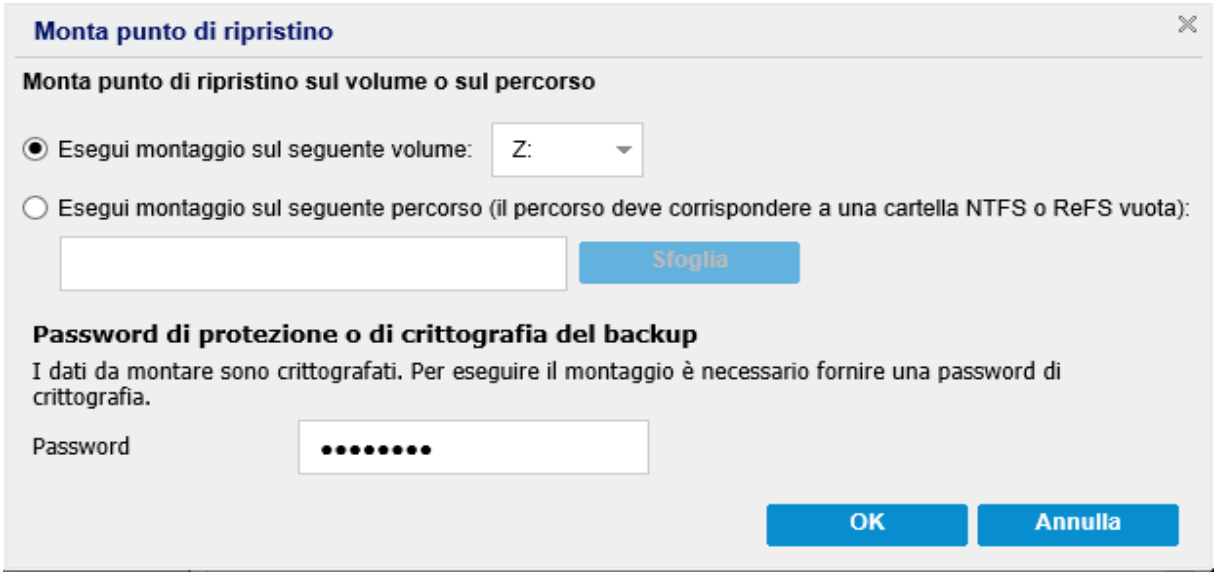


2. Selezionare la data del punto di ripristino e fare clic su **Monta** per i volumi che contengono il database e i registri di Exchange.



Nota: Se il server che esegue il processo di ripristino non è un proxy di Exchange o HBBU, fare clic su **Modifica** per selezionare il Recovery Point Server, l'archivio dati e il server Exchange appropriati.

3. Selezionare la lettera di unità per il montaggio del volume e fare clic su **OK**.



4. Avviare l'utilità del ripristino granulare di Exchange da una delle seguenti posizioni:

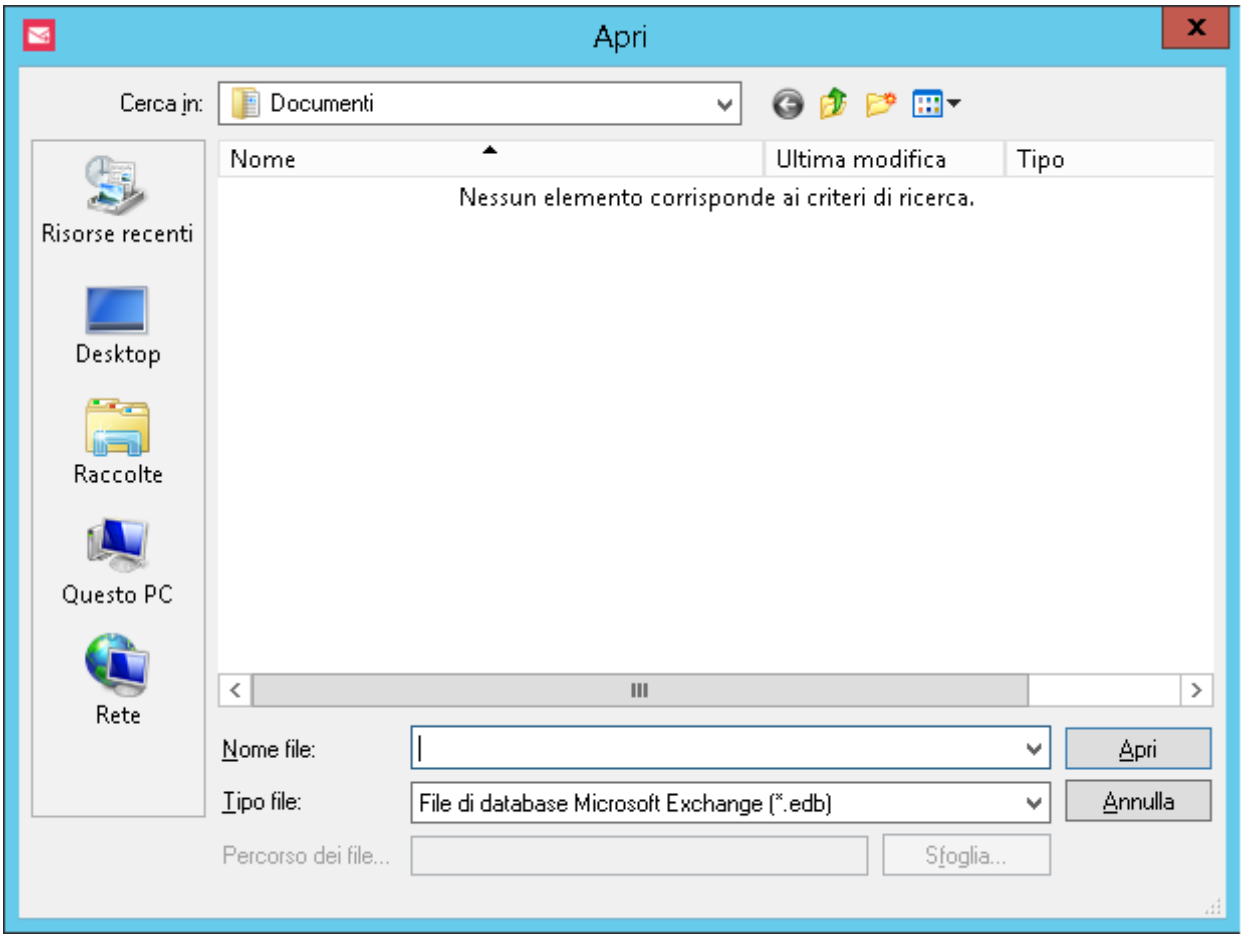
   Start > Tutti i programmi > Arcserve > Unified Data Protection > Arcserve UDP Exchange Granular Restore

   oppure

   X:\Programmi\Arcserve\Unified Data Protection\Engine\Exchange GRT\esr.exe

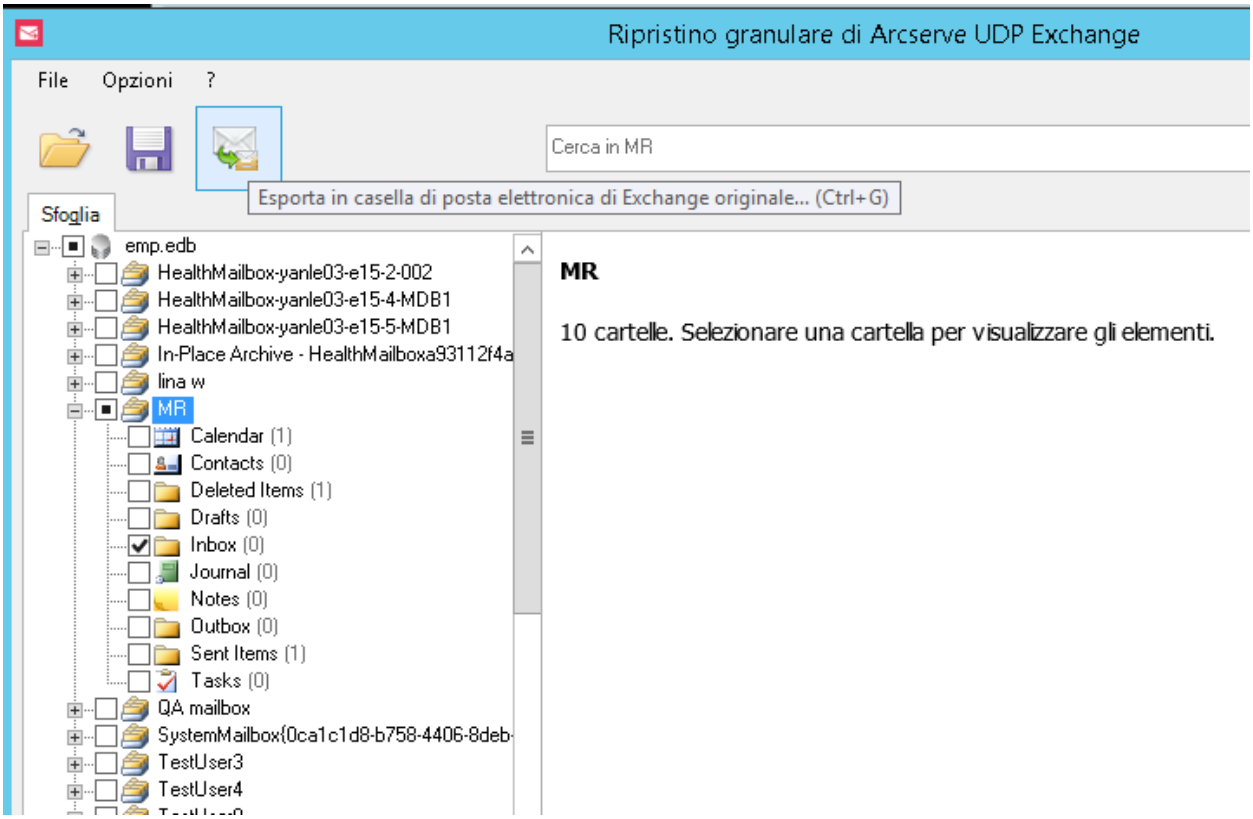
   Viene visualizzata una finestra di dialogo per indicare il percorso del database e dei file di registro.

5. Specificare il percorso nel volume montato e fare clic su **Apri**.



Viene aperta l'utilità Exchange Granular Restore di Arcserve UDP.

6. Selezionare i dati utente da ripristinare e fare clic su **Export into original mailbox (Esporta in casella di posta originale)** o **Export into .PST (Esporta in file .pst)**.



Note:

- Per ulteriori informazioni su specifiche, funzionalità, opzioni utente e limitazioni supportate, consultare la Guida per l'utente di Exchange Granular Restore (esr.pdf) all'indirizzo seguente:

  %Programmi%\Arcserve\Unified Data Protection\Engine\Exchange GRT o Bookshelf.

- Per impostazione predefinita, l'utilità funziona con l'utente attualmente connesso a Windows per stabilire la connessione. Se l'utente corrente non dispone delle autorizzazioni per rappresentare l'utente selezionato, viene riportato un messaggio di errore nel riquadro **Dettagli**:

  In caso di errore, si consiglia di accedere al computer con un account che dispone dei diritti di rappresentazione per l'utente selezionato o con l'account dell'utente selezionato.

7. Al termine del processo di ripristino, smontare il volume utilizzato per il ripristino.

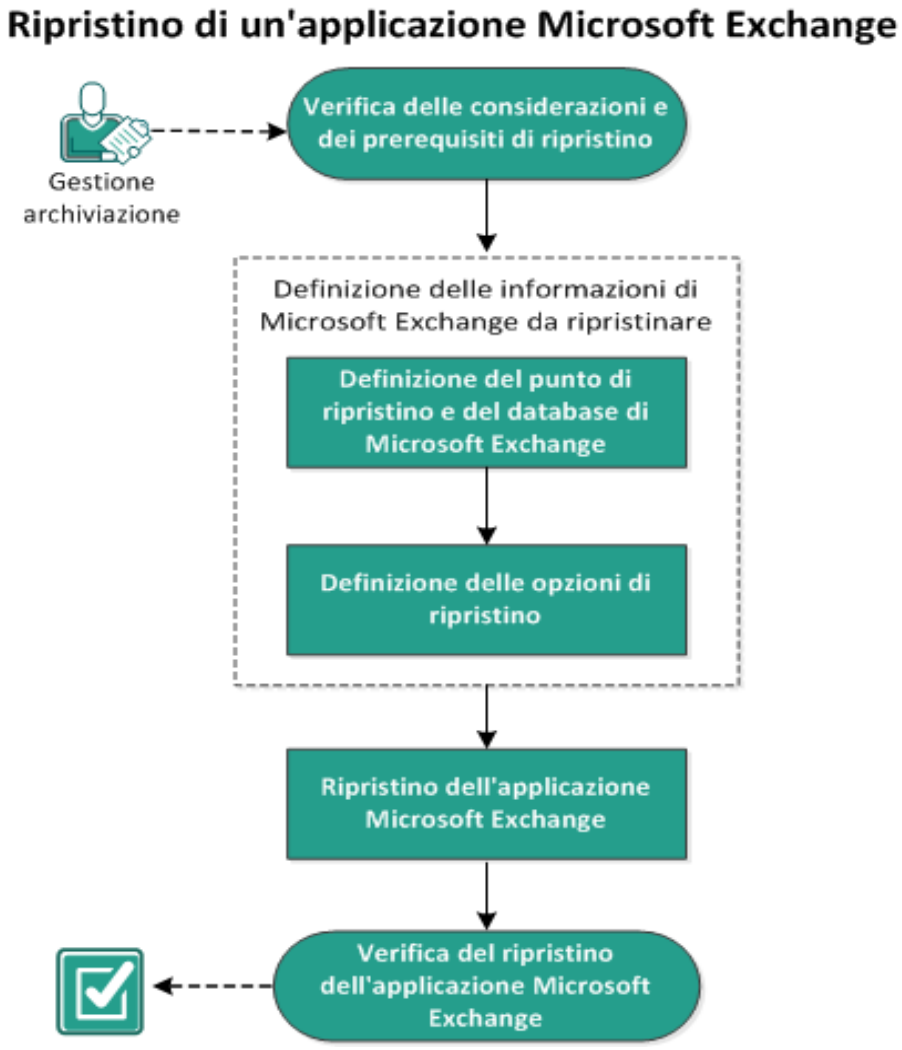
   Per smontare il volume, dalla console dell'agente Arcserve UDP, fare clic su **Monta punto di ripristino**, quindi su **Smonta**.


Monta punto di ripristino
Monta punto di ripristino
Elenco dei volumi montati
Smonta
Punti di montaggio
Punto di ripristino
Volume di origine
Dimensione
Posizione di backup
Smonta
Z:
22/12/2015 15:08:55
C:
29,05 GB
\\arcw2012ivp1\CA_UDP_DS...

Ripristino di un'applicazione Microsoft Exchange

L'agente Arcserve UDP (Windows) consente non solo di proteggere e ripristinare i dati, ma anche di acquisire le applicazioni che utilizzeranno ed eseguiranno il backup dei dati. È possibile eseguire il recupero delle applicazioni soltanto mediante il metodo Ripristino per punti di ripristino. Durante un recupero delle applicazioni, l'agente Arcserve UDP (Windows) consente di mantenere la coerenza dei dati per qualsiasi applicazione compatibile con Volume Shadow Copy Service (VSS) di Windows. L'agente Arcserve UDP (Windows) consente di eseguire il ripristino dell'applicazione Microsoft Exchange Server senza dover eseguire un ripristino di emergenza completo.

Il diagramma seguente illustra il processo di ripristino di un'applicazione Microsoft Exchange:



Eseguire le attività seguenti per ripristinare un'applicazione Microsoft Exchange:

1. Verifica delle considerazioni e dei prerequisiti di ripristino
2. Definizione delle informazioni di Microsoft Exchange da ripristinare
    a. Definizione del punto di ripristino e del database di Microsoft Exchange
    b. Definizione delle opzioni di ripristino
3. Ripristino dell'applicazione Microsoft Exchange
4. Verifica del ripristino dell'applicazione Microsoft Exchange

Verifica delle considerazioni e dei prerequisiti di ripristino

L'agente Arcserve UDP (Windows) supporta le seguenti versioni di Microsoft Exchange Server:

- Microsoft Exchange 2010 - Ambiente con server singolo e per gruppo di disponibilità del database (DAG).
- Microsoft Exchange 2013 e 2016 - Ambiente con server singolo e per gruppo di disponibilità del database (DAG).

  Per l'ambiente Microsoft Exchange Server 2010, 2013 e 2016 DAG, è necessario installare l'agente Arcserve UDP (Windows) su tutti i server membri nel gruppo DAG. Il backup di copie di database attive e passive può essere eseguito da qualsiasi server membro, ma il ripristino può essere eseguito solo su una copia di database attiva.
- Sebbene tutti i membri del DAG possano far parte dello stesso piano di backup o di uno diverso, si consiglia di utilizzare lo stesso archivio dati di deduplicazione per eliminare i dati duplicati.

È possibile eseguire il ripristino di Microsoft Exchange Server ai seguenti livelli:

Writer Microsoft Exchange

Se si desidera ripristinare tutti i dati di Microsoft Exchange Server, è possibile eseguire un ripristino a livello di Writer Microsoft Exchange.

Gruppo di archiviazione

Se si desidera ripristinare un gruppo di archiviazione specifico, è possibile eseguire un ripristino a questo livello.

Nota: Il livello del gruppo di archiviazione non viene applicato a Microsoft Exchange Server 2010, 2013 e 2016.

Database delle caselle di posta (Microsoft Exchange 2010, 2013 e 2016)

Se si desidera ripristinare un database delle caselle di posta specifico, è possibile eseguire un ripristino a questo livello.

Livello della casella di posta (Microsoft Exchange 2010, 2013 e 2016)

Definisce se si desidera ripristinare un archivio caselle di posta specifico o un oggetto di posta.

Verificare i seguenti prerequisiti prima di procedere al ripristino di Microsoft Exchange:

Ripristino a livello di database

- Il computer di destinazione presenta lo stesso nome e la stessa versione di Microsoft Exchange installata.
- Il database di destinazione presenta lo stesso nome database e lo stesso nome gruppo di archiviazione (Microsoft Exchange 200X) ed è incluso nella stessa struttura di Microsoft Exchange.

Ripristino a livello granulare

- Per ripristinare i dati di Microsoft Exchange, utilizzare l'utilità Exchange Granular Restore.

Definizione delle informazioni di Microsoft Exchange da ripristinare

L'agente Arcserve UDP (Windows) consente non solo di proteggere e ripristinare i dati, ma anche di acquisire l'applicazione Microsoft Exchange Server che utilizzerà ed eseguirà il backup dei dati. Il recupero di Microsoft Exchange Server può essere eseguito solo mediante il metodo di Ripristino per punti di ripristino.

Il processo interessato nel ripristino dell'applicazione Microsoft Exchange è il seguente:

1. Definizione del punto di ripristino e del database di Microsoft Exchange
2. Definizione delle opzioni di ripristino

Definizione del punto di ripristino e del database di Microsoft Exchange

Utilizzare l'opzione **Sfoglia punti di ripristino** per eseguire il ripristino da un punto di ripristino. Quando viene selezionata una data di ripristino, verranno visualizzati tutti i punti di ripristino associati a tale data. È possibile, quindi, individuare e selezionare il database Microsoft Exchange da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere alla finestra di dialogo per la selezione del metodo di ripristino in uno dei modi seguenti:

   Da Arcserve UDP:

   a. Accedere ad Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

      Nota: Viene effettuato automaticamente l'accesso al nodo agente e la finestra di dialogo per la selezione del metodo di ripristino viene visualizzata dal nodo agente.

   Dall'agente Arcserve UDP (Windows):

   a. Accedere all'agente Arcserve UDP (Windows).

   b. Dalla pagina principale selezionare **Ripristino**.

   Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

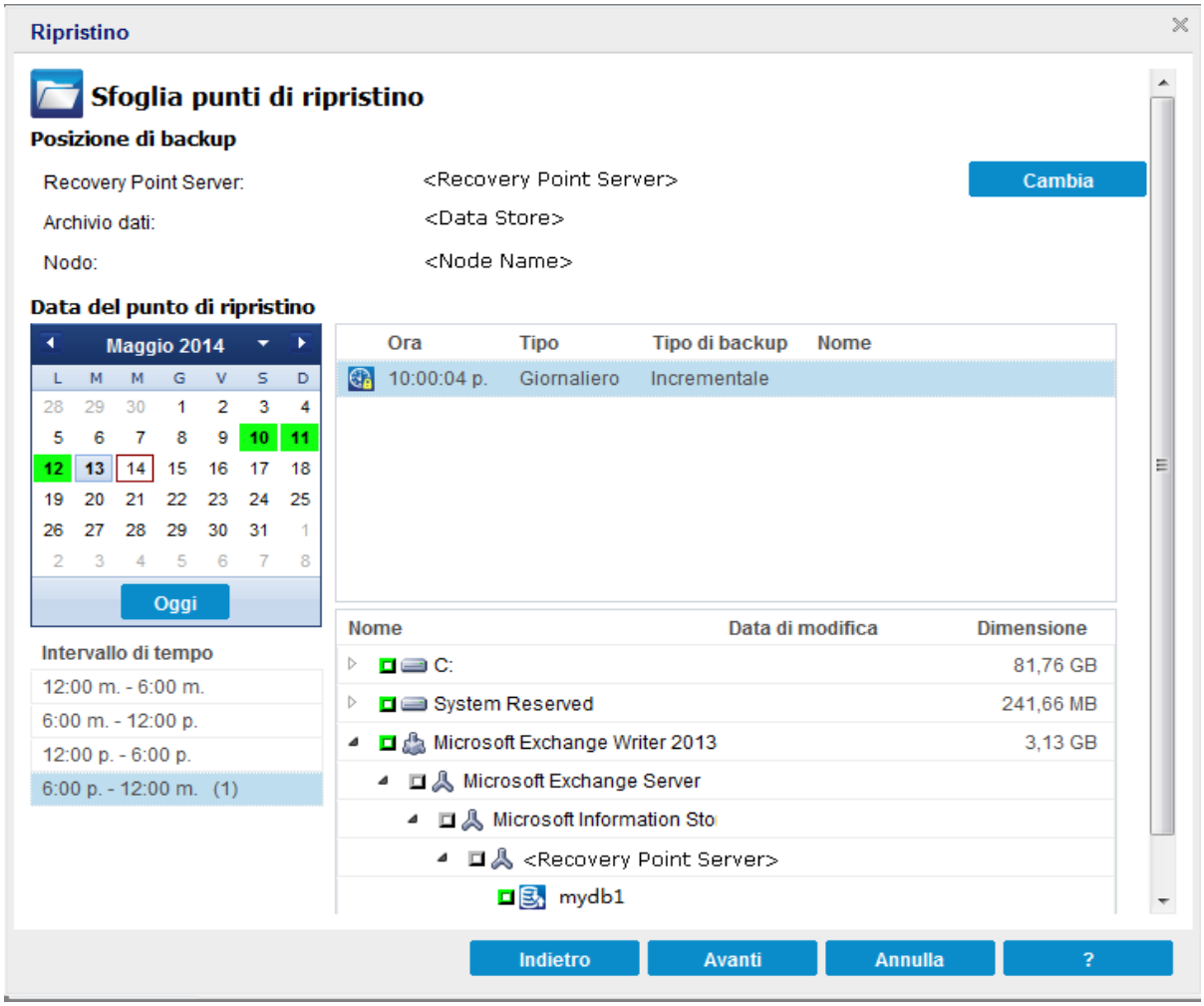
2. Fare clic sull'opzione **Sfoglia punti di ripristino**.

   Verrà visualizzata la finestra di dialogo **Sfoglia punti di ripristino**.

3. Selezionare il punto di ripristino (data e ora) e il database di Microsoft Exchange che si desidera ripristinare.

   La casella dell'indicatore corrispondente viene contrassegnata in verde per indicare che il database è stato selezionato per il ripristino.

Nota: se non si desidera applicare i file di registro delle transazioni dopo il ripristino, sarà necessario eliminarli manualmente prima di eseguire il ripristino. Per ulteriori informazioni sull'eliminazione manuale dei file di registro delle transazioni, consultare la documentazione di Microsoft Exchange Server.



4. Fare clic su **Avanti**.

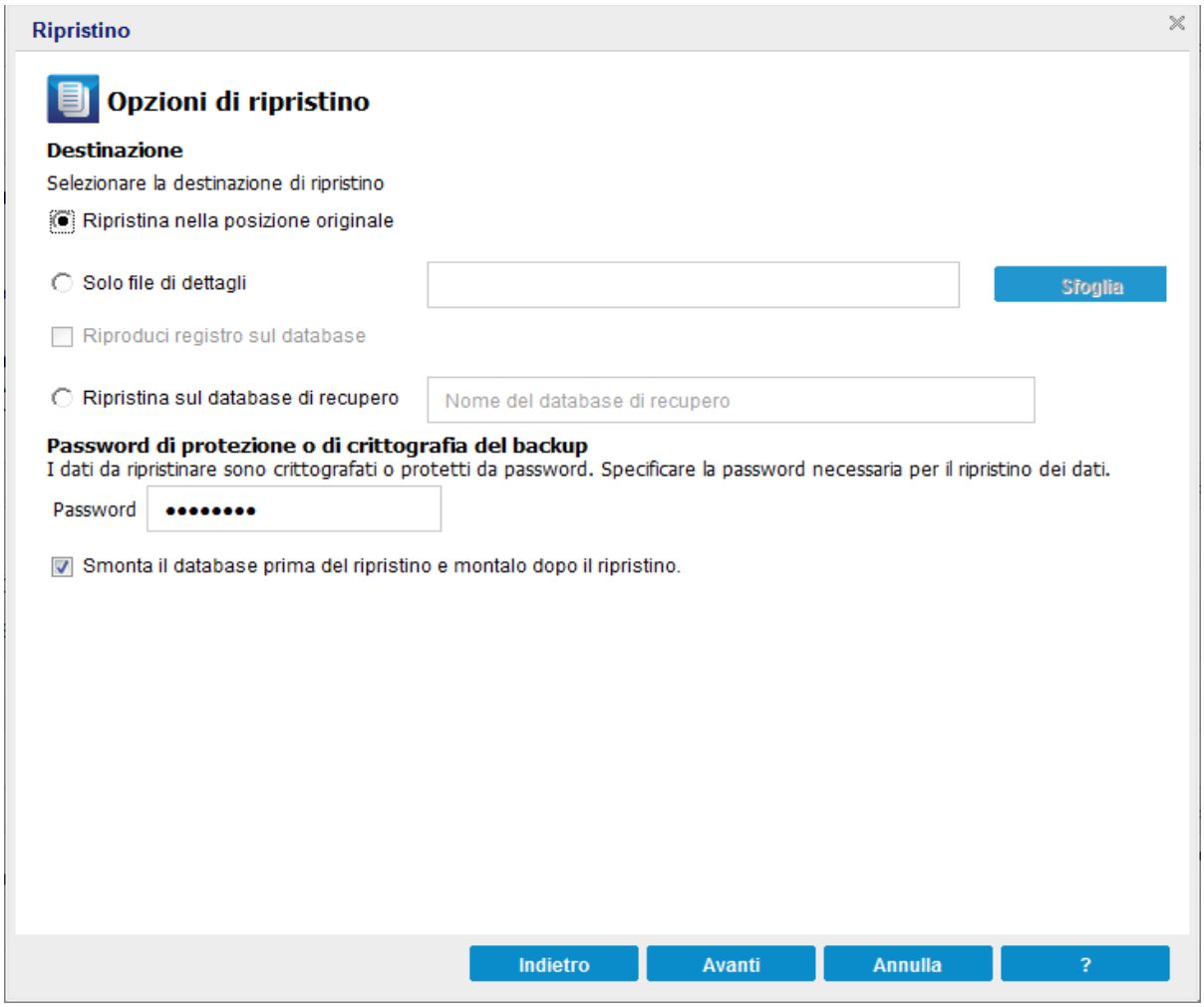
   Verrà visualizzata la finestra di dialogo **Opzioni di ripristino**.

Definizione delle opzioni di ripristino

Dopo avere specificato un punto di ripristino e il contenuto da ripristinare, definire le opzioni di copia per il punto di ripristino selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Opzioni di ripristino**, specificare la destinazione di ripristino.



2. Selezionare la destinazione per il ripristino.

Le opzioni disponibili consentono di eseguire il ripristino nella posizione originale di backup, nel gruppo di archiviazione di recupero, nel database delle caselle di posta di recupero oppure di eseguire il ripristino solo del file di dettagli.

Ripristina in posizione originale

Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

Solo file di dettagli

Esegue il ripristino dei file dei dettagli.

L'agente Arcserve UDP (Windows) esegue il ripristino del file di database di Microsoft Exchange nella cartella specificata, che rimane non in linea una volta completato il ripristino. Sarà quindi possibile utilizzarlo per eseguire il montaggio manuale di Microsoft Exchange Server.

Nota: se è presente un database di elementi ripristinati da caselle di posta, il ripristino mediante l'opzione **Solo file di dettagli** non verrà completato.

Riproduci registro sul database

Specifica che quando viene eseguito il dump dei file di database sulla cartella di destinazione, è possibile riprodurre il file di registro delle transazioni di Microsoft Exchange e confermarli nel file del database.

Smonta il database prima del ripristino e montalo dopo il ripristino.

In genere, prima di eseguire un ripristino, Microsoft Exchange verifica le seguenti condizioni:

- Lo stato del database da ripristinare è *Smontato*.
- Non è stato eseguito il ripristino imprevisto del database.

Per evitare il ripristino imprevisto di un database di produzione di Microsoft Exchange, è disponibile un'opzione che consente di sovrascrivere il database durante il processo di ripristino. Nel caso in cui tale opzione sia disattivata, Microsoft Exchange non esegue il ripristino del database.

Per l'agente Arcserve UDP (Windows), queste due opzioni vengono controllate dall'opzione Smonta il database prima del ripristino e montalo dopo il ripristino. Con questa opzione, l'agente Arcserve UDP (Windows) consente l'avvio automatico del processo di ripristino senza dover eseguire alcuna operazione manuale. Se lo si desidera, è possibile impostare il montaggio/smontaggio manuale del database.

- Se l'opzione è selezionata, il processo di recupero smonta automaticamente il database di Microsoft Exchange prima di avviare il processo di ripristino e

monta il database una volta completato il processo di ripristino. Se selezionata, questa opzione consente inoltre la sovrascrittura del database di Microsoft Exchange durante il ripristino.

- Se deselezionata, l'opzione specifica che il processo di recupero non smonta automaticamente il database di Microsoft Exchange prima di avviare il processo di recupero e monta il database una volta completato il recupero.

È necessario che l'amministratore di Microsoft Exchange esegua alcune operazioni manuali, ad esempio smontare il database di Microsoft Exchange, impostare il flag di sovrascrittura del database e montare il database di Microsoft Exchange. La procedura di recupero viene eseguita da Exchange durante il montaggio del database.

Inoltre, se deselezionata, questa opzione non consente la sovrascrittura del database di Microsoft Exchange durante il ripristino.

Ripristino sul database di ripristino (Microsoft Exchange 2010 e 2013)

Esegue il ripristino del database su un database di recupero. Un database di recupero è un database che può essere utilizzato per operazioni di recupero. È possibile ripristinare i database delle caselle di posta di Microsoft Exchange Server da un backup su un database di recupero, quindi eseguire il recupero e l'estrazione dei dati senza compromettere il database di produzione a cui accedono gli utenti finali.

Prima di eseguire il ripristino di un database Microsoft Exchange 2010 o Exchange 2013 su un database di ripristino, è necessario creare prima di tutto il database di ripristino.

3. Fare clic su **Avanti**.

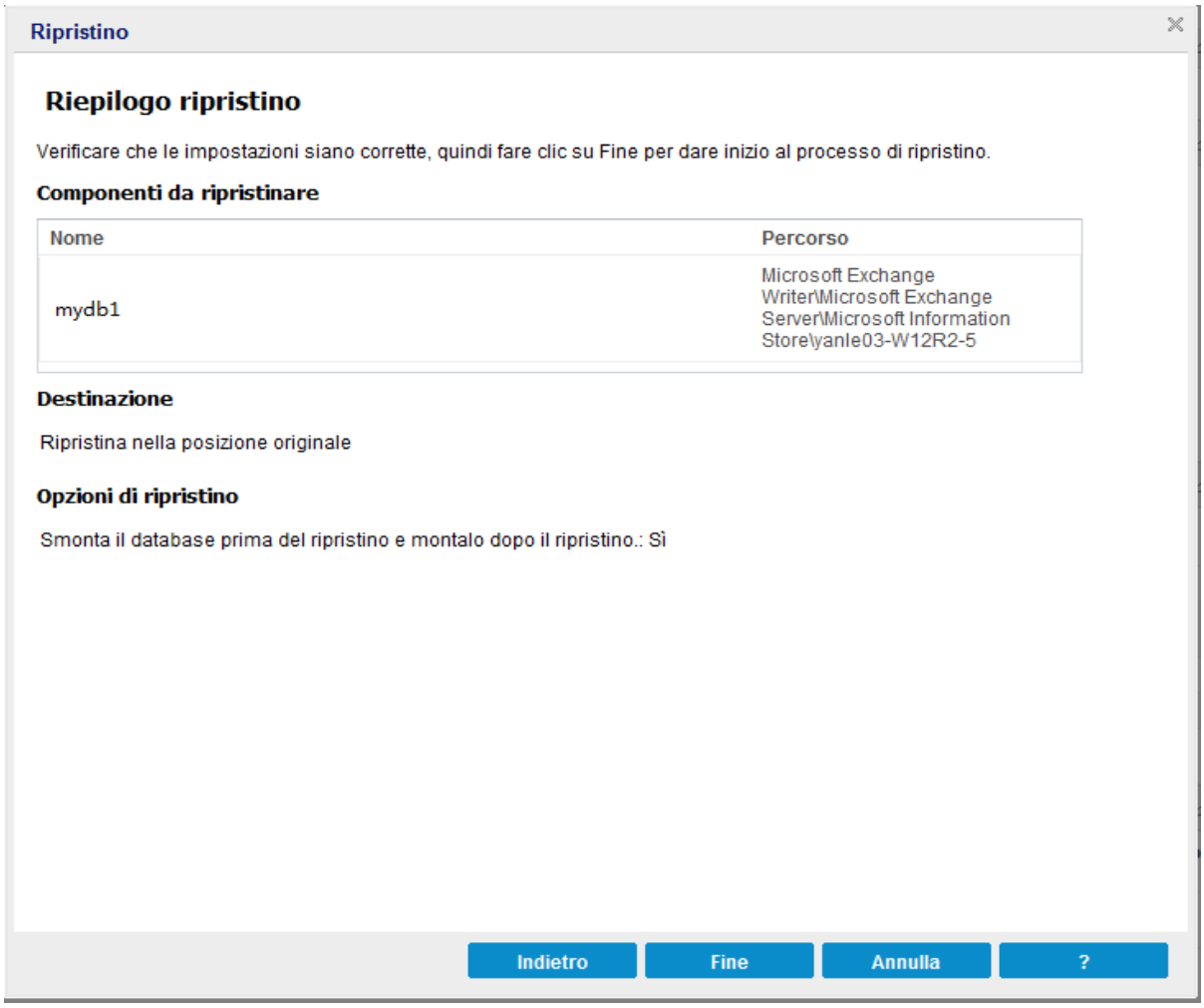
Verrà visualizzata la finestra di dialogo **Riepilogo ripristino**.

Ripristino dell'applicazione Microsoft Exchange

Una volta definite le opzioni di ripristino, verificare che le impostazioni siano corrette e confermare il processo di ripristino. Il **riepilogo di ripristino** consente di verificare tutte le opzioni di ripristino definite e, se necessario, modificarle.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Riepilogo ripristino**, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



- Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
- Se le informazioni di riepilogo sono corrette, fare clic su **Avanti**, quindi su **Fine** per avviare il processo di ripristino.

Viene ripristinata l'applicazione Microsoft Exchange.

Verifica del ripristino dell'applicazione Microsoft Exchange

Effettuare le operazioni seguenti:

1. Accedere alla destinazione di ripristino dell'agente Arcserve UDP (Windows) specificata.

   Ad esempio, se si seleziona il ripristino del database Microsoft Exchange nella posizione originale in seguito al completamento del ripristino, aprire la posizione fisica per verificare che il database e i registri di Microsoft Exchange siano stati ripristinati.

   Se si seleziona il ripristino del database di Microsoft Exchange sulla posizione del file di dettagli, l'agente Arcserve UDP (Windows) eseguirà il ripristino del database di Microsoft Exchange e lo registrerà su una posizione specifica.

2. Verificare che l'applicazione Microsoft Exchange sia stata ripristinata, quindi verificare che il database sia stato montato e sia accessibile.

   Viene ripristinata l'applicazione Microsoft Exchange.

Ripristino dei dati di Exchange su un computer virtuale VMware

Importante! Per ripristinare i dati di Microsoft Exchange su un computer virtuale VMware, si consiglia di utilizzare l'utilità Exchange Granular Restore.

Download di file o cartelle senza ripristino

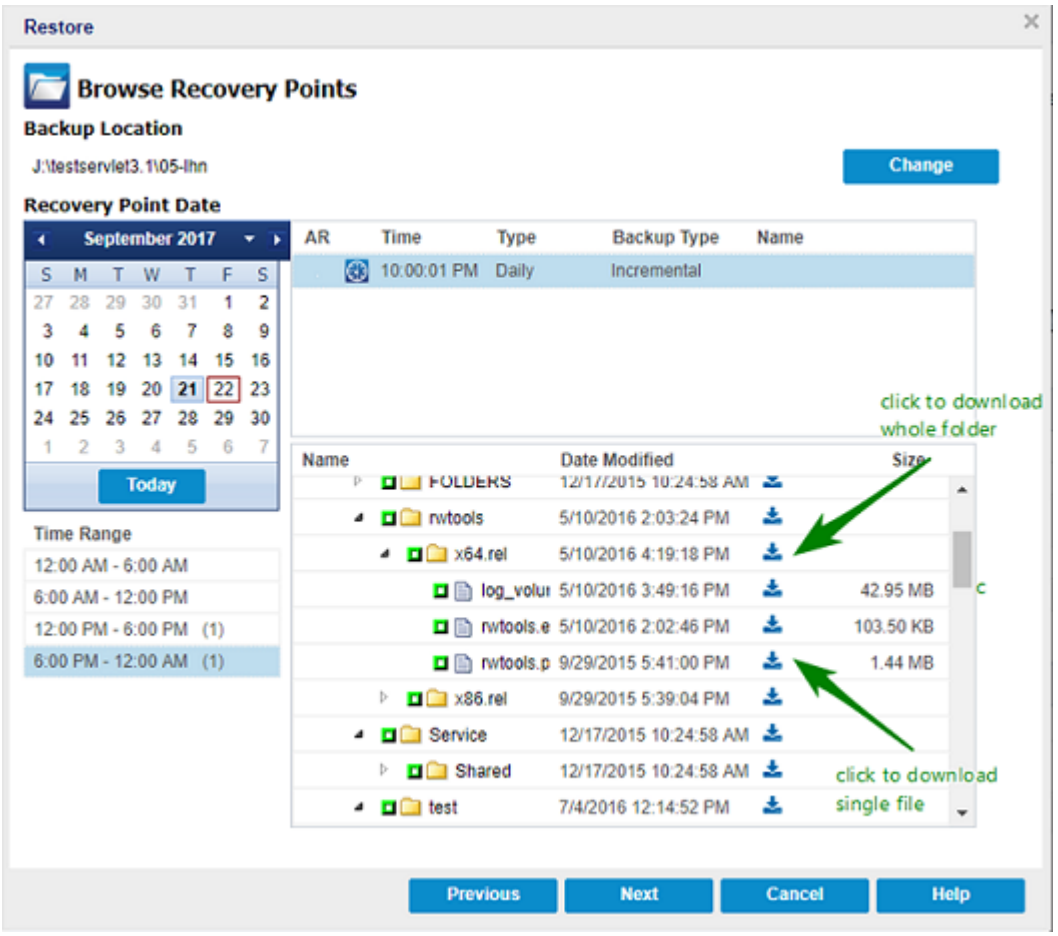
Arcserve UDP consente di scaricare un file o una cartella completa senza doverli inviare per il ripristino. Dalla procedura guidata di ripristino, la schermata Sfoglia punti di ripristino consente di scaricare direttamente qualsiasi file o cartella completa contenente tutti i file. L'esecuzione del download prima del ripristino consente di effettuare una breve ricerca dei file per impedire il ripristino dei file non desiderati.

Nota: Il download dei file non mantiene le autorizzazioni del file o della cartella.

Un singolo file viene scaricato direttamente nello stesso formato, mentre una cartella viene scaricata come file .zip. Il nome del formato del file .zip è il seguente:

[nodename]_[sessionid]_[timestamp].zip

Per eseguire il download, è sufficiente accedere alla schermata Sfoglia punti di ripristino nella procedura guidata di ripristino. La seguente schermata illustra la procedura di download di un file o di una cartella:



Considerazioni per il download:

- Il download o la compressione come file .zip non sono possibili per alcuni file di sistema. Il servizio Tomcat dell'agente non dispone di privilegi sufficienti per accedere al file system o ai file utente dell'altro nodo protetto.
- Per evitare un consumo eccessivo della memoria Tomcat e dell'utilizzo della CPU, si consiglia di inviare un processo di ripristino in un percorso alternativo per il download di file o cartelle di grandi dimensioni.
- L'utilizzo di strumenti per la compressione di cartelle di Windows per l'accesso ai file .zip scaricati potrebbe produrre un errore in quanto lo strumento rileva il superamento della lunghezza massima dei nomi dei file .zip. Si consiglia di utilizzare altri strumenti .zip per aprire il file. Ad esempio WinZip, WinRAR, 7-Zip.
- Gli utenti IE9 che utilizzano https in IE9 e il servizio Web dell'agente potrebbero non essere in grado di scaricare i file. Un problema noto di download delle risorse di IE9 da una pagina dinamica tramite https impedisce il download. Per ottenere ulteriori informazioni e soluzioni, fare clic sul collegamento dell'articolo Microsoft.

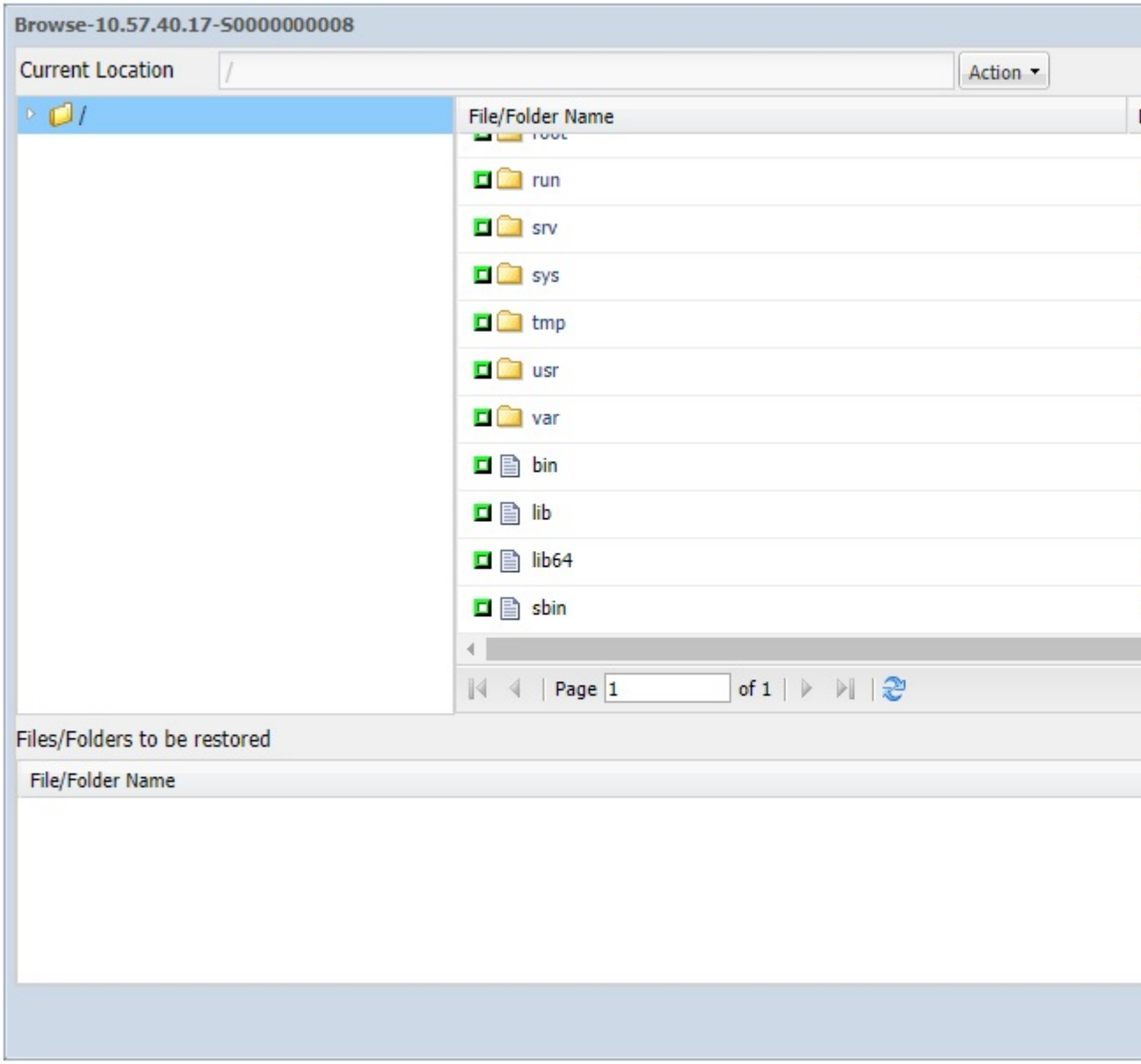
Download di file/cartelle senza ripristino per i nodi Linux

Arcserve UDP consente di scaricare un file o una cartella completa senza doverli inviare per il ripristino. Dalla procedura guidata di ripristino, la schermata Sfoglia punti di ripristino consente di scaricare direttamente qualsiasi file o cartella completa contenente tutti i file. L'esecuzione del download prima del ripristino consente di effettuare una breve ricerca dei file per impedire il ripristino dei file non desiderati.

Un singolo file viene scaricato direttamente nello stesso formato, mentre una cartella viene scaricata come file .zip. Il nome del formato del file .zip è il seguente:

[nodename]_[sessionid]_[timestamp].zip

Per eseguire il download, è sufficiente accedere alla schermata Sfoglia punti di ripristino nella procedura guidata di ripristino. La seguente schermata illustra la procedura di download di un file o di una cartella per i nodi Linux:

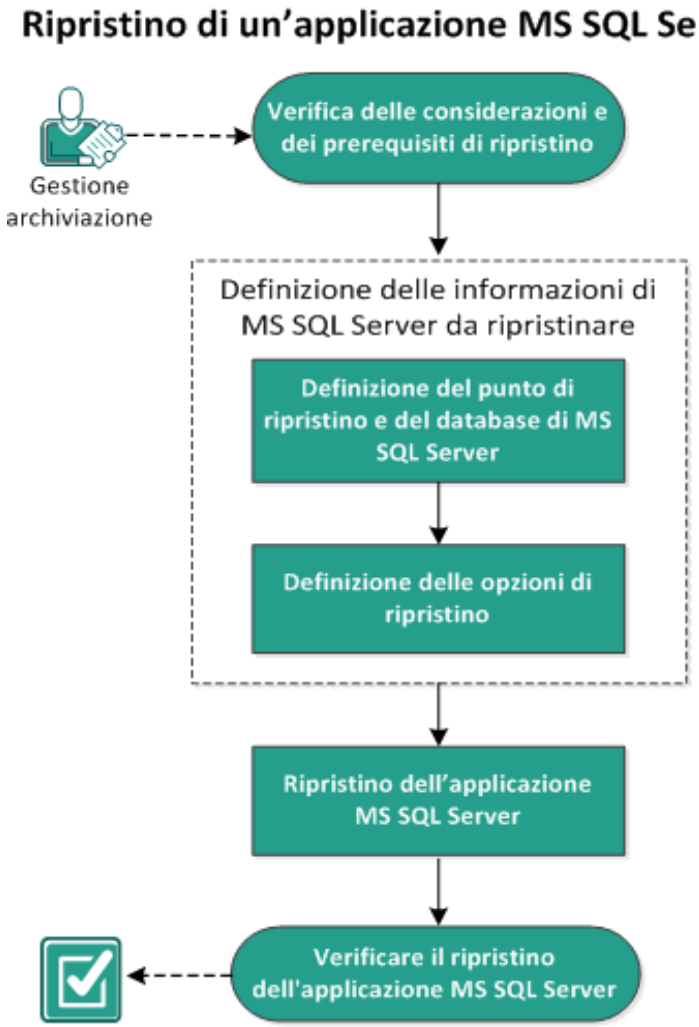


Per aprire i file scaricati, utilizzare gli strumenti zip, ad esempio WinZip, WinRAR, 7-Zip e così via.

Ripristino di un'applicazione Microsoft SQL Server

L'agente Arcserve UDP (Windows) consente non solo di proteggere e ripristinare i dati, ma anche di acquisire le applicazioni che utilizzeranno ed eseguiranno il backup dei dati. È possibile eseguire il recupero delle applicazioni soltanto mediante il metodo Ripristino per punti di ripristino. Durante un recupero delle applicazioni, l'agente Arcserve UDP (Windows) consente di mantenere la coerenza dei dati per qualsiasi applicazione compatibile con Volume Shadow Copy Service (VSS) di Windows. L'agente Arcserve UDP (Windows) consente di eseguire il ripristino dell'applicazione Microsoft SQL Server senza dover eseguire un ripristino di emergenza completo.

Il diagramma seguente illustra il processo di ripristino di un'applicazione Microsoft SQL Server:



Eseguire le attività seguenti per ripristinare un'applicazione Microsoft SQL Server:

1. Verifica delle considerazioni e dei prerequisiti di ripristino
2. Definizione delle informazioni di Microsoft SQL Server da ripristinare
    a. Definizione del punto di ripristino e del database Microsoft SQL Server
    b. Definizione delle opzioni di ripristino
3. Ripristino dell'applicazione Microsoft SQL Server
4. Verifica del ripristino dell'applicazione Microsoft SQL Server

Verifica delle considerazioni e dei prerequisiti di ripristino

Verificare i seguenti prerequisiti prima di procedere al ripristino:

- Per eseguire il ripristino di un'applicazione SQL, è necessaria un'istanza di Microsoft SQL Server.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Verificare le seguenti considerazioni sul ripristino:

- Non è possibile eseguire il ripristino di un database a un'altra istanza. Il ripristino in una posizione alternativa dell'agente Arcserve UDP (Windows) consente di eseguire il ripristino del database e di modificarne il nome e la posizione del file. Per ulteriori informazioni, consultare la sezione Considerazioni sul ripristino Microsoft SQL Server in una posizione alternativa.
- Se i processi non riguardano lo stesso computer virtuale, Arcserve UDP consente di eseguire più processi di ripristino contemporaneamente. Se viene avviato un processo di ripristino durante l'esecuzione di un altro processo di ripristino per lo stesso computer virtuale, viene visualizzato un messaggio di avviso per indicare che è già in esecuzione un altro processo, pertanto sarà necessario riprovare in un momento successivo.
- L'agente Arcserve UDP (Windows) consente di eseguire un solo processo di ripristino alla volta. Se viene avviato manualmente un processo di ripristino durante l'esecuzione di un altro processo di ripristino, viene visualizzato un messaggio di avviso per indicare che è già in esecuzione un altro processo, pertanto sarà necessario riprovare in un momento successivo.

Considerazioni sul ripristino di Microsoft SQL Server in una posizione alternativa

Se si desidera eseguire il ripristino di un'applicazione Microsoft SQL Server in una posizione alternativa, è possibile eseguire l'operazione nello stesso computer o in un computer differente.

Prima di eseguire un ripristino dell'agente Arcserve UDP (Windows) di un'applicazione Microsoft SQL Server in una posizione alternativa, tenere presente quando segue:

Se la posizione alternativa si trova nello stesso computer

In questo caso, è possibile eseguire il ripristino di un database in una nuova posizione (con lo stesso nome) oppure eseguire il ripristino con un nuovo nome (nella stessa posizione).

- **Stesso nome - Nuova posizione**

  Ad esempio, se il database A è installato sul server SQL corrente in C:\DB_A ed è stato sottoposto a backup. È possibile utilizzare questa opzione e specificare un percorso alternativo del file per ripristinare il database A in una posizione alternativa, ad esempio D:\Alternate_A.

  Terminato il ripristino del database verrà utilizzato il file di database disponibile nel nuovo percorso (D:\Alternate_A).

  Importante: Se durante il ripristino si modifica la posizione del database mantenendo però il nome del database, al termine del ripristino il database precedente verrà eliminato. Il file di database ripristinato farà riferimento alla nuova posizione.

  Quando si effettua il ripristino in una posizione alternativa, la sezione relativa al nome dell'istanza non è disponibile, perché il nome dell'istanza deve essere sempre lo stesso e non può essere modificato. Di conseguenza, non è possibile eseguire il ripristino di un database in un'istanza alternativa attualmente presente sullo stesso sistema Microsoft SQL Server.

- **Stessa posizione - Nuovo nome**

  Ad esempio, se si dispone di due database (Database A e Database B) installati nel sistema SQL Server corrente ed entrambi sono stati sottoposti a backup. È possibile utilizzare questa opzione e selezionare l'opzione Nuovo nome database per eseguire il ripristino del Database A nella stessa posizione con il nome Database A_New.

  Terminato il ripristino dei database, nel percorso saranno presenti tre database (Database A, Database B e Database A_New).

Se la posizione alternativa si trova in un computer differente.

- Il percorso di installazione del sistema SQL Server deve coincidere con il percorso di installazione esistente al momento del backup.

  Ad esempio, se il backup del sistema SQL Server è stato installato in C:\SQLServer, anche il sistema SQL Server nel nuovo server dell'agente Arcserve UDP (Windows) deve essere installato in C:\SQLServer.

- Sul server dell'agente Arcserve UDP (Windows) è necessario installare un'istanza con lo stesso nome del database esistente al momento del backup. In caso contrario, il database associato all'istanza in questione verrà ignorato dal

ripristino.

Ad esempio, se il backup del sistema SQL Server contiene "Instance_1", con il database A e il database B, e "Instance_2" con il database C, ma il server dell'agente Arcserve UDP (Windows) contiene soltanto Instance_1. Al completamento del ripristino, il database A ed il database B verranno ripristinati, ma il database C non verrà ripristinato.

- La versione di SQL Server sul server dell'agente Arcserve UDP (Windows) deve essere compatibile con la versione precedente del sistema SQL Server utilizzato durante la sessione di backup.

  Ad esempio, è possibile eseguire il ripristino di un computer SQL Server 2008 su un computer SQL Server 2010. Non è tuttavia possibile eseguire l'operazione contraria.

- Il ripristino di un'istanza di database a 64 bit in un'istanza a 32 bit non è supportato.

Considerazioni sul ripristino di Microsoft SQL Server 2012/2014 AAG

Quando viene eseguito il ripristino di un database Microsoft SQL Server 2012/2014 appartenente a un gruppo AlwaysOn Availability (AAG), è necessario tenere presente alcune considerazioni.

Se il database Microsoft SQL Server appartiene al gruppo AlwaysOn Availability di Microsoft SQL Server 2012/2014 e si verifica un errore durante il ripristino nella posizione originale, completare le attività seguenti:

1. Rimuovere dal Gruppo di disponibilità il database da ripristinare. Per ulteriori informazioni, fare clic sul seguente collegamento.
2. Condividere la sessione di backup con l'agente Arcserve UDP (Windows) su ogni nodo del gruppo di disponibilità, quindi ripristinare la sessione dell'agente Arcserve UDP (Windows) su ogni nodo del gruppo di disponibilità.
3. Aggiungere nuovamente il database a un gruppo di disponibilità. Per ulteriori informazioni, fare clic sul seguente collegamento.

Definizione delle informazioni di Microsoft SQL Server da ripristinare

L'agente Arcserve UDP (Windows) consente non solo di proteggere e ripristinare i dati, ma anche di acquisire l'applicazione Microsoft SQL Server che utilizzerà ed eseguirà il backup dei dati. Il recupero di Microsoft SQL Server può essere eseguito solo utilizzando il metodo di ripristino per punti di ripristino.

Il processo interessato nel ripristino dell'applicazione Microsoft SQL Server è il seguente:

1. Definizione del punto di ripristino e del database Microsoft SQL Server
2. Definizione delle opzioni di ripristino

Definizione del punto di ripristino e del database Microsoft SQL Server

Utilizzare l'opzione **Sfoglia punti di ripristino** per eseguire il ripristino da un punto di ripristino. Quando viene selezionata una data di ripristino, verranno visualizzati tutti i punti di ripristino associati a tale data. È possibile, quindi, individuare e selezionare il database Microsoft SQL Server da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere alla finestra di dialogo per la selezione del metodo di ripristino in uno dei modi seguenti:
   - Da Arcserve UDP:
     a. Accedere ad Arcserve UDP.
     b. Fare clic sulla scheda **Risorse**.
     c. Selezionare **Tutti i nodi** nel riquadro sinistro.

        Tutti i nodi aggiunti vengono visualizzati nel riquadro centrale.
     d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.
     e. Fare clic su **Ripristina** dal menu a discesa del nome del server.

        Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

        Nota: Viene effettuato automaticamente l'accesso al nodo agente e la finestra di dialogo per la selezione del metodo di ripristino viene visualizzata dal nodo agente.
   - Dall'agente Arcserve UDP (Windows):

     Accedere all'agente Arcserve UDP (Windows).

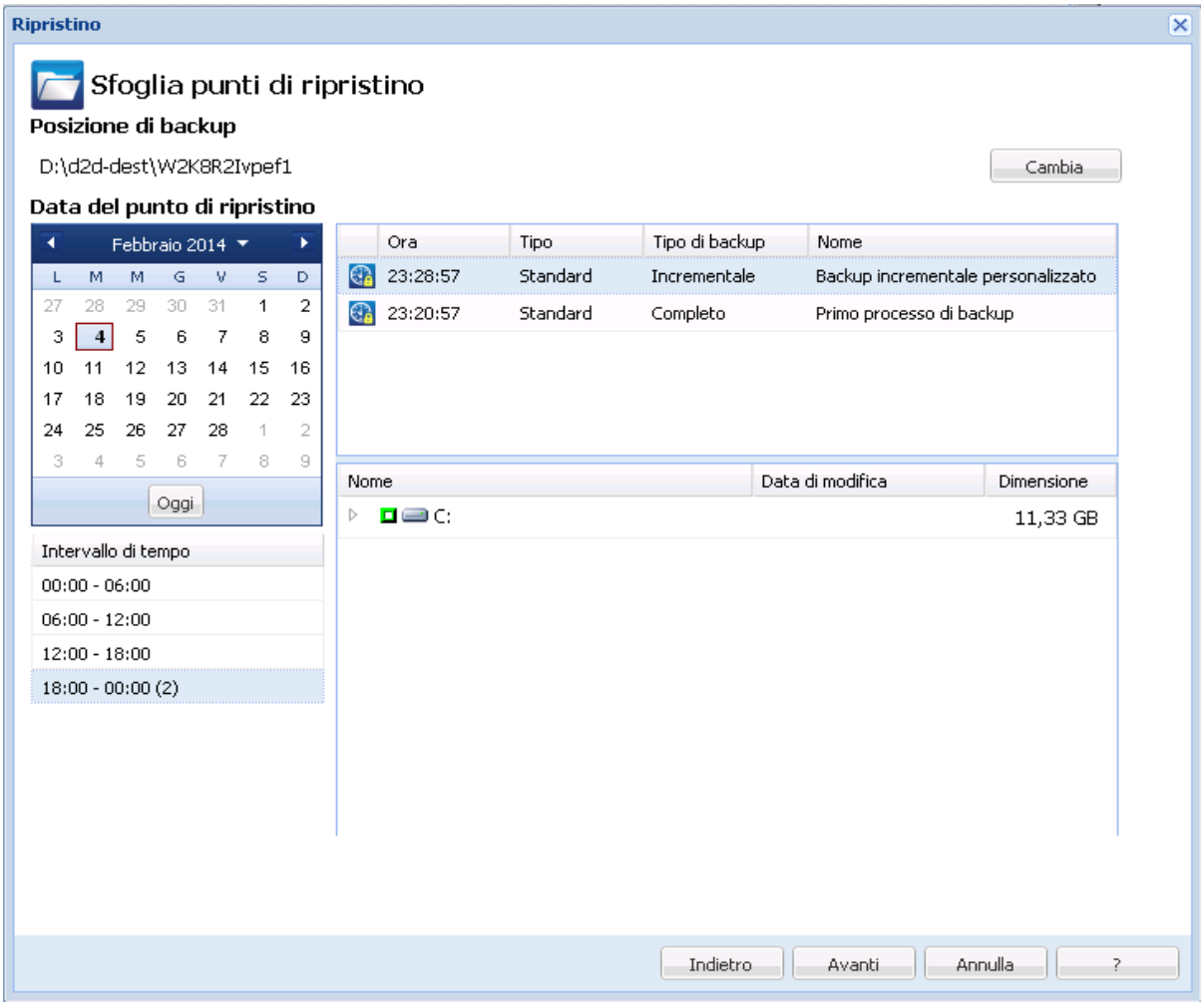
     b. Dalla pagina principale selezionare **Ripristino**.

     Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

2. Fare clic sull'opzione **Sfoglia punti di ripristino**.

   Verrà visualizzata la finestra di dialogo **Sfoglia punti di ripristino**.
3. Selezionare il punto di ripristino (data e ora) e il database Microsoft SQL Server che si desidera ripristinare.
4. La casella dell'indicatore corrispondente viene contrassegnata in verde per indicare che il database è stato selezionato per il ripristino.

Nota: se non si desidera applicare i file di registro delle transazioni dopo il ripristino, sarà necessario eliminarli manualmente prima di eseguire il ripristino. Per ulteriori informazioni sull'eliminazione manuale dei file di registro delle transazioni, consultare la documentazione Microsoft SQL Server.



5. Fare clic su **Avanti**.

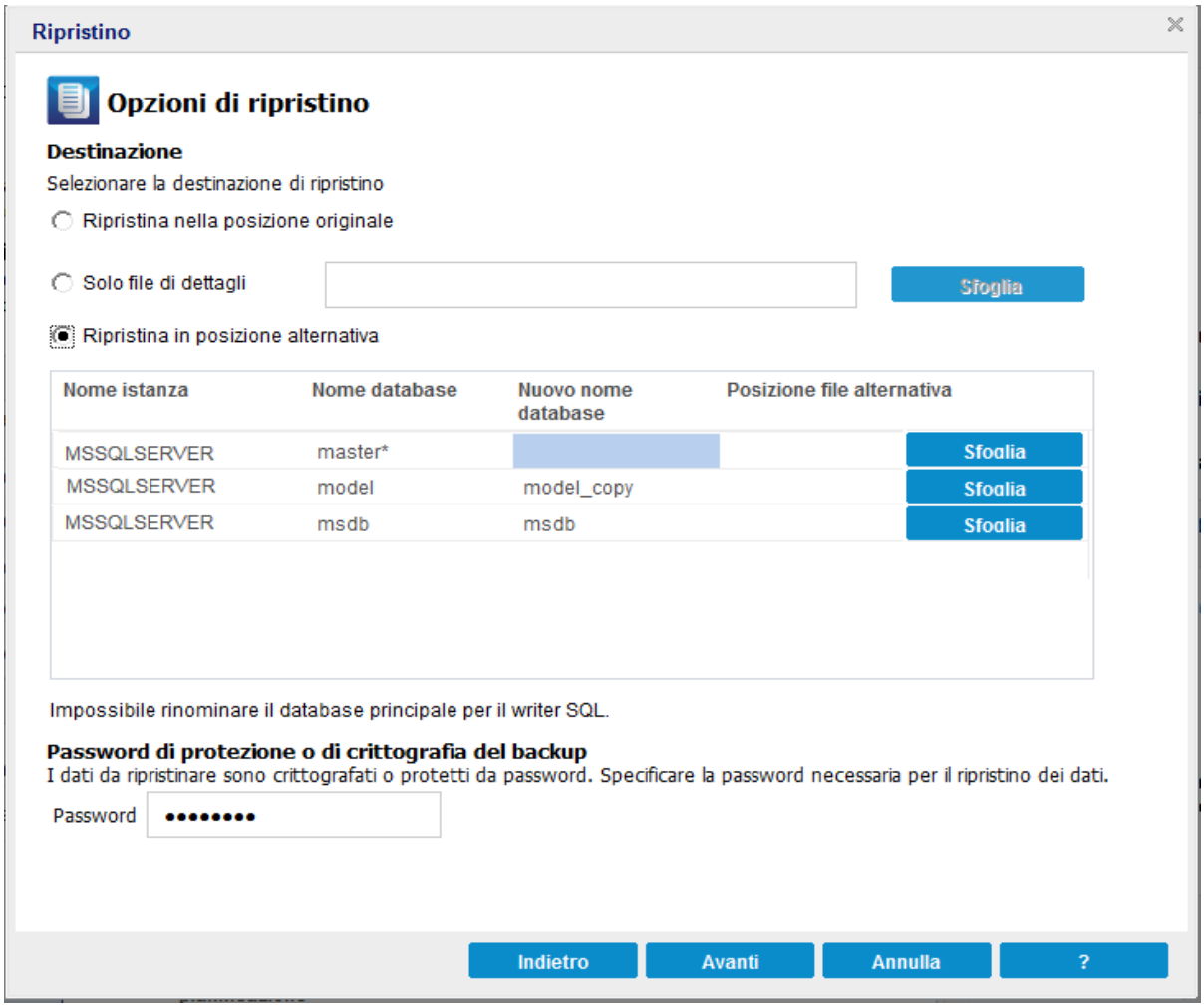
   Verrà visualizzata la finestra di dialogo **Opzioni di ripristino**.

Definizione delle opzioni di ripristino

Dopo avere specificato un punto di ripristino e il contenuto da ripristinare, definire le opzioni di copia per il punto di ripristino selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Opzioni di ripristino**, specificare la destinazione di ripristino.



2. Selezionare la destinazione per il ripristino.

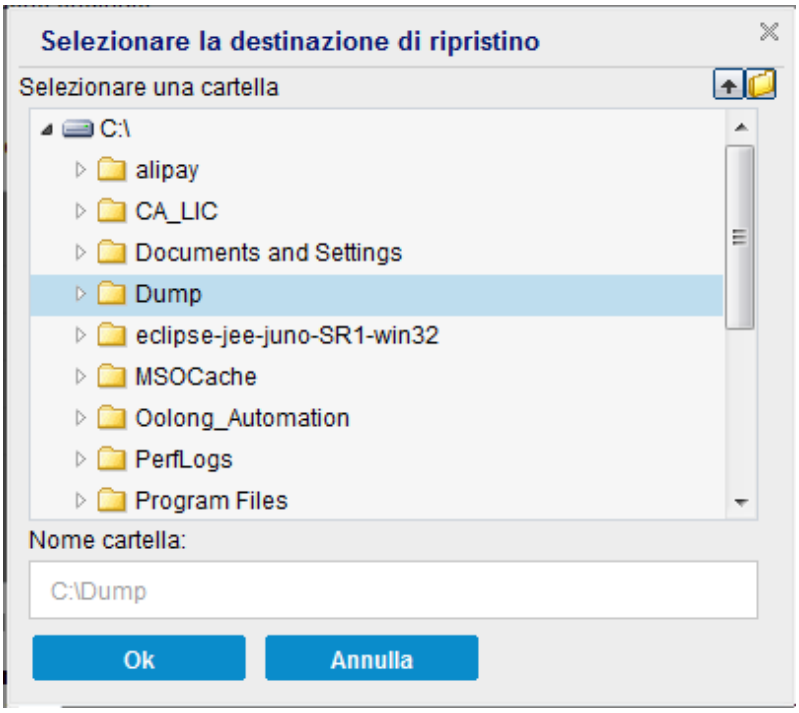
   Le opzioni disponibili consentono di eseguire il ripristino nella posizione originale del backup, in una posizione diversa oppure solo del file di dettagli.

   Ripristina in posizione originale

   Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

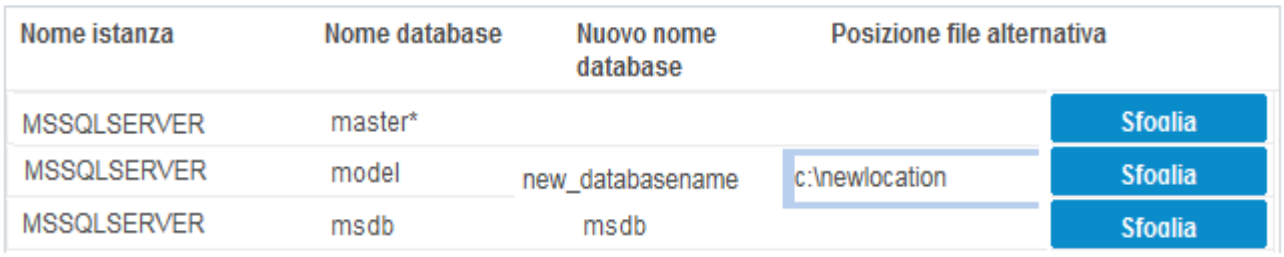
   Solo file di dettagli

   Selezionando questa opzione, l'agente Arcserve UDP (Windows) scarica i file del database Microsoft SQL selezionato nella cartella specificata. Quando si seleziona questa opzione, è possibile specificare o selezionare il percorso della cartella per il ripristino del file di dettagli.



   Ripristina in posizione alternativa

   Esegue il ripristino in un percorso alternativo (diverso dal percorso originale).



I backup possono essere copiati in percorsi di rete, pertanto, possono essere utilizzati da più istanze SQL Server. È possibile eseguire un ripristino di database multiplo (simultaneamente) dal livello di istanza. L'elenco consente di selezionare l'istanza di database e di specificare un nuovo nome di database e un percorso alternativo per il ripristino del database. È inoltre possibile ricercare il percorso alternativo su cui eseguire il ripristino del database.

Il ripristino di applicazioni Microsoft SQL Server su una posizione alternativa presenta alcuni limiti che sarebbe opportuno conoscere. Per ulteriori informazioni, consultare la sezione **Microsoft SQL Server Restore to Alternate Location Considerations** dell'articolo Review the Restore Prerequisites and Considerations.

3. Fare clic su **Avanti**.

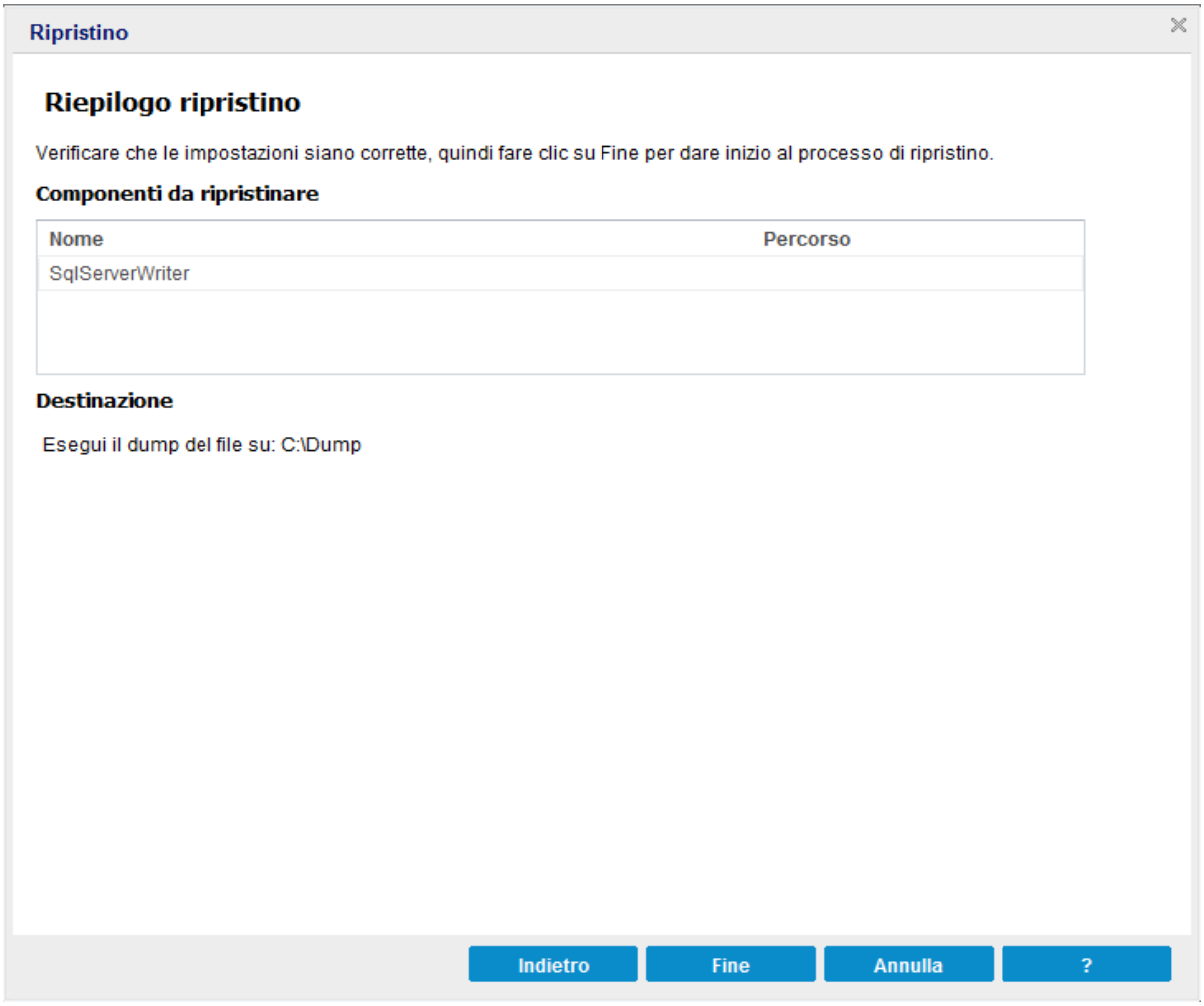
   Verrà visualizzata la finestra di dialogo **Riepilogo ripristino**.

Ripristino dell'applicazione Microsoft SQL Server

Una volta definite le opzioni di ripristino, verificare che le impostazioni siano corrette e confermare il processo di ripristino. Il **riepilogo di ripristino** consente di verificare tutte le opzioni di ripristino definite e, se necessario, modificarle.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Riepilogo ripristino**, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



- Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
- Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

L'applicazione Microsoft SQL Server viene ripristinata.

Verifica del ripristino dell'applicazione Microsoft SQL Server

Effettuare le operazioni seguenti:

1. Accedere alla destinazione di ripristino dell'agente Arcserve UDP (Windows) specificata.

   Ad esempio, se si seleziona il ripristino del database Microsoft SQL Server nella posizione originale in seguito al completamento del ripristino, aprire la posizione fisica per verificare che il database e i registri di Microsoft SQL Server siano stati ripristinati.

   Se si seleziona il ripristino del database di Microsoft SQL Server sulla posizione del file di dettagli, l'agente Arcserve UDP (Windows) eseguirà il ripristino del database di Microsoft SQL Server e lo registrerà su una posizione specifica.

2. Verificare che l'applicazione Microsoft SQL Server sia stata ripristinata, quindi verificare che il database sia stato montato e sia accessibile.

   L'applicazione Microsoft SQL Server viene ripristinata correttamente.

Ripristino da un percorso UNC/NFS

Ogni volta che Arcserve UDP esegue un backup del percorso UNC/NFS, viene eseguito il backup di tutti i file e le cartelle modificati dall'ultimo processo completato correttamente. Questo metodo di ripristino consente di sfogliare i file e le cartelle archiviati e di specificare esattamente i file da ripristinare.

Per eseguire il ripristino da un punto di ripristino, effettuare le seguenti attività:

1. Verifica delle considerazioni e dei prerequisiti di ripristino
2. Definizione di file/directory su un percorso UNC/NFS da ripristinare
    a. Definizione dei file e del contenuto da ripristinare
    b. Definizione delle opzioni di ripristino
3. Ripristino dei file e del contenuto
4. Verifica del corretto ripristino del contenuto

Verifica delle considerazioni e dei prerequisiti di ripristino

Verificare i seguenti prerequisiti prima di procedere al ripristino:

- È necessario disporre di almeno un punto di ripristino per il ripristino.
- È necessario disporre di una destinazione valida e accessibile da cui eseguire il ripristino del contenuto del punto di ripristino.
- È necessario disporre di una posizione di destinazione valida e accessibile dove eseguire il ripristino del punto di ripristino.

Definizione delle informazioni del percorso UNC/NFS da ripristinare

Arcserve UDP include un'opzione per il ripristino dei dati da un percorso UNC/NFS. L'obiettivo di un processo di ripristino è quello di identificare rapidamente i dati necessari e di recuperarli dalla posizione di backup appropriata. Per ciascun processo di ripristino è richiesta un'origine e una destinazione.

Il processo per il ripristino da un percorso UNC/NFS è il seguente:

1. Definizione di file e cartelle e del contenuto da ripristinare
2. Definizione delle opzioni di ripristino

Definizione di file e cartelle UNC/NFS e del contenuto da ripristinare

In questa sezione vengono fornite informazioni su come specificare i file e le cartelle UNC/NFS e il contenuto da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere alla finestra di dialogo per la selezione del metodo di ripristino in uno dei modi seguenti:

   Dalla console Arcserve UDP:

   a. Accedere alla console Arcserve UDP.

   b. Accedere a **Risorse** > **Nodo** > **Tutti i nodi**.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   c. Fare clic con il tasto destro del mouse sul nodo, quindi selezionare **Ripristino**.

      L'utente verrà indirizzato automaticamente alla console del nodo dell'agente e verrà visualizzata la finestra di dialogo Ripristino.

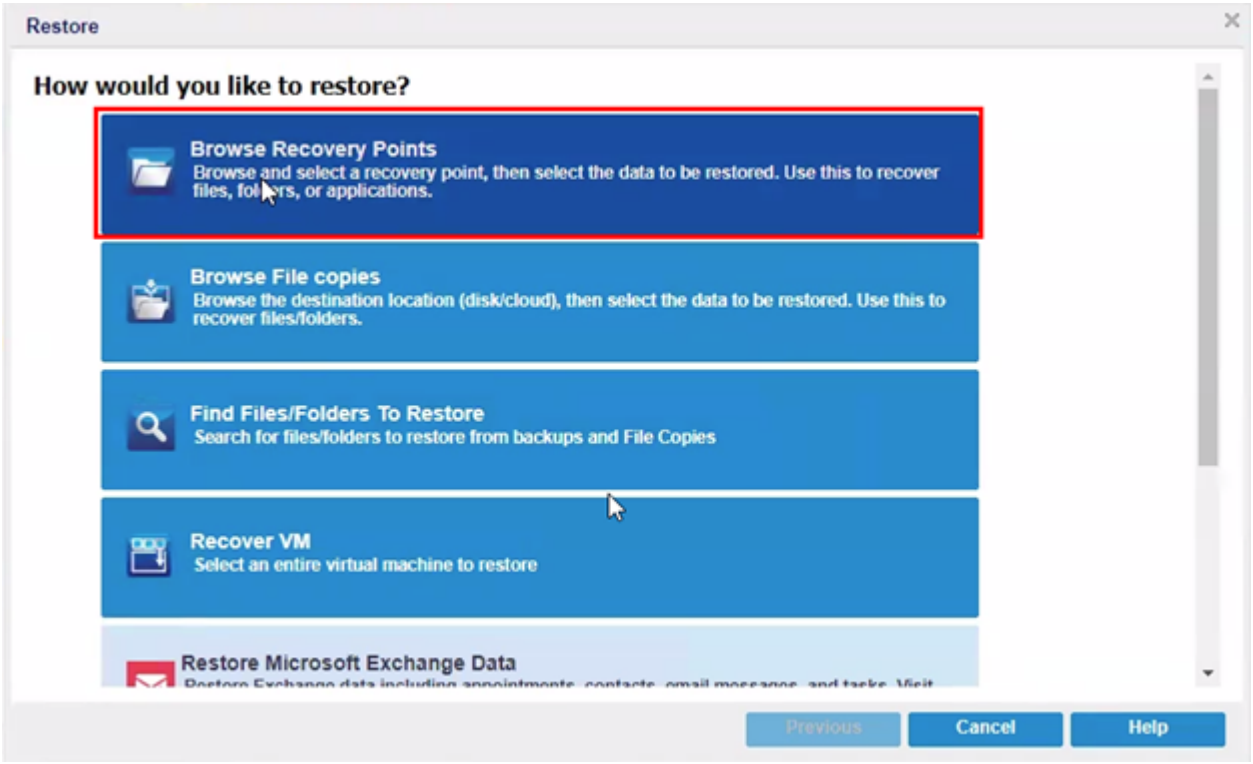
   Dall'agente Arcserve UDP (Windows):

   a. Accedere all'agente Arcserve UDP (Windows).

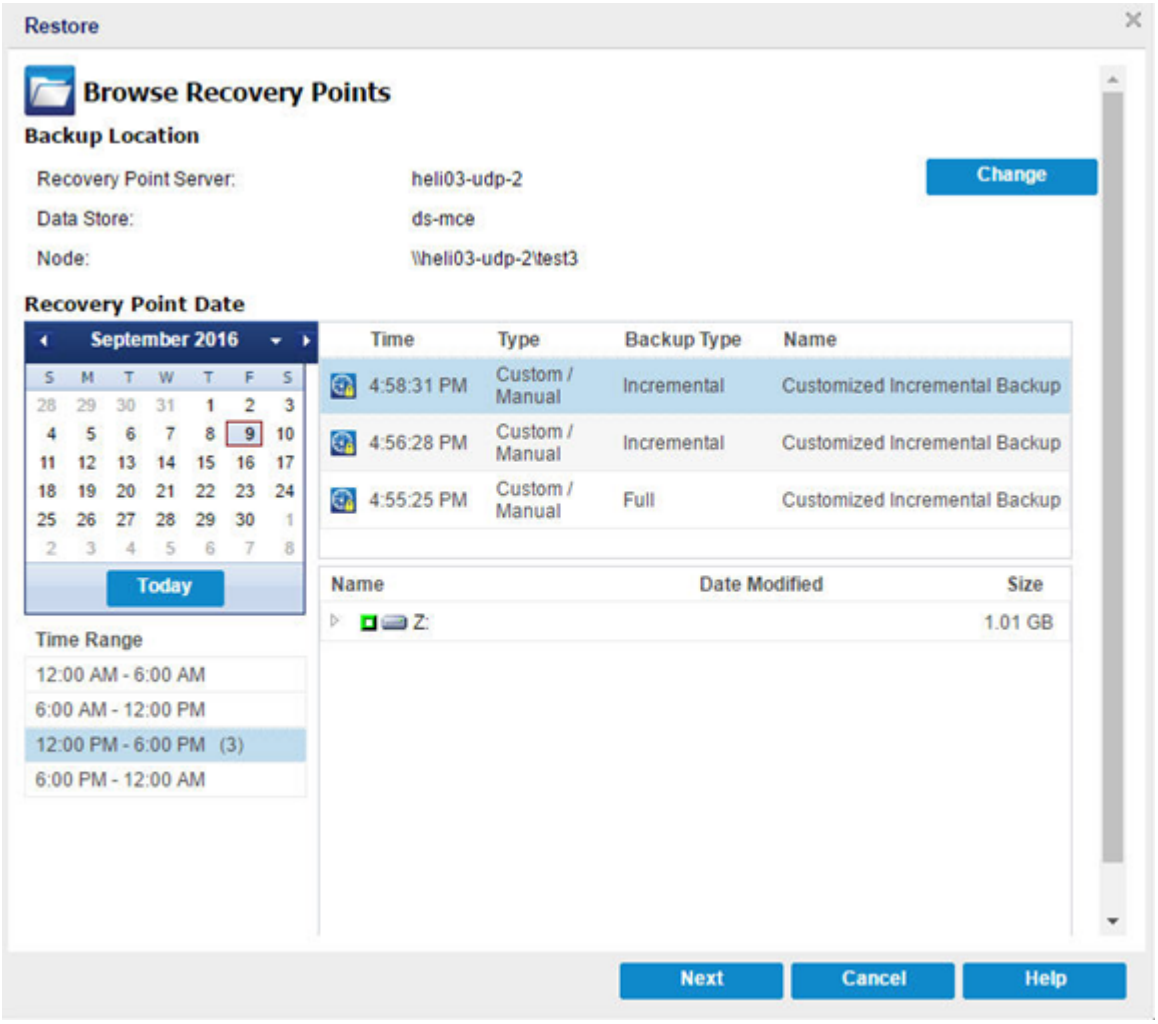
   b. Dalla pagina principale selezionare **Ripristino**.

      Verrà visualizzata la finestra di dialogo di ripristino.

2. Nella finestra di dialogo Ripristino, fare clic su **Sfoglia punti di ripristino**.



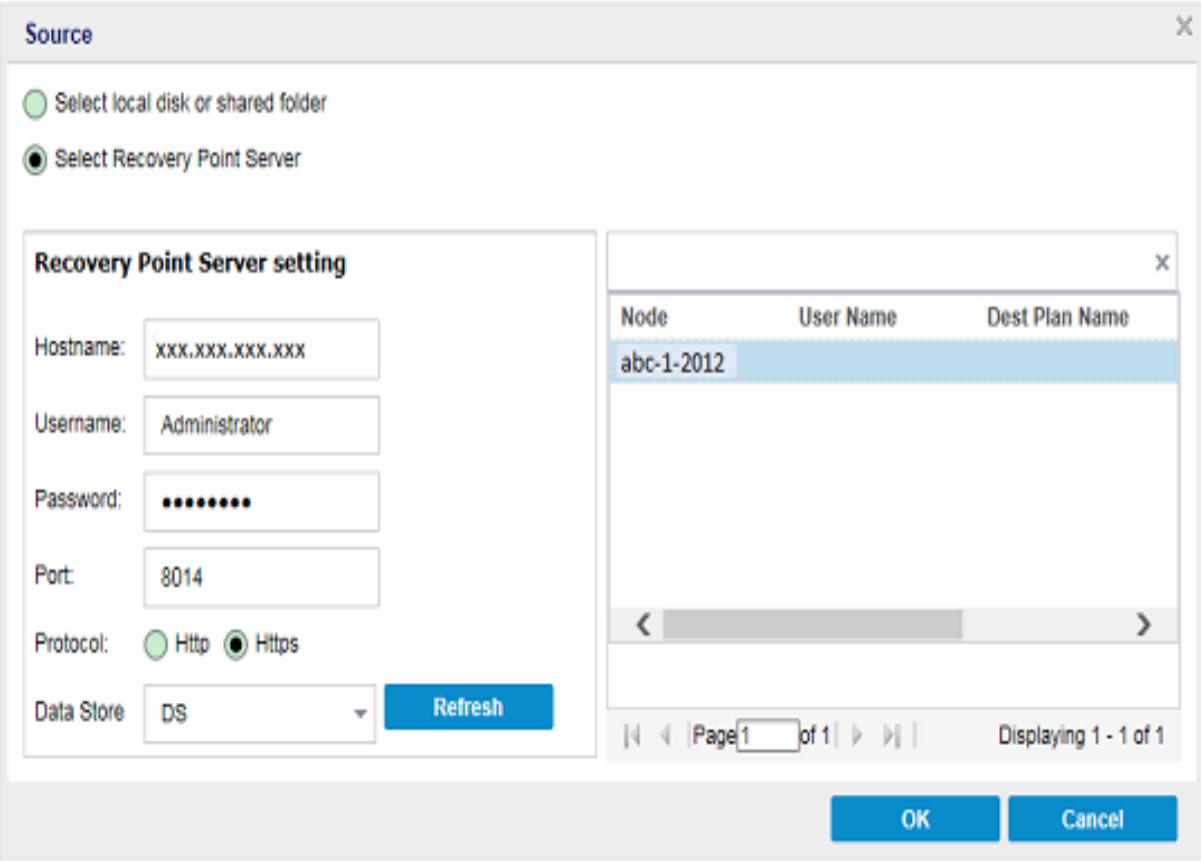
3. Nella pagina Sfoglia punti di ripristino, procedere come segue:



a. Per aggiornare la posizione di backup, fare clic su **Modifica**.

   Viene visualizzata la finestra di dialogo Origine.

b. Nella finestra di dialogo Origine, selezionare una delle seguenti posizioni di backup, quindi fare clic su **OK**:



Selezione di un disco locale o una cartella condivisa

1. Specificare o accedere al percorso di archiviazione delle immagini di backup e selezionare l'origine di backup appropriata.
2. Per verificare la connessione alla posizione specificata, fare clic sul pulsante con una freccia verde. Se necessario, immettere il nome utente e la password per poter accedere alla posizione di origine.

   Viene visualizzata la finestra di dialogo Selezionare la posizione di backup.
3. Selezionare la cartella di archiviazione dei punti di ripristino e fare clic su **OK**.

   La finestra di dialogo Selezionare la posizione di backup viene chiusa e la posizione di backup viene visualizzata nella finestra di dialogo Origine.

   I punti di ripristino vengono elencati nella finestra di dialogo Sfoglia punti di ripristino.

Selezione di un Recovery Point Server

1. Specificare i dettagli dell'impostazione Recovery Point Server e fare clic su **Aggiorna**.

   Tutti gli agenti vengono elencati nella colonna Data Protection Agent (Agente di protezione dati) nella finestra di dialogo Origine.

2. Selezionare l'agente dall'elenco visualizzato.

   I punti di ripristino vengono elencati nella finestra di dialogo Sfoglia punti di ripristino.

c. Selezionare la data dell'immagine di backup che si desidera ripristinare.

   Tutte le date contenenti punti di ripristino per l'origine di backup specificata sono evidenziate in verde.

   Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito (completo, incrementale o di verifica) e al nome del backup.

d. Selezionare un punto di ripristino da ripristinare.

   Viene visualizzato il contenuto di backup (incluse tutte le applicazioni) per i punti di ripristino selezionati.

   Nota: l'icona di un orologio con lucchetto indica che il punto di ripristino contiene informazioni crittografate e potrebbe richiedere una password per il ripristino.

e. Selezionare il contenuto da ripristinare.

   - Per un ripristino a livello di volume, è possibile scegliere di ripristinare l'intero volume oppure alcuni file/cartelle specifici.
   - Per un ripristino a livello di applicazione, è possibile scegliere di ripristinare l'intera applicazione o solo determinati componenti, database, istanze, ecc. dell'applicazione.

4. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

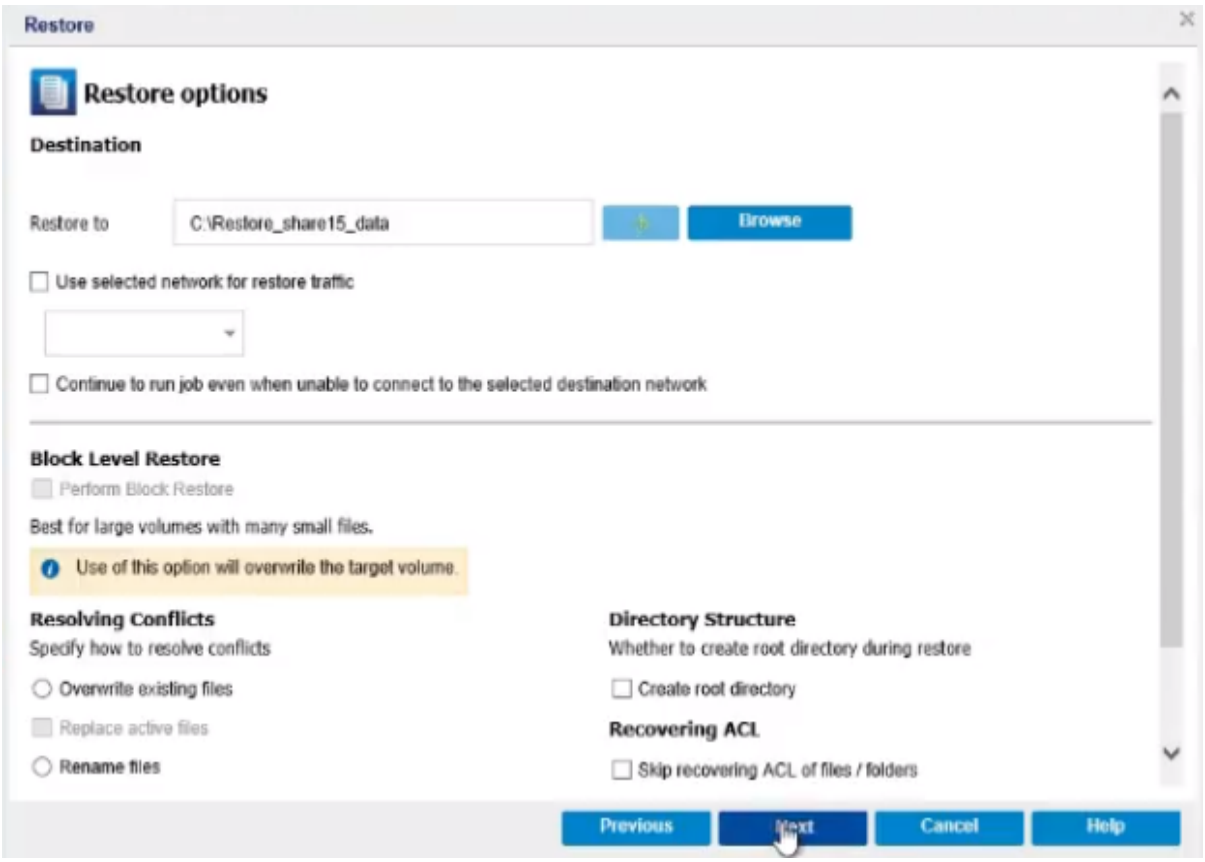
   Il punto di ripristino e il contenuto da ripristinare sono specificati.

Definizione delle opzioni di ripristino

Dopo avere specificato un punto di ripristino e il contenuto da ripristinare, definire le opzioni di copia per il punto di ripristino selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo Opzioni di ripristino, selezionare la destinazione di ripristino.



L'opzione di destinazione disponibile è:

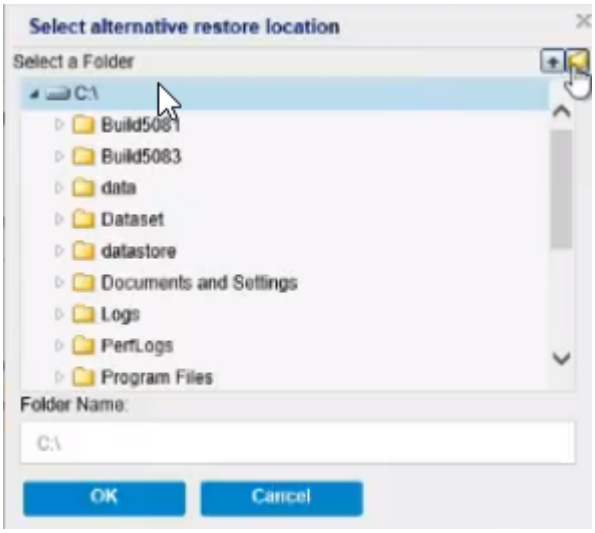
Ripristina su

Esegue il ripristino alla posizione specificata. Per eseguire il ripristino dei dati nella posizione originale, eseguire le seguenti operazioni:

a. Per fornire la destinazione, fare clic su **Sfoglia**.

   Viene visualizzata la finestra di dialogo Seleziona posizione di ripristino alternativa.

b. Selezionare la cartella esistente o crearne una nuova, se necessario, quindi fare clic su **OK**.



c. Per verificare la connessione alla posizione specificata, fare clic sul pulsante con una freccia verde. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso.

Nota: il ripristino da un piano di protezione NFS a una condivisione NFS non è consentito.

2. Per abilitare la comunicazione tra la rete selezionata e il Recovery Point Server, selezionare la casella di controllo **Usa rete selezionata per il traffico di ripristino**, quindi selezionare la rete dall'elenco a discesa.

   Nota: se la rete di backup selezionata non è accessibile, per continuare il processo di backup con la rete disponibile o con la rete predefinita, fare clic sulla casella di controllo **Procedere con l'esecuzione del processo anche nel caso in cui sia impossibile stabilire la connessione alla rete di backup selezionata**.

3. Specificare l'opzione **Risoluzione conflitti** che verrà eseguita da Arcserve UDP in caso di conflitti durante il processo di ripristino.

   Le opzioni disponibili sono:

   Sovrascrivi i file esistenti

   Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dai file di backup, indipendentemente dalla loro presenza sul computer.

   Sostituisci file attivi

   Consente di sostituire i file attivi dopo il riavvio. Se durante il tentativo di ripristino l'agente Arcserve UDP (Windows) rileva che l'utente sta accedendo al file esistente o che quest'ultimo è momentaneamente in uso, tale file non viene sostituito immediatamente. Per evitare l'insorgere di problemi, i file attivi vengono sostituiti al riavvio successivo del computer. (Il ripristino verrà eseguito

immediatamente, ma la sostituzione dei file attivi verrà eseguita con il riavvio successivo).

Questa opzione è disponibile solo se l'opzione **Sovrascrivi i file esistenti** è stata selezionata.

Nota: se l'opzione non è selezionata, tutti i file attivi verranno ignorati durante il processo di ripristino.

Rinomina file

Se il nome file esiste già, consente di creare un nuovo file. Questa opzione consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno quindi ripristinati nel nuovo file.

Ignora file esistenti

Ignora e non sovrascrive (sostituisce) i file esistenti contenuti nella destinazione di ripristino. Solo gli oggetti inesistenti sul computer verranno ripristinati dai file di backup.

Impostazione predefinita: Ignora file esistenti.

4. Per creare una directory principale durante il ripristino, specificare la **struttura della directory**.

Crea directory principale

Se l'immagine di backup acquisita contiene una struttura delle directory principali, Arcserve UDP ricrea la stessa struttura della directory principale nel percorso di destinazione di ripristino.

Se questa opzione non viene selezionata, il file o cartella verrà ripristinato direttamente nella cartella di destinazione.

Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt e C:\Folder1\SubFolder2\B.txt e durante il ripristino è stata specificata la destinazione D:\Restore.

- Se si sceglie di ripristinare i file A.txt e B.txt individualmente, la destinazione dei file ripristinati corrisponderà a D:\Restore\A.txt e D:\Restore\B.txt. La directory principale sopra il livello di file specificato non verrà ricreata.
- Se si sceglie di eseguire il ripristino a partire dal livello SubFolder2, la destinazione dei file ripristinati corrisponderà a D:\Restore\SubFolder2\A.txt e D:\Restore\SubFolder2\B.txt. La directory principale al di sopra del livello di cartella specificato non verrà ricreata.

Se questa opzione è selezionata, verrà ricreato l'intero percorso della directory principale per i file o le cartelle (compreso il nome del volume) nella cartella di destinazione. Se i file o le cartelle da ripristinare appartengono allo stesso

nome del volume, il percorso della directory principale di destinazione non includerà tale nome del volume. Tuttavia, se i file o le cartelle da ripristinare appartengono a diversi nomi di volume, il percorso della directory principale di destinazione includerà il nome del volume.

Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt, C:\Folder1\SubFolder2\B.txt e E:\Folder3\SubFolder4\C.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

- Se si desidera ripristinare soltanto il file A.txt, la destinazione del file ripristinato corrisponderà a D:\Restore\ Folder1\SubFolder2\A.txt (verrà ricreata l'intera directory principale, eccetto il nome del volume).
- Se si esegue il ripristino di entrambi i file A.txt e B.txt, la destinazione dei file ripristinati corrisponderà a D:\Restore\C\Folder1\SubFolder2\A.txt e D:\Restore\E\Folder3\SubFolder4\C.txt (verrà ricreata l'intera directory principale, compreso il nome del volume).

5. Specificare se si desidera che la funzionalità di recupero degli elenchi di controllo ignori il recupero degli elenchi di controllo di file e cartelle.

   Se l'opzione **Ignora recupero elenchi di controllo file/cartelle** è selezionata, vengono ripristinate solo i file e le cartelle di origine. L'attributo dei file o delle cartelle non viene ripristinato, in modo che possano accedervi tutti gli utenti.

   Valore predefinito: esegue il ripristino dei file e delle cartelle di origine con l'attributo Accesso - Elenco di controllo.

6. Se necessario, specificare la **Password di crittografia di backup** nel caso in cui i dati che si desidera ripristinare siano crittografati.

   Se il ripristino viene eseguito dallo stesso computer dell'agente Arcserve UDP (Windows) da cui è stato eseguito il backup crittografato, non è necessario specificare una password. Tuttavia, la password verrà richiesta quando il ripristino viene eseguito da un computer dell'agente Arcserve UDP (Windows) diverso.

   Nota: l'icona di un orologio con lucchetto indica che il punto di ripristino contiene informazioni crittografate e potrebbe richiedere una password per il ripristino.

7. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo Riepilogo ripristino.

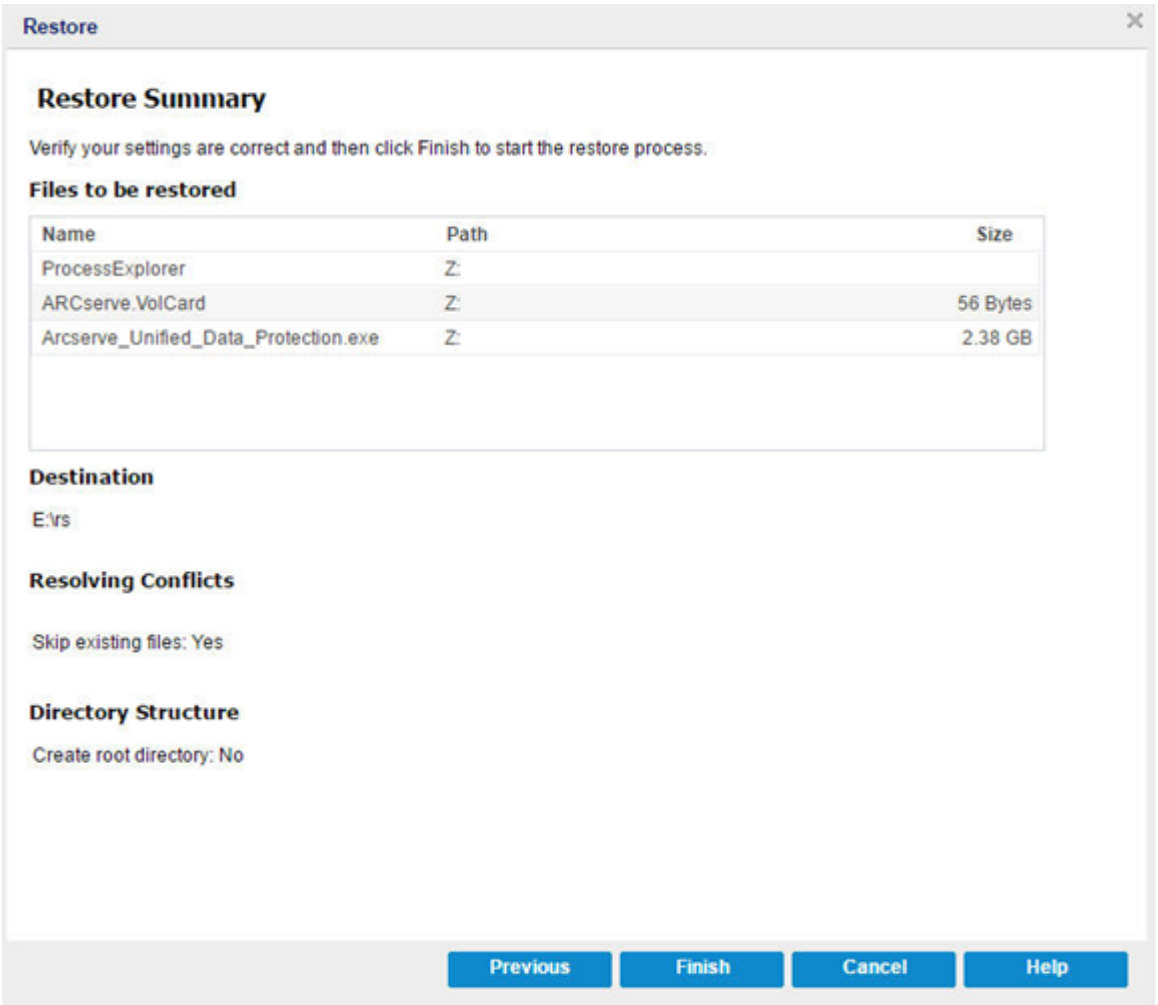
   Le opzioni di ripristino vengono definite per il ripristino da un punto di ripristino.

Ripristino di file e cartelle e del contenuto presente nel percorso UNC/NFS

Una volta definite le opzioni di ripristino, verificare che le impostazioni siano corrette e confermare il processo di ripristino. La pagina Riepilogo di ripristino consente di verificare tutte le opzioni di ripristino definite e, se necessario, modificarle.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo Riepilogo ripristino, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



2. Eseguire una delle seguenti operazioni:
   - Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.

- Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

Il contenuto del punto di ripristino viene ripristinato.

Verifica del corretto ripristino del contenuto

Al completamento del processo di ripristino, verificare che tutti i nodi siano stati ripristinati sul nodo di destinazione. Selezionare la **Cronologia processo** e le schede **Registro attività** nel riquadro Stato per monitorare l'avanzamento del processo di ripristino.

Effettuare le operazioni seguenti:

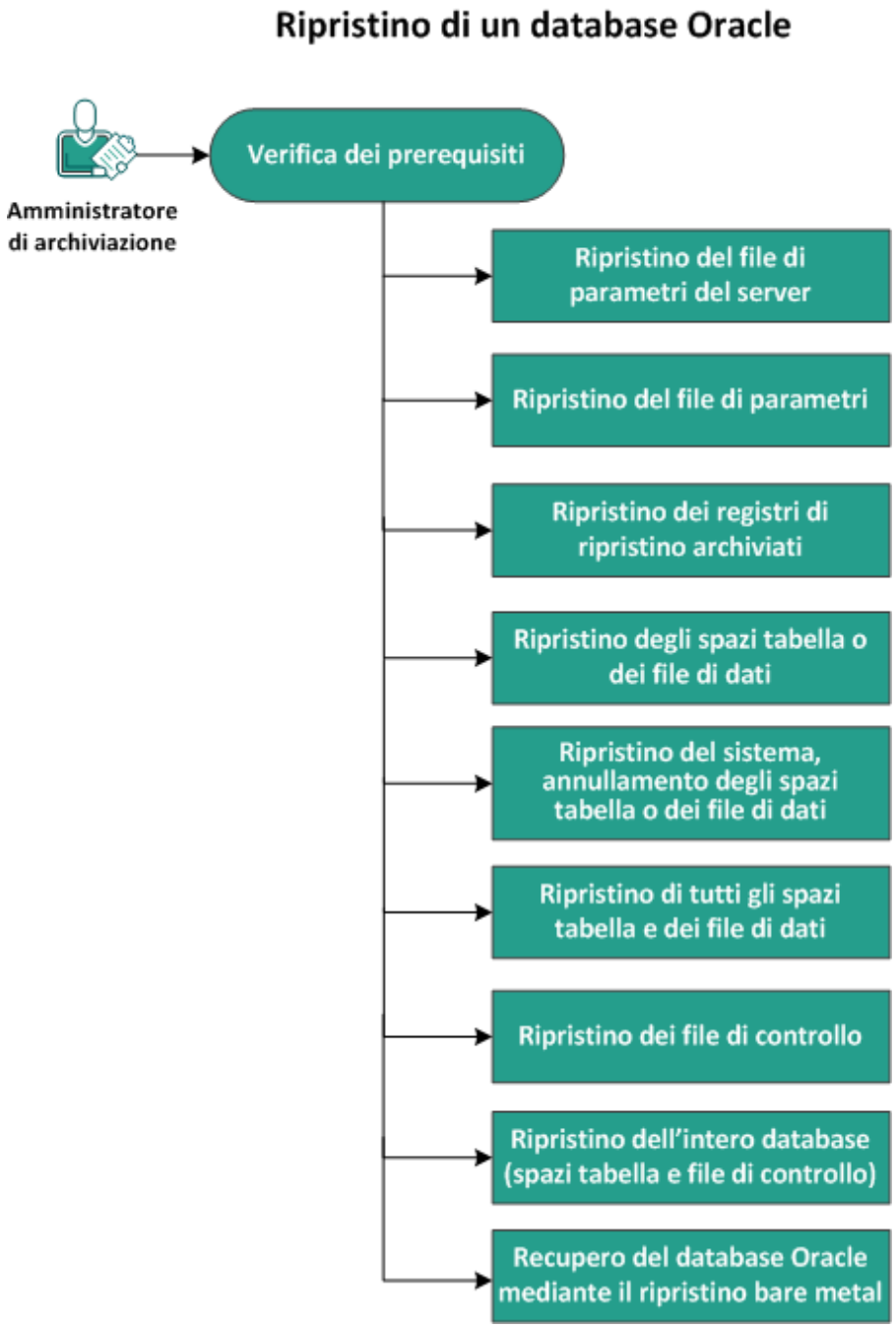
1. Accedere al computer di destinazione su cui sono stati ripristinati i dati.
2. Verificare che i dati obbligatori del punto di ripristino vengano ripristinati.

   Il contenuto ripristinato è stato verificato correttamente.

Ripristino di un database Oracle

È possibile ripristinare determinati file e spazi tabella o l'intero database Oracle mediante la procedura guidata di ripristino. Per ripristinare un database Oracle, individuare i file o lo spazio tabella sul nodo di destinazione. Seguire quindi la procedura guidata per ripristinarli.

Il diagramma seguente illustra la procedura per ripristinare il database Oracle:



Completare le attività seguenti per ripristinare un database Oracle:

- Verifica dei prerequisiti
- Ripristino del file dei parametri per il server
- Ripristino del file dei parametri
- Ripristino dei registri di ripristino archiviati
- Ripristino di spazi tabella o file di dati
- Ripristino di file di sistema, spazi tabella UNDO o file di dati
- Ripristino di tutti gli spazi tabella e i file di dati
- Ripristino dei file di controllo
- Ripristino del database intero (spazi tabella e file di controllo)
- Recupero del database Oracle mediante il ripristino bare metal

Verifica delle considerazioni e dei prerequisiti

Verificare i prerequisiti seguenti prima di ripristinare il database Oracle:

- Il writer Oracle VSS sul nodo di backup funziona correttamente. Se il writer Oracle VSS non funziona correttamente, viene riportato un messaggio di avviso nel registro attività associato al processo di backup.
- È presente un punto di ripristino valido.
- Per evitare qualsiasi errore di ripristino, si consiglia di salvare una copia duplicata dei file di sistema prima di sovrascrivere i file originali.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Ripristino del file dei parametri per il server

Il file dei parametri per il server è un repository dei parametri di inizializzazione. È necessario individuare il file prima del ripristino. Una volta individuato, verificare che lo stato del database sia Open.

Effettuare le operazioni seguenti:

1. Accedere al computer in cui ripristinare i file.
2. Individuare il file dei parametri per il server mediante il comando seguente:

   SQL> SHOW PARAMETER SPFILE;
3. Arrestare il database o l'istanza di Oracle prima di iniziare il processo di ripristino:

   SQL> SHUTDOWN IMMEDIATE;
4. Accedere alla console Arcserve UDP.
5. Ripristinare il file dei parametri per il server mediante la procedura guidata. Per ulteriori informazioni sul processo di ripristino, consultare la sezione Ripristino da un punto di ripristino.
6. Accedere al computer di destinazione.
7. Esplorare le cartelle specifiche e verificare che i file siano stati ripristinati.
8. Connettersi a SQL*Plus per riavviare l'istanza di Oracle con il file dei parametri per il server ripristinato.

   Il file dei parametri per il server è stato ripristinato.

Ripristino del file dei parametri

Il file dei parametri include l'elenco dei parametri di inizializzazione e dei valori per ogni parametro. È necessario individuare il file prima del ripristino. Una volta individuato, verificare che lo stato del database sia Open.

Effettuare le operazioni seguenti:

1. Accedere al computer in cui ripristinare i file.
2. Individuare il file dei parametri (pfile).

   Generalmente, pfile (INIT<SID>.ORA) si trova nella directory %ORACLE_HOME/-database. È possibile digitare "INIT<SID>.ORA" per individuare tale file.
3. Arrestare il database o l'istanza di Oracle prima di iniziare il processo di ripristino:

   SQL> SHUTDOWN IMMEDIATE;
4. Accedere alla console Arcserve UDP.
5. Ripristinare il file dei parametri mediante la procedura guidata. Per ulteriori informazioni sul processo di ripristino, consultare la sezione Ripristino da un punto di ripristino.
6. Accedere al computer di destinazione.
7. Esplorare le cartelle specifiche e verificare che i file siano stati ripristinati.
8. Connettersi a SQL*Plus per riavviare l'istanza di Oracle con il file dei parametri ripristinato.

   Il file dei parametri è stato ripristinato.

Ripristino dei registri di ripristino archiviati

I registri di ripristino archiviati vengono utilizzati per recuperare un database o aggiornare un database di standby. È necessario individuare il file prima del ripristino. Una volta individuato, verificare che lo stato del database sia Open.

Effettuare le operazioni seguenti:

1. Accedere al computer in cui ripristinare i file.
2. Individuare i registri di ripristino archiviati mediante il comando seguente.

   SQL> ARCHIVE LOG LIST;

   SQL> SHOW PARAMETER DB_RECOVERY_FILE_DEST;
3. Accedere alla console Arcserve UDP.
4. Ripristinare i registri di ripristino archiviati mediante la procedura guidata. Per ulteriori informazioni sul processo di ripristino, consultare la sezione Ripristino da un punto di ripristino.
5. Accedere al computer di destinazione.
6. Esplorare le cartelle specifiche e verificare che i registri di ripristino archiviati siano stati ripristinati.

   Il ripristino è stato completato.

Ripristino di spazi tabella o file di dati

È possibile ripristinare lo spazio tabella o i file di dati. È necessario individuare il file prima del ripristino. Una volta individuato, verificare che lo stato del database sia Open. Se il database è aperto, utilizzare l'istruzione ALTER TABLESPACE. Utilizzare OFFLINE per rendere gli spazi tabella o i file di dati non in linea prima di iniziare il processo di ripristino.

Effettuare le operazioni seguenti:

1. Accedere al computer in cui ripristinare gli spazi tabella o i file di dati.
2. Individuare gli spazi tabella o i file di dati dell'utente mediante il comando seguente:

   SQL> SELECT FILE_NAME, TABLESPACE_NAME FROM DBA_DATA_FILES;
3. Modificare lo stato del database in Mount, Nomount o Shutdown prima di ripristinare gli spazi tabella o i file di dati.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Accedere alla console Arcserve UDP.
5. Ripristinare gli spazi tabella o i file di dati mediante la procedura guidata. Per ulteriori informazioni sul processo di ripristino, consultare la sezione Ripristino da un punto di ripristino.
6. Accedere al computer di destinazione.
7. Esplorare le cartelle specifiche e verificare che gli spazi tabella o i file di dati siano stati ripristinati.
8. Recuperare lo spazio tabella o i file di dati.
   - Per recuperare uno spazio tabella, digitare il comando seguente nella schermata di prompt SQL*Plus:

     SQL> RECOVER TABLESPACE "tablespace_name";
   - Per recuperare un file di dati, digitare il comando seguente nella schermata di prompt SQL*Plus:

     SQL> RECOVER DATAFILE 'path';

   Oracle cerca i file di registro di ripristino archiviati da applicare e mostra i nomi dei file in sequenza.
9. Immettere AUTO nella schermata di prompt SQL*Plus per applicare i file.

I dati di registro vengono applicati da Oracle per ripristinare i file di dati. Una volta completata questa operazione, viene visualizzato il messaggio seguente:

Applying suggested logfile

Log applied

Al termine dell'applicazione di ciascun registro, Oracle passa al file di registro successivo fino al completamento dell'operazione di recupero.

10. Digitare il comando seguente per portare lo spazio tabella in linea:

    SQL> ALTER TABLESPACE "tablespace_name" ONLINE;

    È stato recuperato fino all'ultimo file di registro disponibile dello spazio tabella.

Ripristino del sistema o annullamento degli spazi tabella o dei file di dati

È possibile ripristinare i file di sistema o gli spazi tabella UNDO o i file di dati. È necessario individuare il file prima del ripristino. Una volta individuato, verificare che lo stato del database sia Open.

Effettuare le operazioni seguenti:

1. Accedere al computer in cui ripristinare i file di sistema, gli spazi tabella UNDO o i file di dati.
2. Individuare gli spazi tabella o i file di dati dell'utente mediante il comando seguente:

   SQL> SELECT TABLESPACE_NAME, FILE_NAME FROM DBA_DATA_FILES;
3. Modificare lo stato del database in Mount, Nomount o Shutdown prima di ripristinare gli spazi tabella o i file di dati.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Accedere alla console Arcserve UDP.
5. Ripristinare gli spazi tabella o i file di dati mediante la procedura guidata. Per ulteriori informazioni sul processo di ripristino, consultare la sezione Ripristino da un punto di ripristino.
6. Accedere al computer di destinazione.
7. Esplorare le cartelle specifiche e verificare che i file di sistema, gli spazi tabella UNDO o i file di dati siano stati ripristinati.
8. Recuperare lo spazio tabella o i file di dati.
   - Per recuperare uno spazio tabella, digitare il comando seguente nella schermata di prompt SQL*Plus:

     SQL> RECOVER TABLESPACE "tablespace_name";
   - Per recuperare un file di dati, digitare il comando seguente nella schermata di prompt SQL*Plus:

     SQL> RECOVER DATAFILE 'path';

   Oracle cerca i file di registro di ripristino archiviati da applicare e mostra i nomi dei file in sequenza.
9. Immettere AUTO nella schermata di prompt SQL*Plus per applicare i file.

I dati di registro vengono applicati da Oracle per ripristinare i file di dati. Una volta completata questa operazione, viene visualizzato il messaggio seguente:

Applying suggested logfile

Log applied

Al termine dell'applicazione di ciascun registro, Oracle passa al file di registro successivo fino al completamento dell'operazione di recupero.

10. Digitare il comando seguente per portare lo spazio tabella in linea:

    SQL> ALTER TABLESPACE "tablespace_name" ONLINE;

    È stato recuperato fino all'ultimo file di registro disponibile dello spazio tabella.

Ripristino di tutti gli spazi tabella e i file di dati

È possibile ripristinare tutti gli spazi tabella e i file di dati. È necessario individuare il file prima del ripristino. Una volta individuato, verificare che lo stato del database sia Open. Se il database è aperto, utilizzare l'istruzione ALTER TABLESPACE. OFFLINE per rendere gli spazi tabella o i file di dati non in linea prima di iniziare il processo di ripristino.

Effettuare le operazioni seguenti:

1. Accedere al computer in cui ripristinare gli spazi tabella o i file di dati.
2. Individuare gli spazi tabella o i file di dati dell'utente mediante il comando seguente:

   SQL> SELECT FILE_NAME, TABLESPACE_NAME FROM DBA_DATA_FILES;
3. Modificare lo stato del database in Mount, Nomount o Shutdown prima di ripristinare gli spazi tabella o i file di dati.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Accedere alla console Arcserve UDP.
5. Ripristinare gli spazi tabella o i file di dati mediante la procedura guidata. Per ulteriori informazioni sul processo di ripristino, consultare la sezione Ripristino da un punto di ripristino.
6. Accedere al computer di destinazione.
7. Esplorare le cartelle specifiche e verificare che gli spazi tabella o i file di dati siano stati ripristinati.
8. Recuperare il database.

   SQL> RECOVER DATABASE;

   Oracle cerca i file di registro di ripristino archiviati da applicare e mostra i nomi dei file in sequenza.
9. Immettere AUTO nella schermata di prompt SQL*Plus per applicare i file.

   I dati di registro vengono applicati da Oracle per ripristinare i file di dati. Una volta completata questa operazione, viene visualizzato il messaggio seguente:

   Applying suggested logfile

   Log applied

Al termine dell'applicazione di ciascun registro, Oracle passa al file di registro successivo fino al completamento dell'operazione di recupero.

Nota: Se in Oracle viene restituito un messaggio di errore ad indicare che è impossibile aprire il file di registro, è possibile che tale file non sia disponibile. In tali casi, eseguire il ripristino dei supporti incompleto per recuperare di nuovo il database. Una volta applicati tutti i file di registro, il recupero del database è completato. Per ulteriori informazioni sul ripristino dei supporti incompleto, consultare la documentazione Oracle.

10. Digitare il comando seguente per portare il database in linea:

    SQL> ALTER DATABASE OPEN;

    È stato recuperato fino all'ultimo file di registro disponibile del database.

    Nota: Se si esegue un ripristino dei supporti incompleto, digitare il comando seguente per modificare lo stato del database in aperto:

    SQL> ALTER DATABASE OPEN RESETLOGS;

Ripristino dei file di controllo

È possibile ripristinare i file di controllo archiviati dalla struttura fisica del database. È necessario individuare il file prima del ripristino. Una volta individuato, verificare che lo stato del database sia Open.

Effettuare le operazioni seguenti:

1. Accedere al computer in cui ripristinare i file di controllo.
2. Individuare tali file mediante il comando seguente:

   SQL> SHOW PARAMETER CONTROL FILES;
3. Modificare lo stato del database in Nomount o in Shutdown prima del ripristino dei file di controllo.

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Accedere alla console Arcserve UDP.
5. Ripristinare il file di controllo mediante la procedura guidata di ripristino. Per ulteriori informazioni sul processo di ripristino, consultare la sezione Ripristino da un punto di ripristino.
6. Accedere al computer di destinazione.
7. Esplorare le cartelle specifiche e verificare che i file di controllo siano stati ripristinati.
8. Montare il database per iniziare il relativo ripristino:

   SQL> STARTUP MOUNT
9. Digitare il comando RECOVER con la clausola USING BACKUP CONTROLFILE.

   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE

   Il processo di ripristino del database viene avviato.
10. (Facoltativo) Specificare la clausola UNTIL CANCEL per eseguire un ripristino incompleto.

    SQL> RECOVER DATABASE USING BACKUP CONTROLFILE UNTIL CANCEL
11. Applicare i registri archiviati richiesti.

    Nota: Se il registro archiviato richiesto non è disponibile, significa che nei registri di ripristino in linea è contenuto il record di ripristino necessario. Questa situazione si verifica quando nei registri in linea sono presenti modifiche non archiviate in seguito a un errore dell'istanza. È possibile specificare il percorso completo di un

file del registro di ripristino in linea, quindi premere Invio. Per trovare il registro corretto, è possibile che si debba ripetere questa operazione più volte.

12. Digitare il comando seguente per ottenere le informazioni del file di controllo sul registro di ripristino di un database:

    SQL>SELECT * FROM V$LOG;

13. (Facoltativo) Digitare il comando seguente per visualizzare i nomi di tutti i file compresi in un gruppo:

    SQL>SELECT * FROM V$LOGFILE;

    Esempio: Dopo aver applicato i registri archiviati richiesti, è possibile che siano restituiti i messaggi seguenti:

    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. Specificare il percorso completo del file del registro di ripristino in linea e premere Invio.

    Esempio: E:\app\Administrator\oradata\orcl\redo01.log

    Nota: È necessario specificare il percorso completo più volte finché non si individua il registro corretto.

    Vengono visualizzati i messaggi seguenti:

    Log applied

    Media recovery complete

15. Aprire il database con la clausola RESETLOGS una volta completato il processo di ripristino.

    SQL> ALTER DATABASE OPEN RESETLOGS;

    I file di controllo persi sono stati recuperati.

Ripristino del database intero (spazi tabella e file di controllo)

È possibile ripristinare il database intero con tutti gli spazi tabella e i file di controllo. È necessario individuare il file prima del ripristino. Una volta individuato, verificare che lo stato del database sia Open. Se il database è aperto, utilizzare l'istruzione ALTER TABLESPACE. OFFLINE per rendere gli spazi tabella o i file di dati non in linea prima di iniziare il processo di ripristino.

Effettuare le operazioni seguenti:

1. Accedere al computer in cui ripristinare gli spazi tabella o i file di dati.
2. Individuare gli spazi tabella o i file di dati dell'utente mediante il comando seguente:

   SQL> SELECT TABLESPACE_NAME, FILE_NAME from DBA_DATA_FILES;

   SQL> SHOW PARAMETER CONTROL FILES;
3. Modificare lo stato del database in Nomount o in Shutdown prima di ripristinare gli spazi tabella o i file di dati.

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Accedere alla console Arcserve UDP.
5. Ripristinare gli spazi tabella o i file di dati mediante la procedura guidata. Per ulteriori informazioni sul processo di ripristino, consultare la sezione Ripristino da un punto di ripristino.
6. Accedere al computer di destinazione.
7. Esplorare le cartelle specifiche e verificare che gli spazi tabella o i file di dati siano stati ripristinati.
8. Recuperare il database.

   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE UNTIL CANCEL;
9. Applicare i registri archiviati richiesti.

   Nota: Se il registro archiviato richiesto non è disponibile, significa che nei registri di ripristino in linea è contenuto il record di ripristino necessario. Questa situazione si verifica quando nei registri in linea sono presenti modifiche non archiviate in seguito a un errore dell'istanza. È possibile specificare il percorso completo di un file del registro di ripristino in linea, quindi premere Invio. Per trovare il registro corretto, è possibile che si debba ripetere questa operazione più volte.

10. Digitare il comando seguente per ottenere le informazioni del file di controllo sul registro di ripristino di un database:

    SQL>SELECT * FROM V$LOG;

11. (Facoltativo) Digitare il comando seguente per visualizzare i nomi di tutti i file compresi in un gruppo:

    SQL>SELECT * FROM V$LOGFILE;

    Esempio: Dopo aver applicato i registri archiviati richiesti, è possibile che siano restituiti i messaggi seguenti:

    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. Specificare il percorso completo del file del registro di ripristino in linea e premere Invio.

    Esempio: E:\app\Administrator\oradata\orcl\redo01.log

    Nota: È necessario specificare il percorso completo più volte finché non si individua il registro corretto.

    Vengono visualizzati i messaggi seguenti:

    Log applied

    Media recovery complete

13. Aprire il database con la clausola RESETLOGS una volta completato il processo di ripristino.

    SQL> ALTER DATABASE OPEN RESETLOGS;

    Nota: per i database multitenant (CDB/PDB), è necessario aprire anche tutti i database modulari.

    SQL> ALTER PLUGGABLE DATABASE <PDB_NAME> OPEN;

    L'intero database viene ripristinato.

14. Riavviare il server Oracle eseguendo i passaggi da 1 a 13 per i database multitenant.

    Nota: questo passaggio non è necessario per il server che eseguono solo database standalone.

Recupero del database Oracle mediante il ripristino bare metal

Il ripristino bare metal consente di recuperare e ricostruire l'intero sistema informatico in caso di un evento catastrofico. È possibile eseguire il ripristino del computer originale o di un altro computer.

Effettuare le operazioni seguenti:

1. Ripristinare il computer utilizzando uno dei metodi seguenti:
   - Se i punti di ripristino derivano da un backup basato sull'agente, ripristinare il computer mediante ripristino bare metal.
   - Se i punti di ripristino derivano da un backup senza agente basato su host, ripristinare il computer mediante il recupero del computer virtuale.
2. Accedere al computer ripristinato.
3. Aprire il prompt dei comandi e connettersi all'istanza di Oracle (ad esempio ORCL) come sysdba.
4. Verificare lo stato dell'istanza di Oracle.

   SQL> SELECT STATUS FROM V$INSTANCE;
5. Completare uno dei passaggi seguenti a seconda dello stato dell'istanza di Oracle:
   - Se lo stato è Shutdown, avviare e aprire l'istanza.

     SQL> STARTUP;

     SQL> ALTER DATABASE OPEN;
   - Se lo stato è Nomount, montare e aprire l'istanza.

     SQL> ALTER DATABASE MOUNT;

     SQL> ALTER DATABASE OPEN;
   - Se lo stato è Mount, aprire l'istanza di Oracle.

     SQL> ALTER DATABASE OPEN;
6. Ripristino con il comando RECOVER se è necessario eseguire il ripristino dei supporti per il database

   SQL> RECOVER DATABASE;
7. Aprire l'istanza di Oracle una volta completato il ripristino dei supporti.

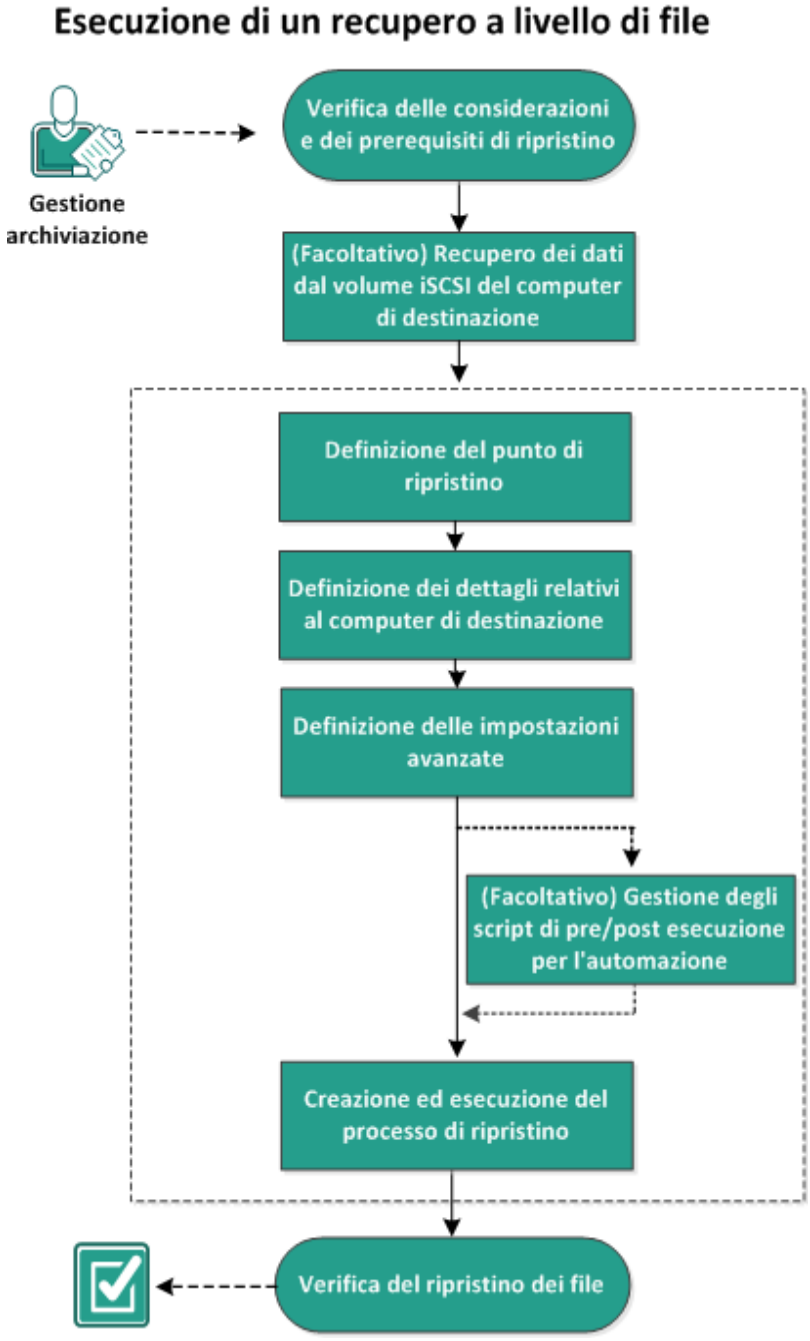
   SQL> ALTER DATABASE OPEN;

   Il database Oracle è stato recuperato mediante il ripristino bare metal.

Esecuzione di un ripristino a livello di file sui nodi Linux

Un recupero a livello di file esegue il ripristino di singoli file e cartelle a partire da un punto di ripristino. È possibile ripristinare un minimo di un file dal punto di ripristino. Questa opzione è utile se si desidera ripristinare i file selezionati e non l'intero punto di ripristino.

Il diagramma seguente mostra il processo di recupero a livello di file:



Eseguire queste attività per un recupero a livello di file:

- Verifica dei prerequisiti di ripristino
- (Facoltativo) Ripristino dei dati dal volume iSCSI nel computer di destinazione
- Definizione del punto di ripristino
- Definizione dei dettagli relativi al computer di destinazione
- Definizione delle impostazioni avanzate
- (Facoltativo) Gestione di pre/post script per l'automazione
- Creazione ed esecuzione del processo di ripristino
- Verifica del ripristino dei file

Verifica dei prerequisiti

Prima di eseguire un recupero a livello di file, è necessario tenere presenti le seguenti considerazioni:

- Si dispone di un punto di ripristino valido e della password di crittografia.
- Si dispone di un nodo di destinazione valido per il recupero dei dati.
- Si è verificato che il server di backup di Linux supporta il file system che si desidera ripristinare.

  Ad esempio, RedHat 7.x non supporta il file system *reiserfs.* Se il sistema operativo del server di backup è RedHat 7.x e si desidera ripristinare il file system reiserfs, è necessario installare il driver del file system per supportare reiserfs. Inoltre, è possibile utilizzare il sistema Live CD dell'Agente Arcserve Unified Data Protection per Linux per il ripristino a livello di file, in quanto il Live CD supporta tutti i tipi di file system.
- Sul server di backup Linux sono stati installati i seguenti pacchetti:
  - mdadm
  - kpartx
  - lvm2
  - Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

(Facoltativo) Ripristino dei dati dal volume iSCSI nel computer di destinazione

Se sono stati archiviati i dati in un volume di destinazione iSCSI, è possibile connettersi al volume iSCSI e ripristinare i dati. Il volume iSCSI consente di gestire i dati e di trasferirli su una rete.

Verificare che nel server di backup sia installata l'ultima versione del software iniziatore di iSCSI. Nei sistemi RHEL, il software iniziatore viene organizzato come iscsi-initiator-utils. Nei sistemi SLES, il software iniziatore viene organizzato come open-iscsi.

Effettuare le operazioni seguenti:

1. Accedere all'ambiente della shell del server di backup.
2. Eseguire uno dei seguenti comandi per avviare il daemon iniziatore di iSCSI.
   - Per i sistemi RHEL:

     /etc/init.d/iscsid start

     Il servizio sui sistemi RHEL è denominato iscsid.
   - Per i sistemi SLES:

     /etc/init.d/open-iscsi start

     Il servizio sui sistemi SLES è denominato open-iscsi.
3. Eseguire uno script di rilevamento per rilevare l'host di destinazione di iSCSI.

   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>

   Il valore predefinito della porta dell'host di destinazione di iSCSI è 3260.
4. Prendere nota del nome completo iSCSI (IQN) dell'host di destinazione di iSCSI rilevato dallo script di rilevamento prima di accedere manualmente alla destinazione individuata.
5. Elencare la periferica a blocchi disponibile del server di backup.

   #fdisk -l
6. Accedere alla destinazione rilevata.

   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l

   È possibile visualizzare una periferica a blocchi nella directory /dev del server di backup.
7. Eseguire il comando seguente per ottenere il nuovo nome della periferica:

#fdisk -l

È possibile visualizzare una periferica aggiuntiva chiamata /dev/sd<x> nel server di backup.

Ad esempio, supporre che il nome della periferica sia /dev/sdc. Tale nome della periferica viene utilizzato per creare una partizione e un file system nelle seguenti fasi.

8. Montare il volume iSCSI utilizzando i comandi seguenti:

   # mkdir /iscsi

   # mount /dev/sdc1 /iscsi

   Nota: Quando si specifica il percorso di sessione nella procedura guidata di ripristino, è necessario selezionare Locale e immette il percorso /iscsi.

   Esempio: <path>/iscsi

9. (Facoltativo) Aggiungere il record seguente al file /etc/fstab in modo che il volume iSCSI si connetta automaticamente al server di backup dopo il riavvio del server.

   /dev/sdc1 /iscsi ext3 _netdev 0 0

   Ora il computer di backup può connettersi al volume iSCSI e può ripristinare i dati in esso contenuti.

Definizione del punto di ripristino per il backup basato sull'agente

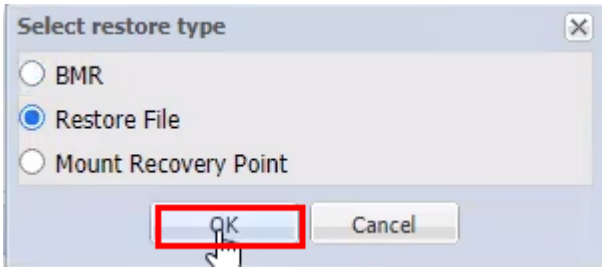
L'esecuzione di un backup implica la creazione di un punto di ripristino. Specificare le informazioni relative al punto di ripristino della Procedura guidata di ripristino, in modo da poter eseguire il ripristino dei dati desiderati. È possibile ripristinare file specifici o tutti i file in base alle proprie esigenze.

Effettuare le operazioni seguenti:

1. Accedere alla procedura guidata di ripristino in uno dei modi seguenti:
   - **Da Arcserve UDP :**
     a. Accedere a Arcserve UDP.
     b. Accedere a **Risorse** > **Nodo** > **Tutti i nodi**.

        Tutti i nodi aggiunti vengono visualizzati nel riquadro centrale.
     c. Fare clic con il tasto destro del mouse sul nodo, quindi selezionare **Ripristino**.

        Vengono visualizzate l'interfaccia Web dell'agente Arcserve UDP (Linux) e la finestra di dialogo Seleziona tipo di ripristino.
     d. Nella finestra di dialogo Seleziona tipo di ripristino, fare clic sull'opzione **Ripristina file**, quindi su **OK**.

        Nota: si accede automaticamente al nodo dell'agente e la Procedura guidata di ripristino viene visualizzata dal nodo dell'agente.
   - **Dall'Agente Arcserve Unified Data Protection per Linux:**
     a. Aprire l'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux.

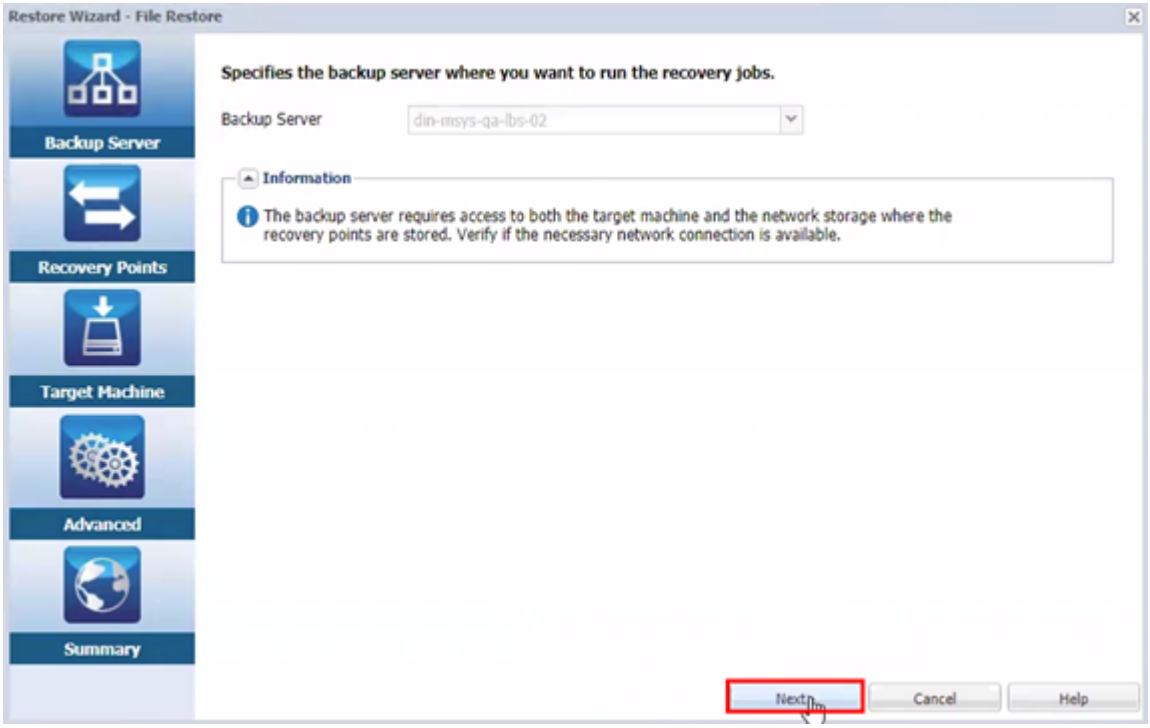
        Nota: durante l'installazione dell'Agente Arcserve Unified Data Protection per Linux, l'URL per l'accesso e la gestione del server

viene fornito all'utente. Accedere ad Agente Arcserve Unified Data Protection per Linux.

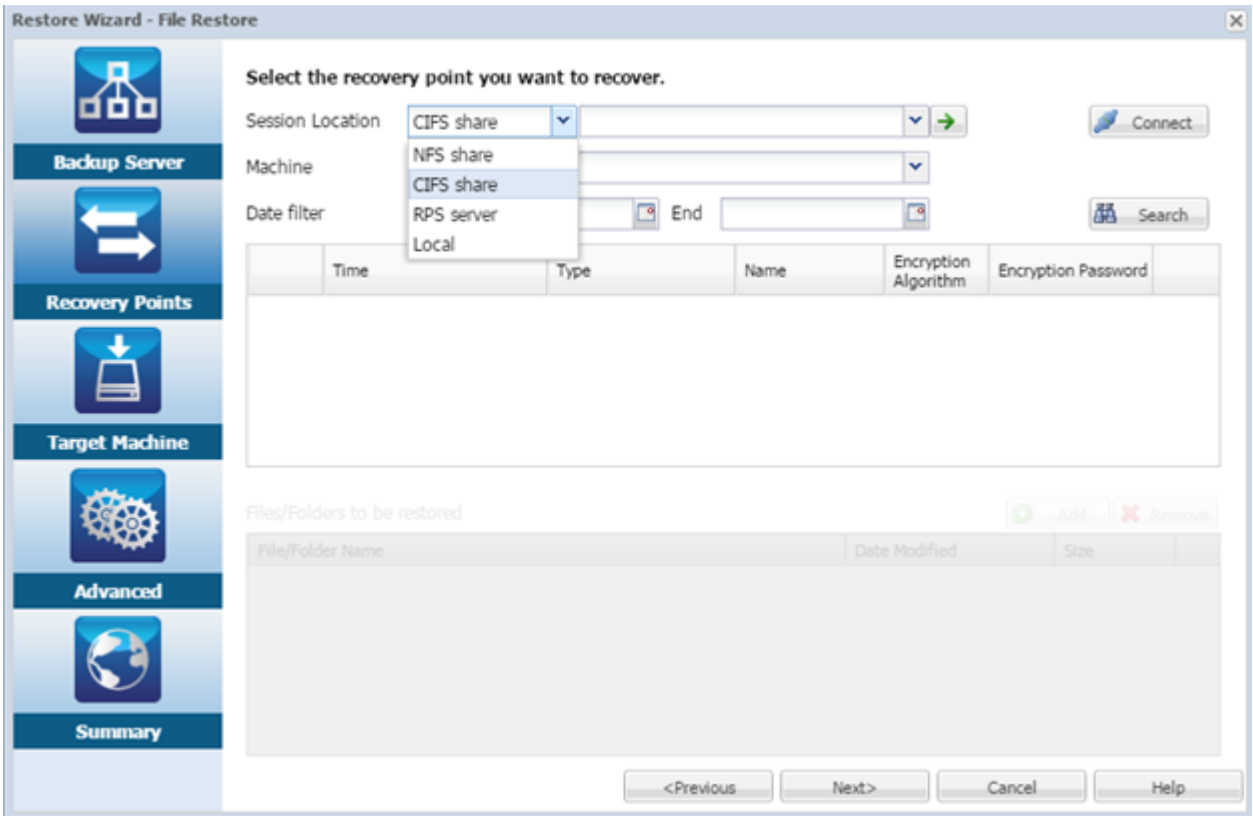
b. Dal menu Procedura guidata, fare clic su **Ripristina**, quindi selezionare **Ripristina file**.

   Viene visualizzata la finestra di dialogo Ripristino guidato - Ripristino file.

2. Nella pagina Server di backup della procedura guidata di ripristino, è possibile visualizzare il server di backup. Non è possibile selezionare alcuna opzione dall'elenco a discesa Server di backup. Fare clic su **Avanti**.



3. Nella pagina Punti di ripristino della procedura guidata di ripristino, eseguire le seguenti operazioni:



Importante! Se la procedura guidata è stata aperta dalla console, vengono visualizzati automaticamente i dettagli della posizione della sessione e del computer. È possibile andare al passaggio 4.

a. Selezionare uno dei seguenti elementi: **Condivisione CIFS/Condivisione NFS/Condivisione RPS/locale** dall'elenco a discesa Percorso di sessione.

b. Eseguire una delle operazioni riportate di seguito in base al percorso della sessione:

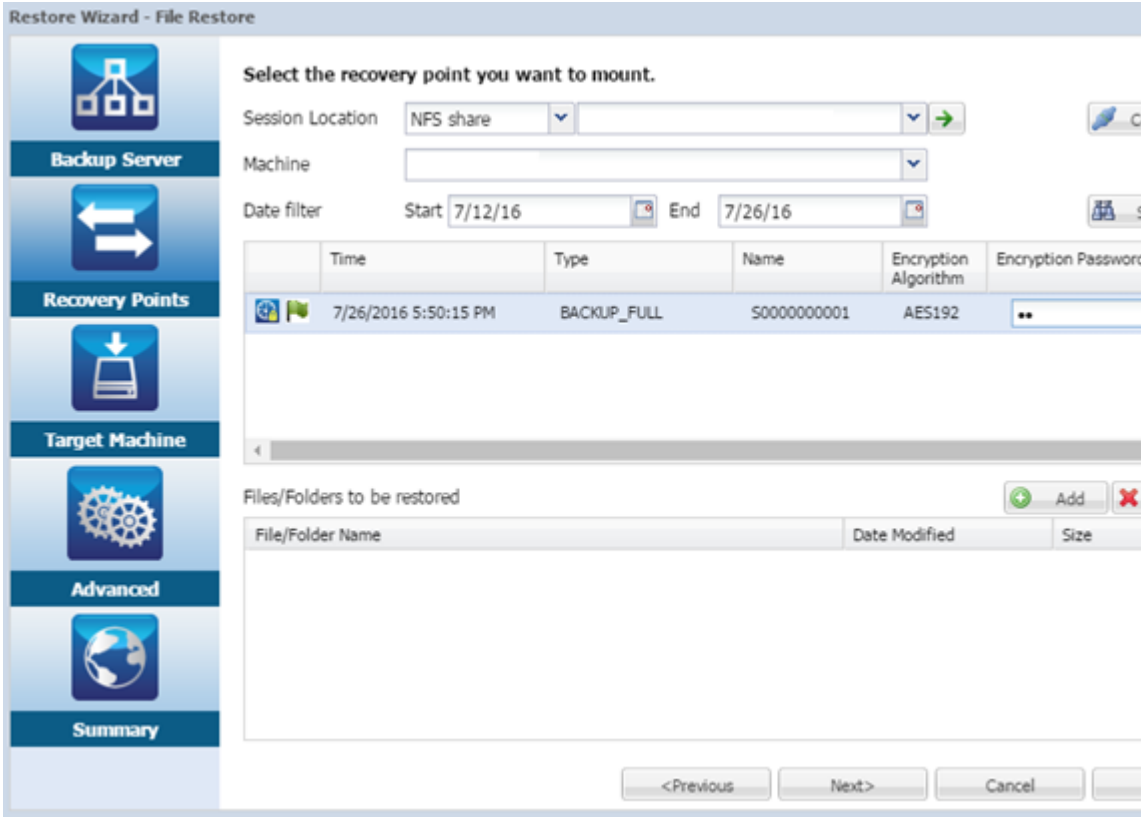
Per condivisione CIFS/condivisione NFS/Locale

Specificare il percorso completo della condivisione CIFS/-condivisione NFS/Locale e fare clic su **Connetti**.

Tutti i computer vengono elencati nell'elenco a discesa Computer.

Nota: se si seleziona l'opzione di **condivisione CIFS**, specificare il

nome utente e la password.



Per il server RPS

a. Selezionare il server RPS, quindi fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo Informazioni sul server del punto di ripristino.

b. Fornire i dettagli RPS e fare clic su **Sì**.

c. Selezionare l'archivio dati dall'elenco a discesa.

   La finestra di dialogo Informazioni sul server del punto di ripristino viene chiusa e viene visualizzata la procedura guidata.

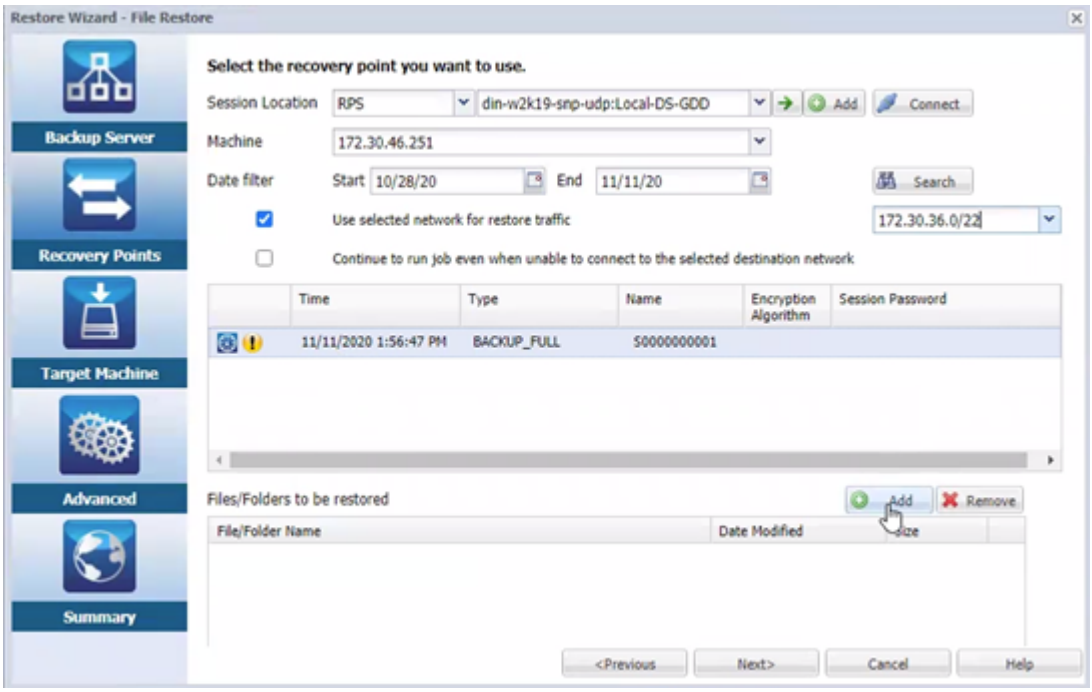
d. Fare clic su **Connetti**.

   Tutti i nodi di cui è stato eseguito il backup per il percorso specificato saranno contenuti nell'elenco a discesa Computer.

e. Dall'elenco a discesa Computer, selezionare il nodo che si desidera ripristinare.

   Verrà creato un elenco contenente tutti i punti di ripristino per il

nodo selezionato.



4. Applicare il filtro data per visualizzare i punti di ripristino generati tra le date specificate e fare clic su **Cerca**.

   Valore predefinito: ultime due settimane.

   Vengono visualizzati tutti i punti di ripristino disponibili tra le date specificate.

5. Per abilitare la comunicazione tra l'agente Linux e il Recovery Point Server, selezionare la casella di controllo **Usa rete selezionata per il traffico di ripristino**, quindi selezionare la rete dall'elenco a discesa.

   Nota: se la rete di backup selezionata non è accessibile, per continuare il processo di backup con la rete disponibile o con la rete predefinita, fare clic sulla casella di controllo **Procedere con l'esecuzione del processo anche nel caso in cui sia impossibile stabilire la connessione alla rete di backup selezionata**.

6. Selezionare il punto di ripristino desiderato. Se il punto di ripristino è crittografato, specificare la password di crittografia per il ripristino dei dati.

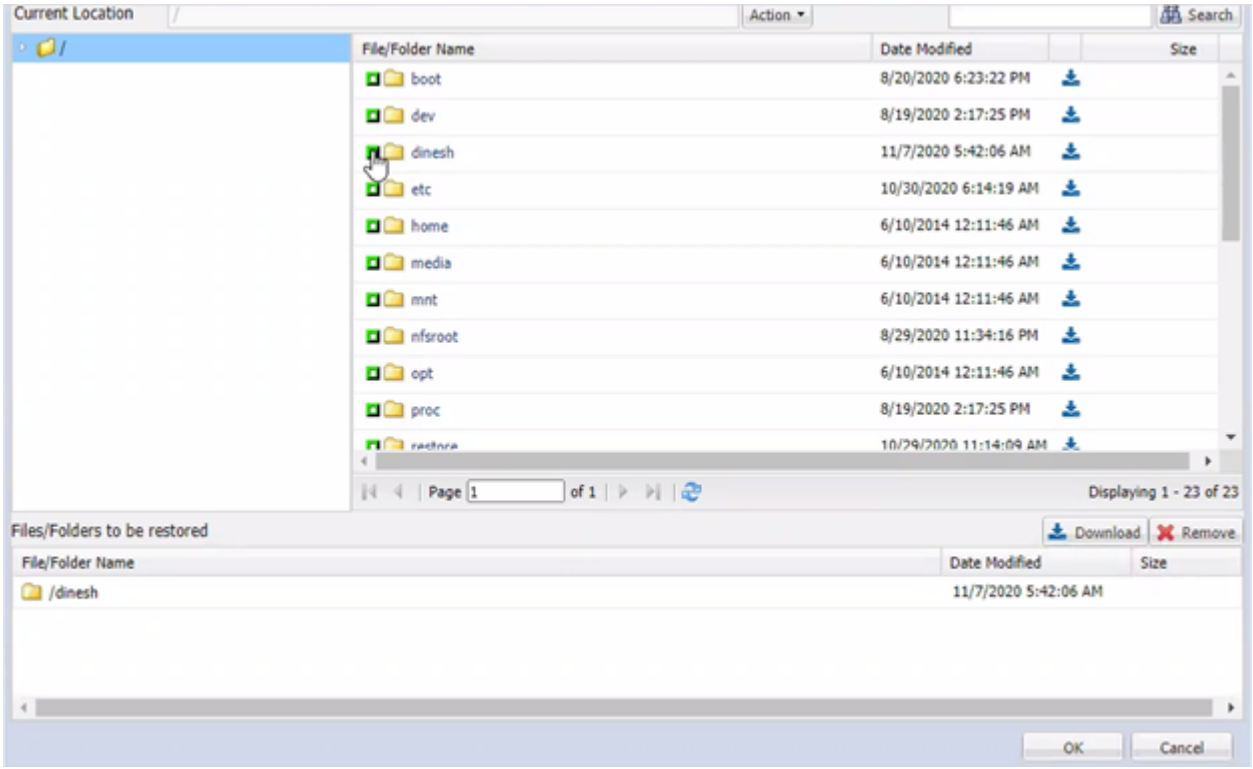
7. Per i file e le cartelle da ripristinare, fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo Sfoglia-<nome nodo>.

   Importante! Se viene visualizzato il messaggio di avviso "I file o le cartelle vengono visualizzati nel file di periferica. Fare clic per ulteriori informazioni." sulla console, facendo riferimento alla nota seguente per la risoluzione.

Nota: Per alcuni layout di disco complessi, viene visualizzato il file system in base al file di periferica. La modifica del comportamento di visualizzazione del file system non influisce sulla funzione di ripristino a livello di file del computer virtuale Linux basato su host. È possibile cercare il file system nel file di periferica. Inoltre, è possibile utilizzare la funzione di ricerca per eseguire la ricerca di un determinato file o una determinata directory.

8. Nella finestra di dialogo Sfoglia-<nome nodo>, selezionare il file o la cartella che si desidera ripristinare, quindi fare clic su **OK**.



Nota: se si esegue la ricerca di un file o una cartella mediante il campo **Cerca**, accertarsi di selezionare la cartella più elevata nella gerarchia. La ricerca viene condotta in tutte le cartelle figlie della cartella selezionata.

La finestra di dialogo Sfoglia <nome nodo> viene chiusa e si verrà reindirizzati alla pagina Punti di ripristino. I file e le cartelle selezionati sono contenuti nell'elenco File/Cartelle da ripristinare.

9. Fare clic su **Avanti**.

   Verrà visualizzata la pagina Computer di destinazione.

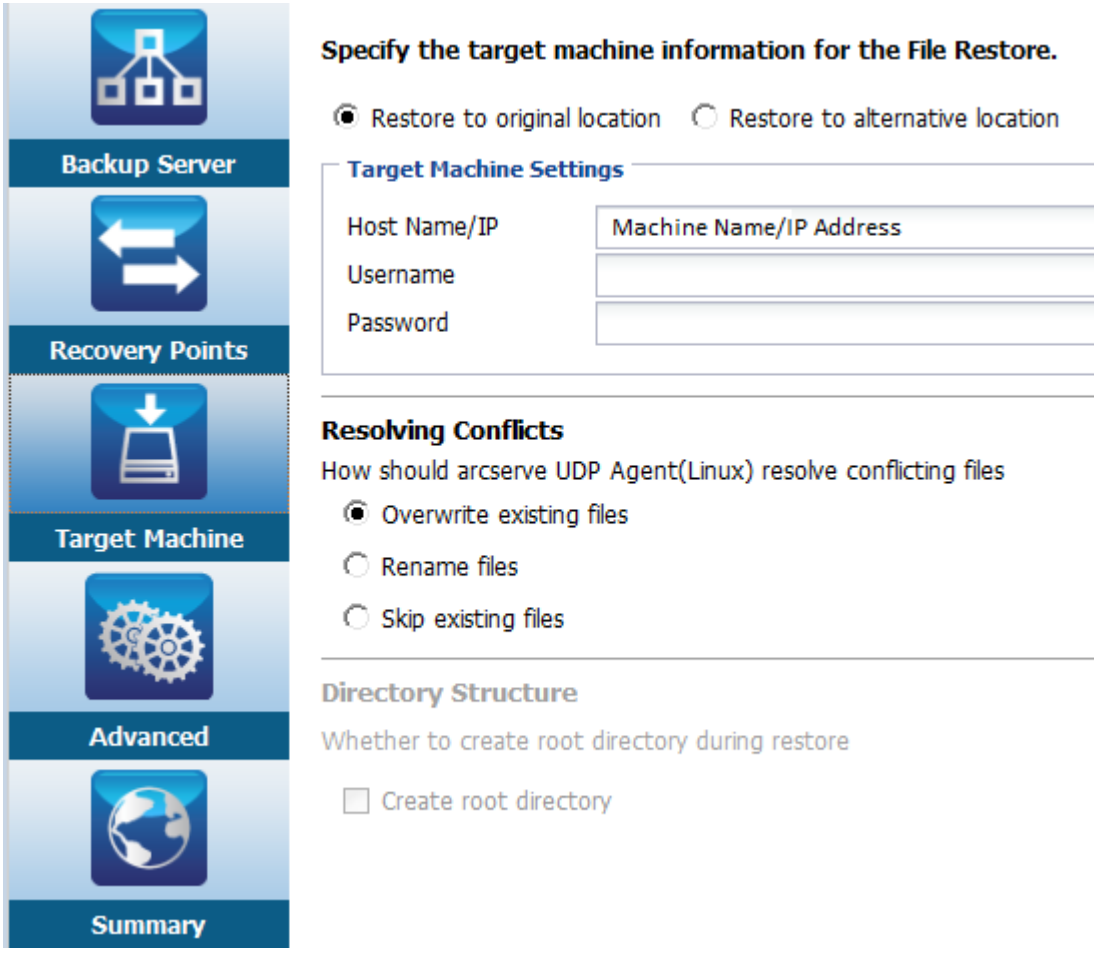
Il punto di ripristino viene specificato.

Definizione dei dettagli relativi al computer di destinazione

Specificare i dettagli relativi al nodo di destinazione in modo che i dati vengano ripristinati su tale computer. È possibile eseguire il ripristino delle cartelle o dei file selezionati sul nodo di origine o su un nuovo nodo.

Per eseguire il ripristino sul nodo di backup dei dati, attenersi alla procedura riportata di seguito:

1. Nella pagina Computer di destinazione selezionare **Ripristina in posizione originale**.



2. Immettere il nome utente e la password del nodo.
3. Per risolvere i file in conflitto, selezionare una delle seguenti opzioni:

   Sovrascrivi i file esistenti

Indica che se il file è presente sul computer di destinazione, il file di backup del punto di ripristino sostituirà il file esistente.

Rinomina file

Specifica che se il file esiste nel computer di destinazione, viene creato un nuovo file con lo stesso nome file e con l'estensione file *.d2d-duplicate<x>*. <x> specifica il numero di volte in cui il file viene ripristinato. Tutti i dati vengono ripristinati nel nuovo file.

Ignora file esistenti

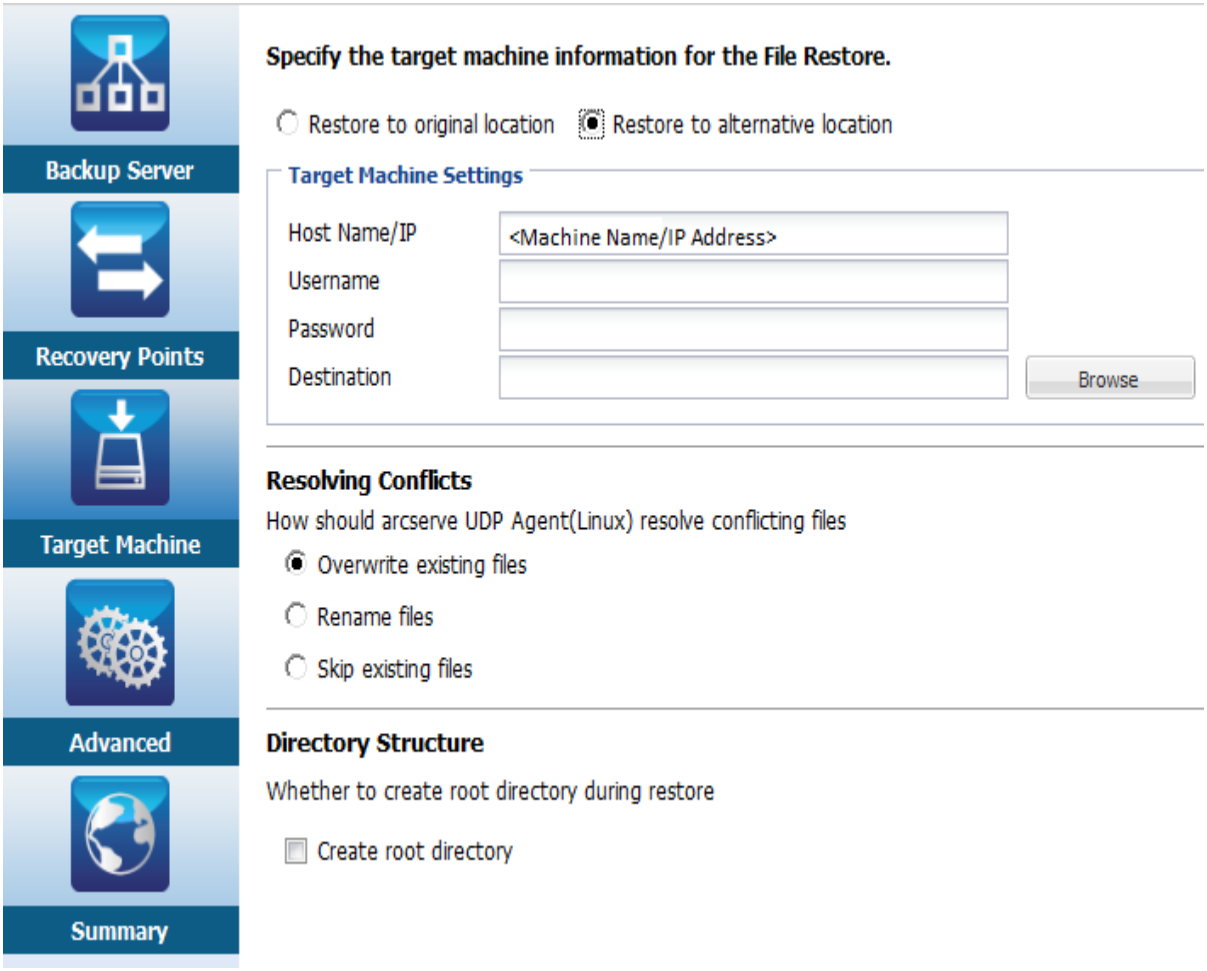
Specifica che se lo stesso file è già presente nel computer di destinazione, il ripristino di tali file non verrà eseguito a partire dal punto di ripristino.

4. (Facoltativo) Selezionare **Crea directory principale**.
5. Fare clic su **Avanti**.

   Viene visualizzata la pagina Impostazioni avanzate.

Per eseguire il ripristino di un nuovo nodo, attenersi alla procedura riportata di seguito:

1. Nella pagina Computer di destinazione selezionare **Ripristina in posizione alternativa**.



2. Immettere il nome host o l'indirizzo IP del nodo di destinazione.
3. Immettere il nome utente e la password del nodo.
4. Immettere il percorso di ripristino dei dati, oppure fare clic su **Sfoglia** per selezionare la cartella di ripristino dei dati, quindi fare clic su **OK**.
5. Per risolvere i file in conflitto, selezionare una delle seguenti opzioni:

   Sovrascrivi i file esistenti

   Indica che se il file è presente sul computer di destinazione, il file di backup del punto di ripristino sostituirà il file esistente.

   Rinomina file

   Specifica che se il file esiste nel computer di destinazione, viene creato un nuovo file con lo stesso nome file e con l'estensione file *.d2d-duplicate<x>*. <x> specifica il numero di volte in cui il file viene ripristinato. Tutti i dati vengono ripristinati nel nuovo file.

   Ignora file esistenti

Specifica che se lo stesso file è già presente nel computer di destinazione, il ripristino di tali file non verrà eseguito a partire dal punto di ripristino.

6. (Facoltativo) Selezionare **Crea directory principale**.
7. Fare clic su **Avanti**.

   Viene visualizzata la pagina Impostazioni avanzate.

Vengono specificati i dettagli relativi al computer di destinazione.

Definizione delle impostazioni avanzate

Specificare le impostazioni avanzate per eseguire un recupero pianificato dei dati. Il recupero pianificato garantisce che i dati vengano recuperati all'ora specificata anche in caso di assenza dell'utente.

Effettuare le operazioni seguenti:

1. Impostare la data e l'ora di inizio selezionando una delle seguenti opzioni:

   Esegui ora

   Avvia il processo di ripristino a livello di file dopo l'invio del processo.

   Imposta data e ora di inizio

   Avvia il processo di ripristino a livello di file nella data e ora specificata dopo l'invio del processo.

2. (Facoltativo) Selezionare **Stima dimensioni del file**.
3. (Facoltativo) Selezionare uno script dall'opzione **Impostazioni pre/post script**.

   Questi script eseguono comandi di script per le azioni da eseguire prima dell'inizio del processo e/o al completamento del processo.

   Nota: i campi **Impostazioni pre/post script** vengono popolati solamente se un file di script è già stato creato e collocato nel percorso seguente:

   /opt/Arcserve/d2dserver/usr/prepost

   Nota: per ulteriori informazioni sulla creazione di pre/post script, consultare la sezione *Gestione di pre/post script per l'automazione*.

4. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Riepilogo**.

   Vengono specificate le impostazioni avanzate.

(Facoltativo) Gestione di pre/post script per l'automazione

Gli script di pre/post esecuzione consentono di eseguire regole di business a intervalli specifici di un processo in esecuzione. È possibile specificare quando eseguire gli script nelle **Impostazioni pre/post script** della **Procedura guidata di backup** e della **Procedura guidata di ripristino** dell'interfaccia utente. È possibile eseguire gli script sul server di backup in base alle impostazioni dell'utente.

La gestione del pre/post script è un processo costituito da due passaggi: la creazione del pre/post script e la sua collocazione nella cartella prepost.

Creazione di pre/post script

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare un file di script mediante le variabili di ambiente nel linguaggio di scripting preferito.

Variabili di ambiente del pre/post script

Per creare lo script, utilizzare le variabili di ambiente seguenti:

D2D_JOBNAME

Indica il nome del processo.

D2D_JOBID

Identifica l'ID del processo. L'ID di processo è un numero attribuito al processo durante la sua esecuzione. Se si esegue lo stesso processo nuovamente, verrà fornito un nuovo numero di processo.

D2D_TARGETNODE

Identifica il nodo di cui viene eseguito il backup o il ripristino.

D2D_JOBTYPE

Identifica il tipo di processo in esecuzione. I valori seguenti identificano la variabile D2D_JOBTYPE:

backup.full

Identifica il processo come backup completo.

backup.incremental

Identifica il processo come backup incrementale.

backup.verify

Identifica il processo come backup di verifica.

restore.bmr

Identifica il processo come ripristino bare metal (BMR). Si tratta di un processo di ripristino.

restore.file

Identifica il processo come ripristino a livello di file. Si tratta di un processo di ripristino.

D2D_SESSIONLOCATION

Identifica la posizione in cui vengono archiviati i punti di ripristino.

D2D_PREPOST_OUTPUT

Identifica un file temp. Il contenuto della prima linea del file temp viene visualizzato nel registro attività.

D2D_JOBSTAGE

Indica la fase del processo. I valori seguenti identificano la variabile D2D_ JOBSTAGE:

pre-job-server

Identifica lo script eseguito sul server di backup prima dell'avvio del processo.

post-job-server

Identifica lo script eseguito sul server di backup dopo il completamento del processo.

pre-job-target

Identifica lo script eseguito sul computer di destinazione prima dell'avvio del processo.

post-job-target

Identifica lo script eseguito sul computer di destinazione dopo il completamento del processo.

pre-snapshot

Identifica lo script eseguito sul computer di destinazione prima dell'acquisizione della snapshot.

post-snapshot

Identifica lo script eseguito sul computer di destinazione dopo l'acquisizione della snapshot.

D2D_TARGETVOLUME

Identifica il volume di cui viene eseguito il backup durante un processo di backup. Questa variabile è adatta per gli script di snapshot di pre/post automazione per un processo di backup.

D2D_JOBRESULT

Identifica il risultato di uno script del processo di post-esecuzione. I valori seguenti identificano la variabile di D2D_JOBRESULT:

success

Identifica il risultato come corretto.

fail

Identifica il risultato come non corretto.

D2DSVR_HOME

Identifica la cartella in cui è installato il server di backup. È possibile applicare la variabile agli script in esecuzione sul server di backup.

Lo script viene creato.

Nota: per tutti gli script, un valore restituito pari a zero indica un'operazione riuscita, mentre un valore restituito diverso da zero indica la presenza di un errore.

Collocare lo script nella cartella prepost ed eseguire la verifica

Tutti gli script di pre/post per un server di backup sono gestiti centralmente dalla cartella prepost nella posizione seguente:

/opt/Arcserve/d2dserver/usr/prepost

Effettuare le operazioni seguenti:

1. Collocare il file nella posizione seguente del server di backup:

   /opt/Arcserve/d2dserver/usr/prepost

2. Fornire le autorizzazioni di esecuzione per il file di script.
3. Accedere all'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux.
4. Aprire la procedura guidata di **backup** o **ripristino** ed accedere alla scheda **Impostazioni avanzate**.
5. Selezionare il file di script nell'elenco del menu a discesa **Impostazioni di pre/post script**, quindi inviare il processo.
6. Fare clic sul **Registro attività** e verificare che lo script venga eseguito per il processo di backup specificato.

Lo script viene eseguito.

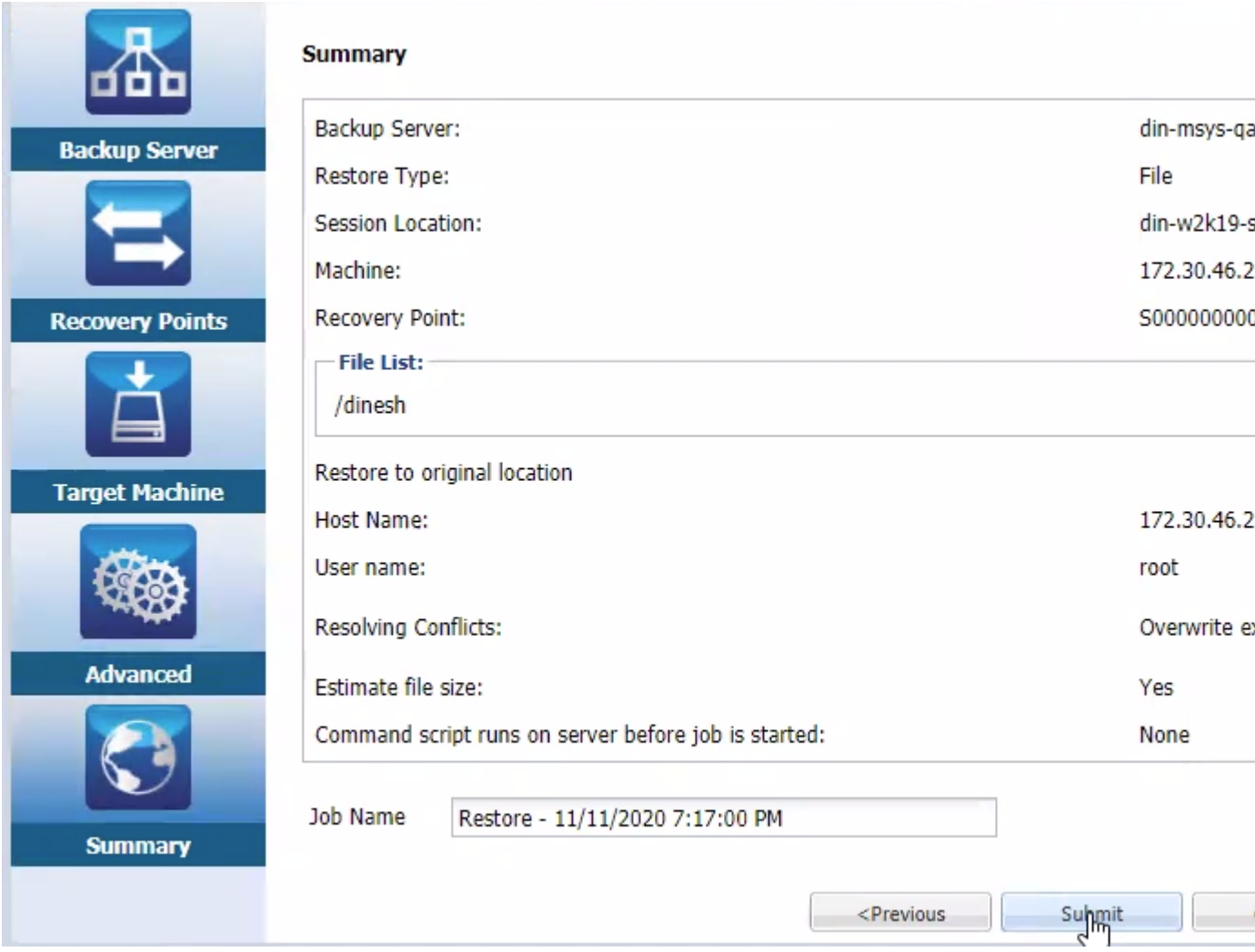
I pre/post script vengono creati correttamente e inseriti nella cartella prevista.

Creazione ed esecuzione del processo di ripristino

Creare e eseguire il processo di ripristino in modo da poter avviare il recupero a livello di file. Verificare le informazioni relative al punto di ripristino prima di eseguire il ripristino dei file. Se necessario, è possibile tornare indietro e modificare le impostazioni di ripristino nella procedura guidata.

Effettuare le operazioni seguenti:

1. Nella pagina Riepilogo della procedura guidata di ripristino, verificare i dettagli del ripristino.



2. Eseguire una delle seguenti operazioni:
   - Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.

- Se le informazioni di riepilogo sono corrette, immettere un nome per il processo, quindi fare clic su **Invia** per avviare il processo di ripristino.

Nota: il campo Nome processo è associato a un nome predefinito. È possibile specificare un nuovo nome per il processo ma non è possibile lasciare il campo vuoto.

La Procedura guidata di ripristino viene chiusa. È possibile visualizzare lo stato del processo nella pagina Stato processo.

Il processo di ripristino viene creato ed eseguito correttamente.

Verifica del ripristino dei file

Al completamento del processo di ripristino, verificare che tutti i nodi siano stati ripristinati sul nodo di destinazione. Selezionare **Cronologia processo** e le schede **Registro attività** nel riquadro **Stato** per monitorare l'avanzamento del processo di ripristino.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione su cui sono stati ripristinati i dati.
2. Verificare che i dati obbligatori del punto di ripristino vengano ripristinati.

   La verifica dei file viene eseguita correttamente.

   Il recupero a livello di file viene eseguito correttamente.

Esecuzione di un ripristino a livello di file da nodi di backup senza agente basati su host per Linux

Un recupero a livello di file esegue il ripristino di singoli file e cartelle a partire da un punto di ripristino. È possibile ripristinare un minimo di un file dal punto di ripristino. Questa opzione è utile se si desidera ripristinare i file selezionati e non l'intero punto di ripristino.

Eseguire queste attività per un recupero a livello di file:

- Verifica dei prerequisiti di ripristino
- Definizione del punto di ripristino
- Definizione dei dettagli relativi al computer di destinazione
- Definizione delle impostazioni avanzate
- (Facoltativo) Gestione di pre/post script per l'automazione
- Creazione ed esecuzione del processo di ripristino
- Verifica del ripristino dei file

Verifica dei prerequisiti

Prima di eseguire un recupero a livello di file, è necessario tenere presenti le seguenti considerazioni:

- Si dispone di un punto di ripristino valido e della password di crittografia.
- Si dispone di un nodo di destinazione valido per il recupero dei dati.
- Si è verificato che il server di backup di Linux supporta il file system che si desidera ripristinare.

  Ad esempio, RedHat 7.x non supporta il file system *reiserfs.* Se il sistema operativo del server di backup è RedHat 7.x e si desidera ripristinare il file system reiserfs, è necessario installare il driver del file system per supportare reiserfs. Inoltre, è possibile utilizzare il Live CD dell'Agente Arcserve Unified Data Protection per Linux per il ripristino a livello di file, in quanto il Live CD supporta tutti i tipi di file system.
- Sul server di backup Linux sono stati installati i seguenti pacchetti:
  - mdadm
  - kpartx
  - lvm2
  - Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Definizione del punto di ripristino

L'esecuzione di un backup implica la creazione di un punto di ripristino. Specificare le informazioni relative al punto di ripristino della **Procedura guidata di ripristino**, in modo da poter eseguire il ripristino dei dati desiderati. È possibile ripristinare file specifici o tutti i file in base alle proprie esigenze.

Effettuare le operazioni seguenti:

1. Accedere alla procedura guidata di ripristino in uno dei modi seguenti:

   Da Arcserve UDP :

   a. Accedere ad Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata l'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux. La finestra di dialogo di selezione del tipo di ripristino viene visualizzata nell'interfaccia utente dell'agente.

   f. Selezionare il tipo di ripristino e fare clic su **OK**.

      Nota: si accede automaticamente al nodo agente e la **Procedura guidata di ripristino** viene visualizzata dal nodo agente.

   Dall'Agente Arcserve Unified Data Protection per Linux:

   a. Aprire l'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux.

      Nota: durante l'installazione dell'Agente Arcserve Unified Data Protection per Linux, l'URL per l'accesso e la gestione del server viene fornito all'utente. Accedere all'Agente Arcserve Unified Data Protection per Linux.

   b. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Ripristino a livello di file**.

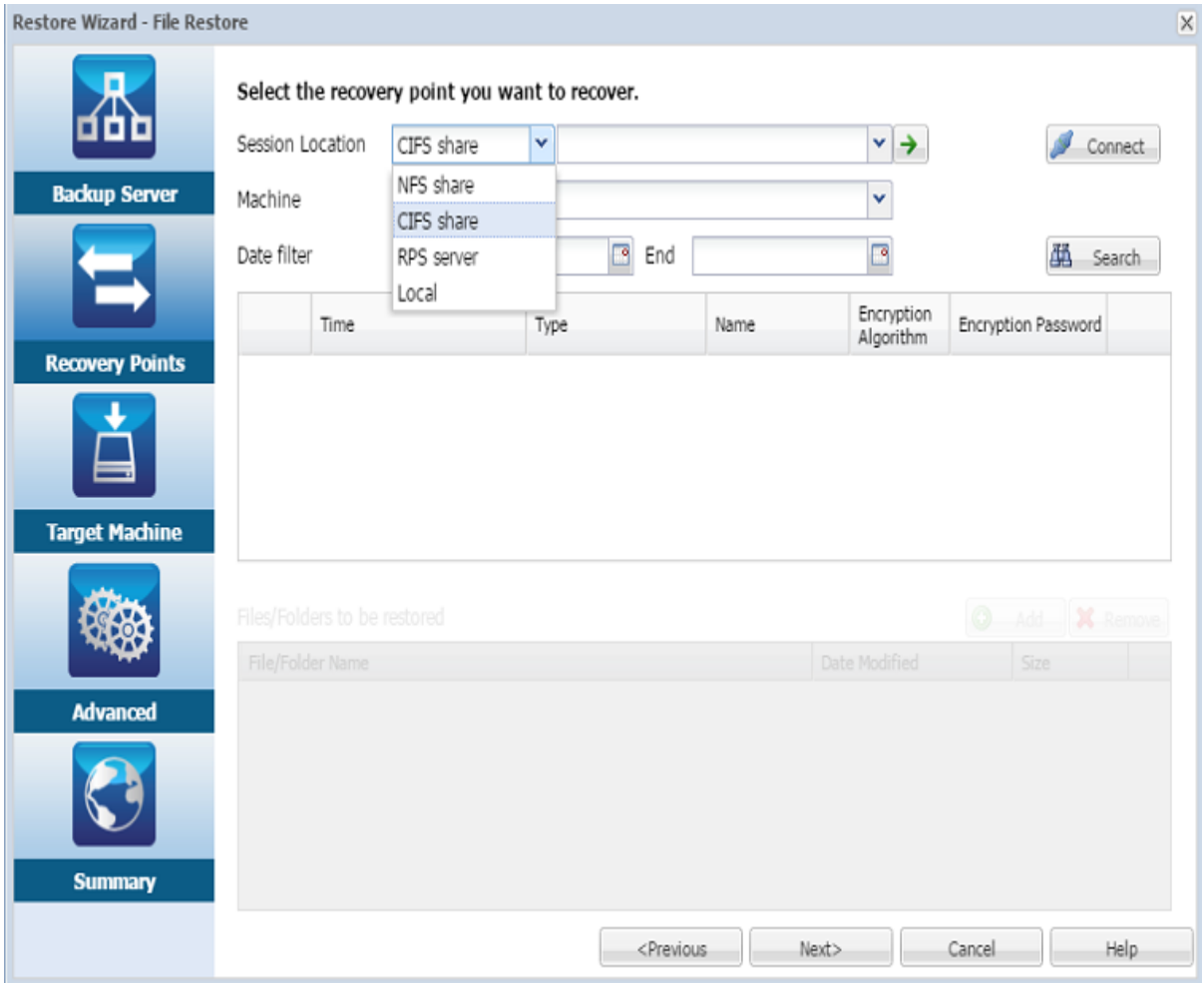
      Viene visualizzata la schermata **Procedura guidata di ripristino - Ripristino file**.

      È possibile visualizzare il server di backup selezionato nella pagina **Server di backup** della **Procedura guidata di ripristino**. Non è possibile selezionare alcuna opzione dall'elenco a discesa **Server di backup**.

2. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Punti di ripristino** della **Procedura guidata di ripristino**.

   Importante! Se la procedura guidata è stata aperta dalla console, vengono visualizzati automaticamente i dettagli della posizione della sessione e del computer. È possibile andare al passaggio 5.



3. Selezionare una **condivisione CIFS** o un **server RPS** dall'elenco a discesa **Percorso di sessione**.

   Nota: Non è possibile selezionare una condivisione NFS o locale per il ripristino delle sessioni di backup senza agente basate su host.

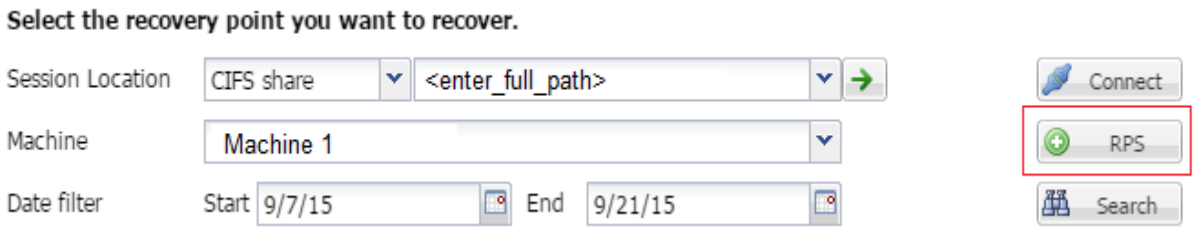
4. Eseguire una delle operazioni riportate di seguito in base al percorso di sessione:

   Per la condivisione CIFS

   a. Specificare il percorso completo della condivisione CIFS e fare clic su **Connetti**.

b. Specificare il nome utente e la password per connettersi alla condivisione CIFS, quindi fare clic su **OK**.

   Nell'elenco a discesa Computer vengono elencati tutti i computer e viene visualizzato un pulsante RPS accanto al computer.



c. Selezionare il computer dall'elenco a discesa e fare clic su RPS.

   Viene visualizzata la finestra di dialogo **Informazioni sul server del punto di ripristino**.

d. Fornire i dettagli RPS e fare clic su Sì.

   La finestra di dialogo **Informazioni sul Recovery Point Server** viene chiusa. Tutti i punti di ripristino del computer selezionato vengono visualizzati sotto l'opzione **Filtro data**.

Per il server RPS

a. Selezionare il server RPS e fare clic su Aggiungi.

   Viene visualizzata la finestra di dialogo **Informazioni sul server del punto di ripristino**.

b. Fornire i dettagli RPS e fare clic sul pulsante Carica.

c. Selezionare l'archivio dati dall'elenco a discesa e fare clic su **Sì**.

   La finestra di dialogo **Informazioni sul server del punto di ripristino** viene chiusa e viene visualizzata la procedura guidata.

d. Fare clic su **Connetti**.

   Tutti i computer vengono elencati nell'elenco a discesa Computer.

e. Selezionare il computer dall'elenco a discesa.

   Tutti i punti di ripristino del computer selezionato vengono visualizzati sotto l'opzione **Filtro data**.

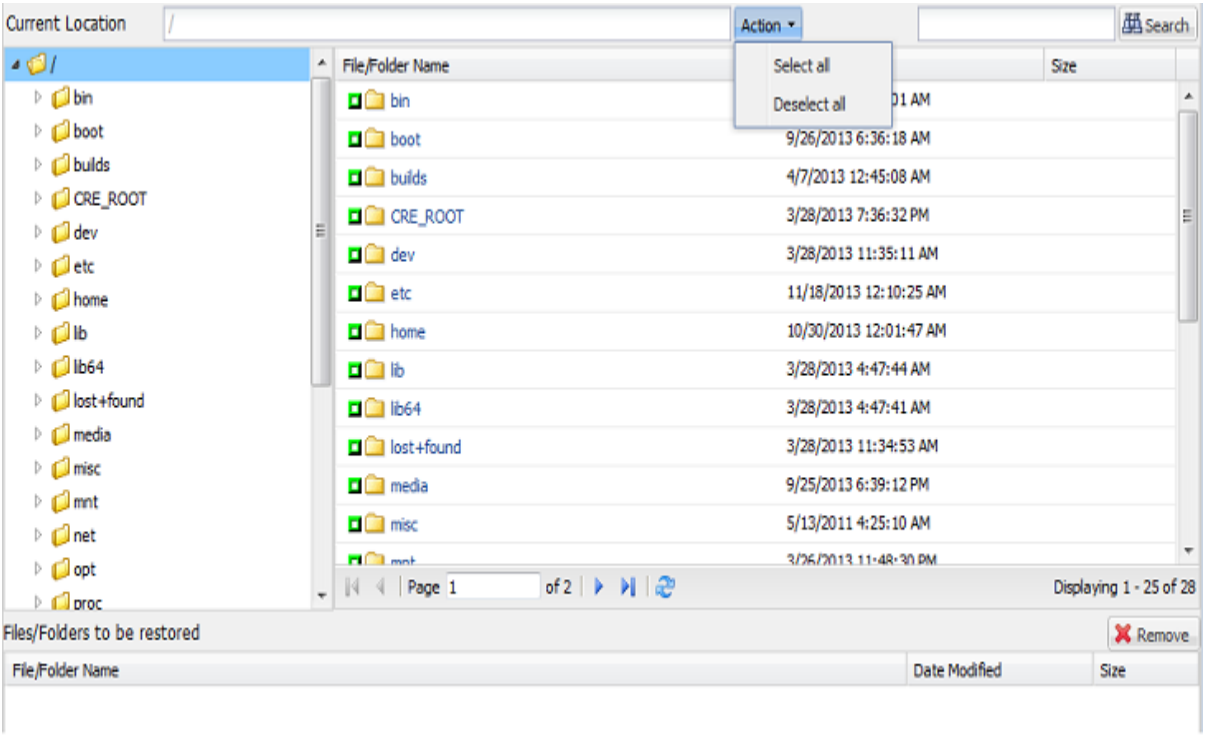
5. Applicare il filtro data per visualizzare i punti di ripristino generati tra le date specificate e fare clic su **Cerca**.

   Valore predefinito: ultime due settimane.

   Vengono visualizzati tutti i punti di ripristino disponibili tra le date specificate.

6. Selezionare il punto di ripristino di cui si desidera eseguire il ripristino e fare clic su **Aggiungi**. Se il punto di ripristino è crittografato, specificare la password di crittografia per il ripristino dei dati.

   Viene visualizzata la finestra di dialogo **Sfoglia-<nome nodo>**.



   Importante! Se viene visualizzato il messaggio di avviso "I file o le cartelle vengono visualizzati nel file di periferica. Fare clic per ulteriori informazioni." sulla console, consultare la nota seguente per la risoluzione.

   Nota: Per alcuni layout di disco complessi, viene visualizzato il file system in base al file di periferica. La modifica del comportamento di visualizzazione del file system non influisce sulla funzione di ripristino a livello di file del computer virtuale Linux basato su host. È possibile cercare il file system nel file di periferica. Inoltre, è possibile utilizzare la funzione di ricerca per eseguire la ricerca di un determinato file o una determinata directory.

7. Selezionare i file e le cartelle di cui si desidera eseguire il ripristino e fare clic su **OK**.

   Nota: se si esegue la ricerca di un file o una cartella mediante il campo **Cerca**, accertarsi di selezionare la cartella più elevata nella gerarchia. La ricerca viene condotta in tutte le cartelle figlie della cartella selezionata.

La finestra di dialogo **Sfoglia <nome nodo>** viene chiusa e si verrà reindirizzati alla pagina **Punti di ripristino**. I file e le cartelle selezionati sono contenuti nell'elenco **File/Cartelle da ripristinare**.

8. Fare clic su **Avanti**.

   Verrà visualizzata la pagina **Computer di destinazione**.

   Il punto di ripristino viene specificato.

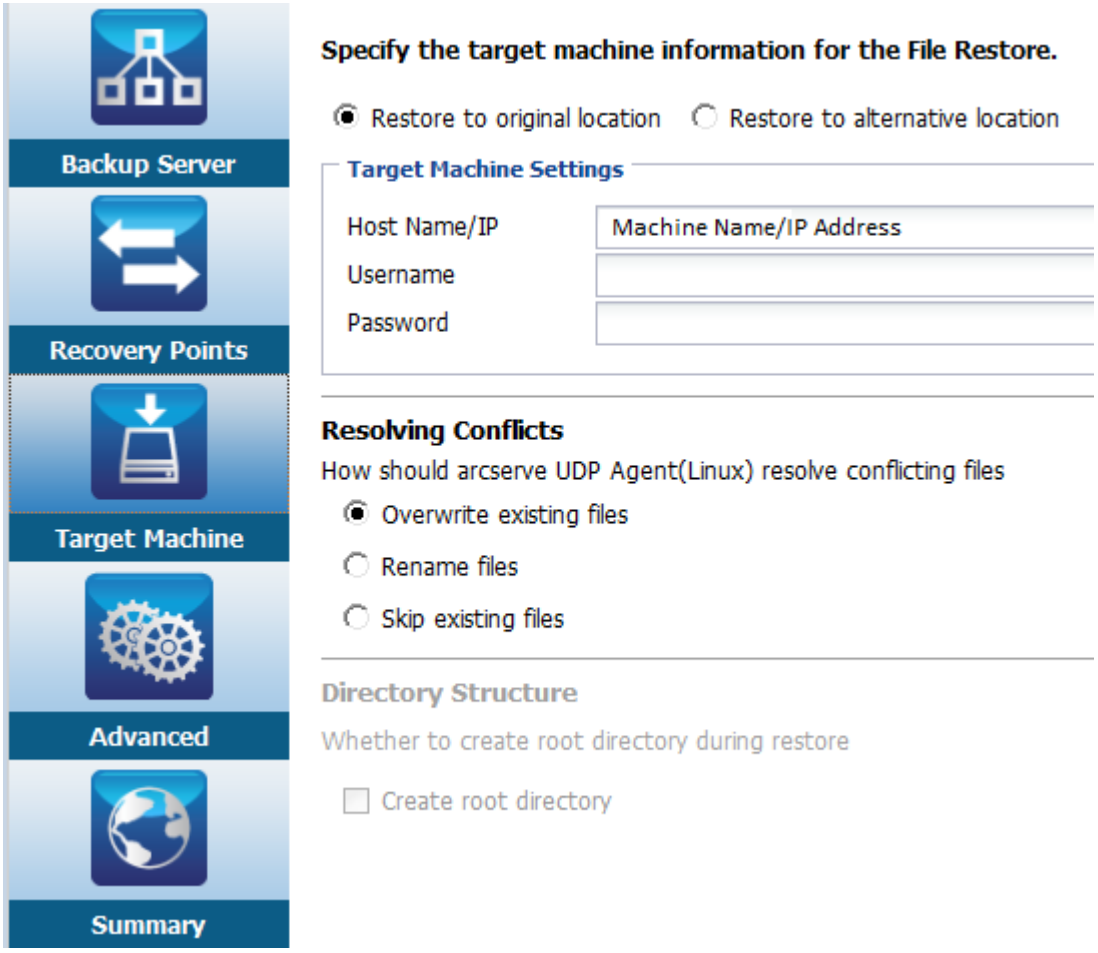
Definizione dei dettagli relativi al computer di destinazione

Specificare i dettagli relativi al nodo di destinazione in modo che i dati vengano ripristinati su tale computer. È possibile eseguire il ripristino delle cartelle o dei file selezionati sul nodo di origine o su un nuovo nodo.

Per eseguire il ripristino sul nodo di backup dei dati, attenersi alla procedura riportata di seguito:

1. Selezionare l'opzione **Ripristina in posizione originale della pagina** della pagina **Computer di destinazione**.

   Il campo **Nome host** delle **impostazioni del computer di destinazione** viene compilato con il nome del nodo di origine.



2. Immettere il nome utente e la password del nodo.
3. Per risolvere i file in conflitto, selezionare una delle seguenti opzioni:

   Sovrascrivi i file esistenti

Indica che se il file è presente sul computer di destinazione, il file di backup del punto di ripristino sostituirà il file esistente.

Rinomina file

Specifica che se il file esiste nel computer di destinazione, viene creato un nuovo file con lo stesso nome file e con l'estensione file *.d2d-duplicate<x>*. <x> specifica il numero di volte in cui il file viene ripristinato. Tutti i dati vengono ripristinati nel nuovo file.

Ignora file esistenti

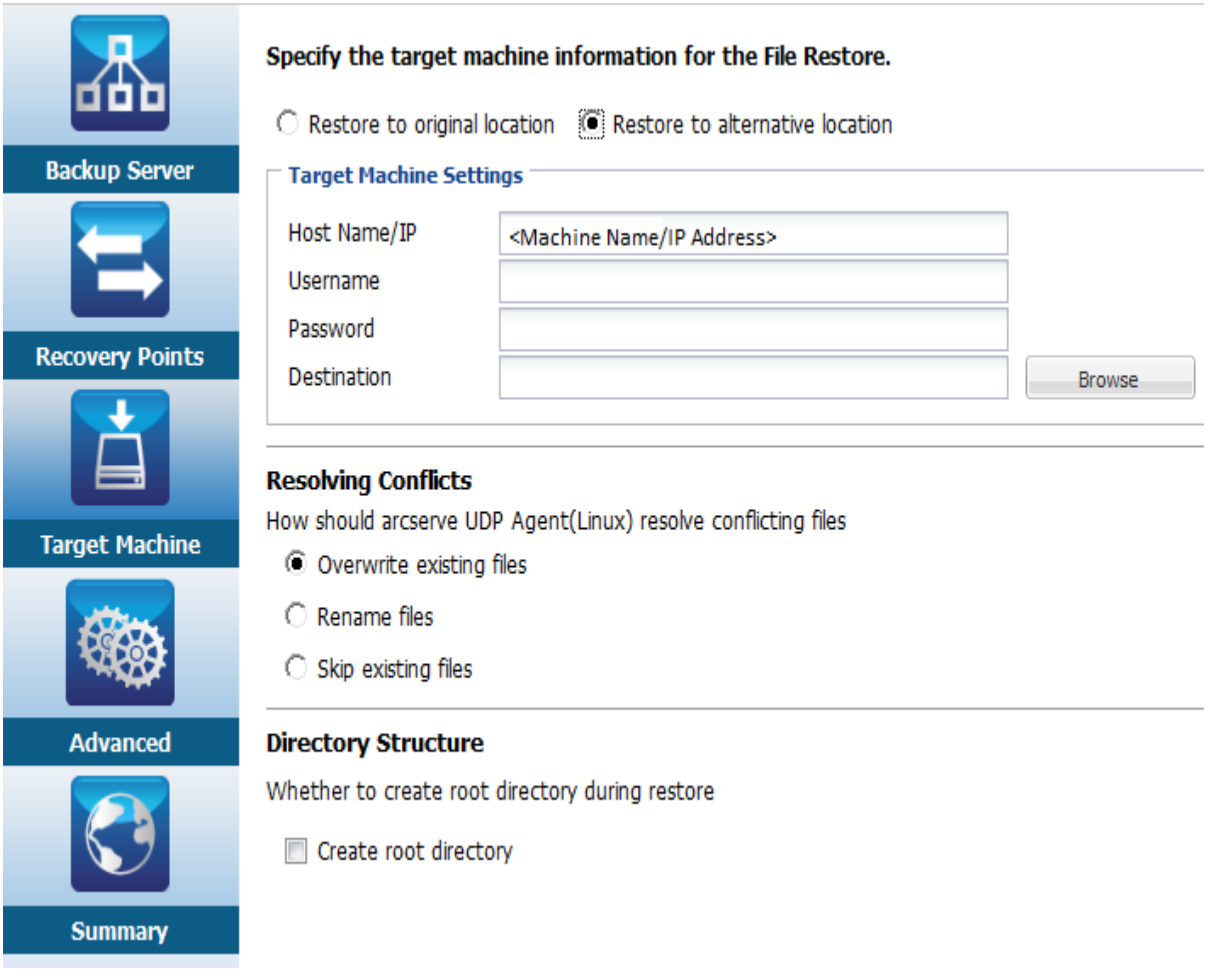
Specifica che se lo stesso file è già presente nel computer di destinazione, il ripristino di tali file non verrà eseguito a partire dal punto di ripristino.

4. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Impostazioni avanzate**.

Per eseguire il ripristino di un nuovo nodo, attenersi alla procedura riportata di seguito:

1. Selezionare l'opzione **Ripristina in posizione alternativa** della pagina **Computer di destinazione**.



2. Immettere il nome host o l'indirizzo IP del nodo di destinazione.
3. Immettere il nome utente e la password del nodo.
4. Immettere il percorso di ripristino dei dati, oppure fare clic su **Sfoglia** per selezionare la cartella di ripristino dei dati, quindi fare clic su **OK**.
5. Per risolvere i file in conflitto, selezionare una delle seguenti opzioni:

   Sovrascrivi i file esistenti

   Indica che se il file è presente sul computer di destinazione, il file di backup del punto di ripristino sostituirà il file esistente.

   Rinomina file

   Specifica che se il file esiste nel computer di destinazione, viene creato un nuovo file con lo stesso nome file e con l'estensione file *.d2d-duplicate<x>*. <x> specifica il numero di volte in cui il file viene ripristinato. Tutti i dati vengono ripristinati nel nuovo file.

   Ignora file esistenti

Specifica che se lo stesso file è già presente nel computer di destinazione, il ripristino di tali file non verrà eseguito a partire dal punto di ripristino.

6. (Facoltativo) Selezionare **Crea directory principale**.
7. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Impostazioni avanzate**.

Vengono specificati i dettagli relativi al computer di destinazione.

Definizione delle impostazioni avanzate

Specificare le impostazioni avanzate per eseguire un recupero pianificato dei dati. Il recupero pianificato garantisce che i dati vengano recuperati all'ora specificata anche in caso di assenza dell'utente.

Effettuare le operazioni seguenti:

1. Impostare la data e l'ora di inizio selezionando una delle seguenti opzioni:

   Esegui ora

   Avvia il processo di ripristino a livello di file dopo l'invio del processo.

   Imposta data e ora di inizio

   Avvia il processo di ripristino a livello di file nella data e ora specificata dopo l'invio del processo.

2. (Facoltativo) Selezionare **Stima dimensioni del file**.
3. (Facoltativo) Selezionare uno script dall'opzione **Impostazioni pre/post script**.

   Questi script eseguono comandi di script per le azioni da eseguire prima dell'inizio del processo e/o al completamento del processo.

   Nota: i campi **Impostazioni pre/post script** vengono popolati solamente se un file di script è già stato creato e collocato nel percorso seguente:

   /opt/Arcserve/d2dserver/usr/prepost

   Nota: per ulteriori informazioni sulla creazione di pre/post script, consultare la sezione *Gestione di pre/post script per l'automazione*.

4. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Riepilogo**.

   Vengono specificate le impostazioni avanzate.

(Facoltativo) Gestione di pre/post script per l'automazione

Gli script di pre/post esecuzione consentono di eseguire regole di business a intervalli specifici di un processo in esecuzione. È possibile specificare quando eseguire gli script nelle **Impostazioni pre/post script** della **Procedura guidata di backup** e della **Procedura guidata di ripristino** dell'interfaccia utente. È possibile eseguire gli script sul server di backup in base alle impostazioni dell'utente.

La gestione del pre/post script è un processo costituito da due passaggi: la creazione del pre/post script e la sua collocazione nella cartella prepost.

Creazione di pre/post script

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare un file di script mediante le variabili di ambiente nel linguaggio di scripting preferito.

   Variabili di ambiente del pre/post script

   Per creare lo script, utilizzare le variabili di ambiente seguenti:

   D2D_JOBNAME

   Indica il nome del processo.

   D2D_JOBID

   Identifica l'ID del processo. L'ID di processo è un numero attribuito al processo durante la sua esecuzione. Se si esegue lo stesso processo nuovamente, verrà fornito un nuovo numero di processo.

   D2D_TARGETNODE

   Identifica il nodo di cui viene eseguito il backup o il ripristino.

   D2D_JOBTYPE

   Identifica il tipo di processo in esecuzione. I valori seguenti identificano la variabile D2D_JOBTYPE:

   backup.full

   Identifica il processo come backup completo.

   backup.incremental

   Identifica il processo come backup incrementale.

   backup.verify

Identifica il processo come backup di verifica.

restore.bmr

Identifica il processo come ripristino bare metal (BMR). Si tratta di un processo di ripristino.

restore.file

Identifica il processo come ripristino a livello di file. Si tratta di un processo di ripristino.

D2D_SESSIONLOCATION

Identifica la posizione in cui vengono archiviati i punti di ripristino.

D2D_PREPOST_OUTPUT

Identifica un file temp. Il contenuto della prima linea del file temp viene visualizzato nel registro attività.

D2D_JOBSTAGE

Indica la fase del processo. I valori seguenti identificano la variabile D2D_ JOBSTAGE:

pre-job-server

Identifica lo script eseguito sul server di backup prima dell'avvio del processo.

post-job-server

Identifica lo script eseguito sul server di backup dopo il completamento del processo.

pre-job-target

Identifica lo script eseguito sul computer di destinazione prima dell'avvio del processo.

post-job-target

Identifica lo script eseguito sul computer di destinazione dopo il completamento del processo.

pre-snapshot

Identifica lo script eseguito sul computer di destinazione prima dell'acquisizione della snapshot.

post-snapshot

Identifica lo script eseguito sul computer di destinazione dopo l'acquisizione della snapshot.

D2D_TARGETVOLUME

Identifica il volume di cui viene eseguito il backup durante un processo di backup. Questa variabile è adatta per gli script di snapshot di pre/post automazione per un processo di backup.

D2D_JOBRESULT

Identifica il risultato di uno script del processo di post-esecuzione. I valori seguenti identificano la variabile di D2D_JOBRESULT:

success

Identifica il risultato come corretto.

fail

Identifica il risultato come non corretto.

D2DSVR_HOME

Identifica la cartella in cui è installato il server di backup. È possibile applicare la variabile agli script in esecuzione sul server di backup.

Lo script viene creato.

Nota: per tutti gli script, un valore restituito pari a zero indica un'operazione riuscita, mentre un valore restituito diverso da zero indica la presenza di un errore.

Collocare lo script nella cartella prepost ed eseguire la verifica

Tutti gli script di pre/post per un server di backup sono gestiti centralmente dalla cartella prepost nella posizione seguente:

/opt/Arcserve/d2dserver/usr/prepost

Effettuare le operazioni seguenti:

1. Collocare il file nella posizione seguente del server di backup:

   /opt/Arcserve/d2dserver/usr/prepost
2. Fornire le autorizzazioni di esecuzione per il file di script.
3. Accedere all'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux.
4. Aprire la procedura guidata di **backup** o **ripristino** ed accedere alla scheda **Impostazioni avanzate**.
5. Selezionare il file di script nell'elenco del menu a discesa **Impostazioni di pre/post script**, quindi inviare il processo.
6. Fare clic sul **Registro attività** e verificare che lo script venga eseguito per il processo di backup specificato.

Lo script viene eseguito.

I pre/post script vengono creati correttamente e inseriti nella cartella prevista.

Creazione ed esecuzione del processo di ripristino

Creare e eseguire il processo di ripristino in modo da poter avviare il recupero a livello di file. Verificare le informazioni relative al punto di ripristino prima di eseguire il ripristino dei file. Se necessario, è possibile tornare indietro e modificare le impostazioni di ripristino nella procedura guidata.

Effettuare le operazioni seguenti:

1. Verificare i dettagli relativi al ripristino nella pagina **Riepilogo** della **Procedura guidata di ripristino**.
2. (Facoltativo) Fare clic su **Indietro** per modificare le informazioni immesse in una pagina qualsiasi della **Procedura guidata di ripristino.**
3. Immettere un nome per il del processo e fare clic su **Invia**.

   Il campo **Nome processo** è associato a un nome predefinito. È possibile specificare un nuovo nome per il processo ma non è possibile lasciare il campo vuoto.

   La **Procedura guidata di ripristino** viene chiusa. È possibile visualizzare lo stato del processo dalla scheda **Stato processo**.

   Il processo di ripristino viene creato ed eseguito correttamente.

Verifica del ripristino dei file

Al completamento del processo di ripristino, verificare che tutti i nodi siano stati ripristinati sul nodo di destinazione. Selezionare **Cronologia processo** e le schede **Registro attività** nel riquadro **Stato** per monitorare l'avanzamento del processo di ripristino.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione su cui sono stati ripristinati i dati.
2. Verificare che i dati obbligatori del punto di ripristino vengano ripristinati.

   La verifica dei file viene eseguita correttamente.

   Il recupero a livello di file viene eseguito correttamente.

Migrazione di un computer virtuale istantaneo (da un punto di ripristino Linux) da cloud a locale

Se si dispone di un punto di ripristino Linux su Amazon S3, è possibile eseguire un processo del computer virtuale istantaneo su AWS, quindi eseguire la migrazione del computer virtuale istantaneo da AWS in locale.

Completare le attività seguenti per eseguire la migrazione del computer virtuale istantaneo:

- Verifica dei prerequisiti per la migrazione del computer virtuale istantaneo
- Migrazione di un computer virtuale istantaneo da cloud a locale

Verifica dei prerequisiti e considerazioni per la migrazione di un computer virtuale Istantaneo

Prerequisiti:

- Si dispone di un punto di ripristino valido e della password di crittografia per il ripristino.
- Si dispone di account Amazon EC2 e Amazon S3.
- Il server Samba è installato sul server di backup Linux.

Considerazioni:

questa funzionalità è supportata solo sui server di backup Linux installati su RHEL/CentOS/Oracle Linux 7.x o SLES 12.x.

Migrazione di un computer virtuale istantaneo da cloud a locale

È possibile eseguire la migrazione del computer virtuale Istantaneo da cloud a locale mediante le seguenti tre procedure dettagliate. Fare clic sui collegamenti di ogni procedura per completarne l'esecuzione e la migrazione.

- Per creare un computer virtuale istantaneo su Amazon EC2, eseguire il computer virtuale istantaneo da un punto di ripristino del computer virtuale Linux su Amazon EC2.
- Installare il server di backup Linux all'interno del computer virtuale istantaneo appena creato. Eseguire il backup all'interno del computer virtuale istantaneo, quindi eseguirlo su Amazon S3.
- Eseguire il backup del computer Linux su Amazon S3.
- Eseguire il processo di ripristino bare metal dal punto di ripristino in Amazon S3 di cui è stato eseguito il backup.

Esecuzione di un ripristino bare metal per computer Linux

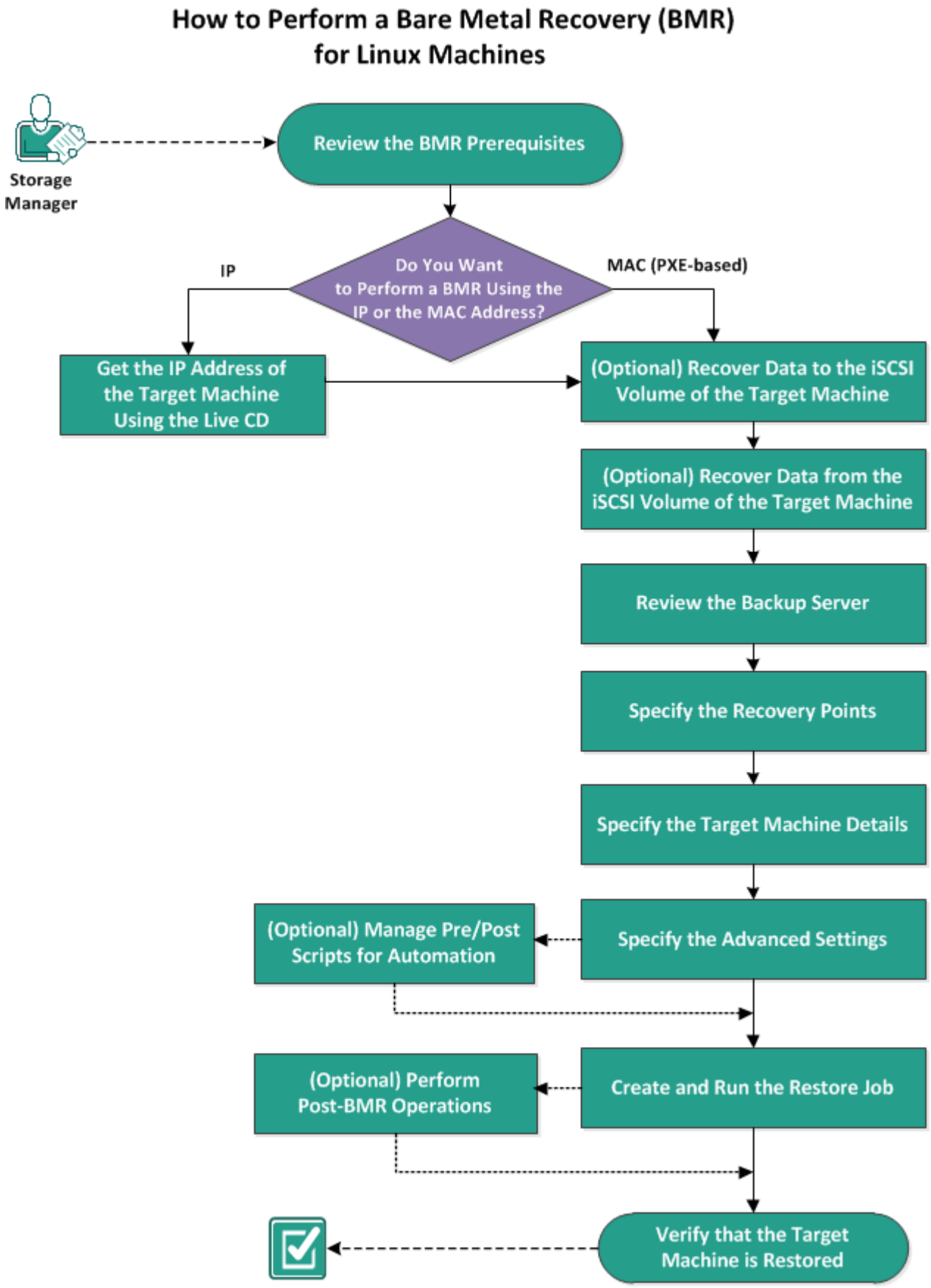
Un ripristino bare metal esegue il ripristino del sistema operativo e delle applicazioni software, ed esegue il recupero di tutti i dati sottoposti a backup. Il ripristino bare metal consiste nel ripristino di un sistema del computer avviato a partire da un sistema *bare metal*. Bare metal è un computer senza sistema operativo, driver e applicazioni software. Al completamento del ripristino, il computer di destinazione viene riavviato automaticamente sullo stesso ambiente operativo del nodo di origine del backup e tutti i dati vengono ripristinati.

È possibile eseguire un ripristino bare metal completo poiché quando si esegue un backup di dati, esso acquisisce anche informazioni relative al sistema operativo, alle applicazioni installate, ai driver e così via.

È possibile eseguire un ripristino bare metal mediante l'indirizzo IP o l'indirizzo MAC del computer di destinazione. Se il computer di destinazione viene avviato mediante il Live CD dell'Agente Arcserve Unified Data Protection per Linux, è possibile ottenere l'indirizzo IP del computer di destinazione.

Nota: È possibile avviare il computer. È stata configurata una sola scheda NIC.

Il diagramma seguente mostra il processo di ripristino bare metal:



Completare le attività seguenti per eseguire un ripristino bare metal:

- Verifica dei prerequisiti di ripristino bare metal
- Acquisizione dell'indirizzo IP del computer di destinazione con Live CD
- (Facoltativo) Ripristino dei dati nel volume iSCSI del computer di destinazione
- (Facoltativo) Ripristino dei dati dal volume iSCSI nel computer di destinazione
- Verifica del server di backup
- Definizione dei punti di ripristino
- Definizione dei dettagli relativi al computer di destinazione
- Definizione delle impostazioni avanzate
- (Facoltativo) Gestione di pre/post script per l'automazione
- Creazione ed esecuzione del processo di ripristino
- (Facoltativo) Esecuzione di operazioni successive al ripristino bare metal
- Verifica del ripristino del computer di destinazione

Verifica dei prerequisiti di ripristino bare metal

Prima di eseguire un ripristino bare metal, devono verificarsi le seguenti condizioni:

- Si dispone di un punto di ripristino valido e della password di crittografia per il ripristino.
- Si dispone di un computer di destinazione valido per il ripristino bare metal.
- È stato creato Live CD dell'Agente Arcserve Unified Data Protection per Linux.
- Se si desidera eseguire il ripristino bare metal con l'indirizzo IP, è necessario acquisire l'indirizzo IP del computer di destinazione utilizzando Live CD.
- Se si desidera eseguire il ripristino bare metal PXE con l'indirizzo MAC, è necessario acquisire l'indirizzo MAC del computer di destinazione.
- È necessario che il punto di ripristino sia creato dal backup basato su agente Linux.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Acquisizione dell'indirizzo IP del computer di destinazione con Live CD

Prima di eseguire un ripristino bare metal mediante l'indirizzo IP, è necessario acquisire tale indirizzo del computer di destinazione. Un computer bare metal non è inizialmente associato a nessun indirizzo IP. Pertanto, è necessario avviare il computer bare metal mediante il Live CD predefinito, ossia il Live CD dell'Agente Arcserve Unified Data Protection per Linux, o quello basato su CentOS, per ottenere l'indirizzo IP. Dopo aver acquisito l'indirizzo IP del computer di destinazione, è possibile configurarne l'IP statico.

Effettuare le operazioni seguenti:

1. Inserire il Live CD o montare il file .iso del Live CD nell'unità CD-ROM del nodo di destinazione.
2. Avviare il computer di destinazione dal CD-ROM.

   Il computer di destinazione viene avviato nell'ambiente Live CD dell'Agente Arcserve Unified Data Protection per Linux. Verrà visualizzato l'indirizzo IP del computer di destinazione.
3. Per configurare l'IP statico del computer di destinazione utilizzando il Live CD predefinito, attenersi alla procedura seguente:
   a. Sulla schermata del computer di destinazione, premere Invio per entrare nell'ambiente shell.
   b. Eseguire il comando seguente per configurare l'IP statico:

      ifconfig <NIC name> <static IP address> netmask <netmask>

      route add default gw <gateway IP address> <NIC name>

   Nota: Il nome della scheda di interfaccia di rete (NIC) dipende dall'hardware. Ad esempio, eth0 o em0 sono nomi tipici della scheda NIC.
4. Per configurare l'IP statico del computer di destinazione utilizzando il Live CD basato su CentOS, attenersi alla procedura seguente:
   a. Aprire una finestra del terminale sul computer di destinazione facendo clic su Applicazioni, Strumenti di sistema, Terminale.
   b. Eseguire i comandi seguenti:

      sudo ifconfig <NIC name> <static IP address> netmask <netmask>

      sudo route add default gw <gateway IP address> <NIC name>

   L'IP statico è stato configurato.

   L'acquisizione dell'indirizzo IP del computer di destinazione è stata completata.

Importante. Annotare l'indirizzo IP in quanto verrà utilizzato nella **Procedura guidata di ripristino** in fase di indicazione dei dettagli relativi al computer di destinazione.

(Facoltativo) Ripristino dei dati nel volume iSCSI del computer di destinazione

È possibile integrare il volume iSCSI nel computer di destinazione e rendere quel volume parte del computer di destinazione. Quindi, è possibile ripristinare i dati nel volume iSCSI del computer di destinazione. In questo modo, è possibile gestire i dati e trasferirli su una rete.

Importante. Quando si integra il volume iSCSI nel computer di destinazione, tutti i dati esistenti nel volume iSCSI verranno persi.

Effettuare le operazioni seguenti:

1. Inserire il Live CD dell'Agente Arcserve Unified Data Protection per Linux o montare il file .iso del Live CD dell'Agente Arcserve Unified Data Protection per Linux nell'unità CD-ROM del computer di destinazione.
2. Avviare il computer di destinazione dal CD-ROM.

   Il computer di destinazione viene avviato nell'ambiente Live CD dell'Agente Arcserve Unified Data Protection per Linux. Verrà visualizzato l'indirizzo IP del computer di destinazione.
3. Accedere all'ambiente della shell del computer di destinazione.
4. Eseguire il comando seguente per avviare il daemon iniziatore di iSCSI:

   ```
   /etc/init.d/iscsid start
   ```
5. Eseguire uno script di rilevamento per rilevare l'host di destinazione di iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   Il valore predefinito della porta dell'host di destinazione di iSCSI è 3260.
6. Prendere nota del nome completo iSCSI (IQN) dell'host di destinazione di iSCSI rilevato dallo script di rilevamento prima di accedere manualmente alla destinazione individuata.
7. Elencare la periferica a blocchi disponibile del nodo di destinazione.

   ```
   #fdisk -l
   ```
8. Accedere alla destinazione rilevata.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l
   ```

   È possibile visualizzare una periferica a blocchi nella directory /dev del nodo di destinazione.

9. Eseguire il comando seguente per ottenere il nuovo nome della periferica:

   #fdisk -l

   È possibile visualizzare una periferica aggiuntiva chiamata /dev/sd<x> nel nodo di destinazione.

   Il volume iSCSI viene integrato nel volume di destinazione.

(Facoltativo) Ripristino dei dati dal volume iSCSI nel computer di destinazione

Se sono stati archiviati i dati in un volume di destinazione iSCSI, è possibile connettersi al volume iSCSI e ripristinare i dati. Il volume iSCSI consente di gestire i dati e di trasferirli su una rete.

Effettuare le operazioni seguenti:

1. Inserire il Live CD dell'Agente Arcserve Unified Data Protection per Linux o montare il file .iso del Live CD dell'Agente Arcserve Unified Data Protection per Linux nell'unità CD-ROM del computer di destinazione.
2. Avviare il computer di destinazione dal CD-ROM.

   Il computer di destinazione viene avviato nell'ambiente Live CD dell'Agente Arcserve Unified Data Protection per Linux. Verrà visualizzato l'indirizzo IP del computer di destinazione.
3. Accedere all'ambiente della shell del computer di destinazione.
4. Eseguire il comando seguente per avviare il daemon iniziatore di iSCSI:

   /etc/init.d/iscsid start
5. Eseguire uno script di rilevamento per rilevare l'host di destinazione di iSCSI.

   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>

   Il valore predefinito della porta dell'host di destinazione di iSCSI è 3260.
6. Prendere nota del nome completo iSCSI (IQN) dell'host di destinazione di iSCSI rilevato dallo script di rilevamento prima di accedere manualmente alla destinazione individuata.
7. Elencare la periferica a blocchi disponibile del nodo di destinazione.

   #fdisk -l
8. Accedere alla destinazione rilevata.

   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l

   È possibile visualizzare una periferica a blocchi nella directory /dev del nodo di destinazione.
9. Eseguire il comando seguente per ottenere il nuovo nome della periferica:

   #fdisk -l

È possibile visualizzare una periferica aggiuntiva chiamata /dev/sd<x> nel nodo di destinazione.

Ad esempio, supporre che il nome della periferica sia /dev/sdc. Tale nome della periferica viene utilizzato per creare una partizione e un file system nelle seguenti fasi.

10. Montare il volume iSCSI utilizzando i comandi seguenti:

    # mkdir /iscsi

    # mount /dev/sdc1 /iscsi

    Nota: Quando si specifica il percorso di sessione nella procedura guidata di ripristino, è necessario selezionare Locale e immette il percorso /iscsi.

    Esempio: <path>/iscsi

    Il computer di destinazione può connettersi ora al volume iSCSI e può ripristinare i dati in esso contenuti.

Verifica del server di backup

Quando si apre la **Procedura guidata di ripristino**, verificare il server di backup su cui si desidera eseguire l'operazione di ripristino.

Effettuare le operazioni seguenti:

1. Accedere alla procedura guidata di ripristino in uno dei modi seguenti:

   Da Arcserve UDP :

   a. Accedere ad Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata l'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux. La finestra di dialogo di selezione del tipo di ripristino viene visualizzata nell'interfaccia utente dell'agente.

   f. Selezionare il tipo di ripristino e fare clic su **OK**.

      Nota: si accede automaticamente al nodo agente e la **Procedura guidata di ripristino** viene visualizzata dal nodo agente.

   Dall'Agente Arcserve Unified Data Protection per Linux:

   a. Aprire l'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux.

      Nota: durante l'installazione dell'Agente Arcserve Unified Data Protection per Linux, l'URL per l'accesso e la gestione del server viene fornito all'utente. Accedere all'Agente Arcserve Unified Data Protection per Linux.

   b. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Ripristino bare metal (BMR)**.

      Viene visualizzata la pagina **Server di backup** della **Procedura guidata di ripristino - Ripristino bare metal**.

2. Verificare il server nell'elenco a discesa **Server di backup** nella pagina **Server di backup**.

   Non è possibile selezionare alcuna opzione dall'elenco a discesa **Server di backup**.

3. Fare clic su **Avanti**.

Viene visualizzata la pagina **Punti di ripristino** della finestra di dialogo **Procedura guidata di ripristino - Ripristino bare metal**.

Viene specificato il server di backup.

Definizione dei punti di ripristino

L'esecuzione di un backup implica la creazione di un punto di ripristino. Specificare le informazioni relative al punto di ripristino della **Procedura guidata di ripristino**, in modo da poter eseguire il ripristino dei dati desiderati. È possibile ripristinare file specifici o tutti i file in base alle proprie esigenze.

Importante! Per eseguire un ripristino bare metal da un punto di ripristino, il volume principale e il volume di avvio devono essere presenti nel punto di ripristino.

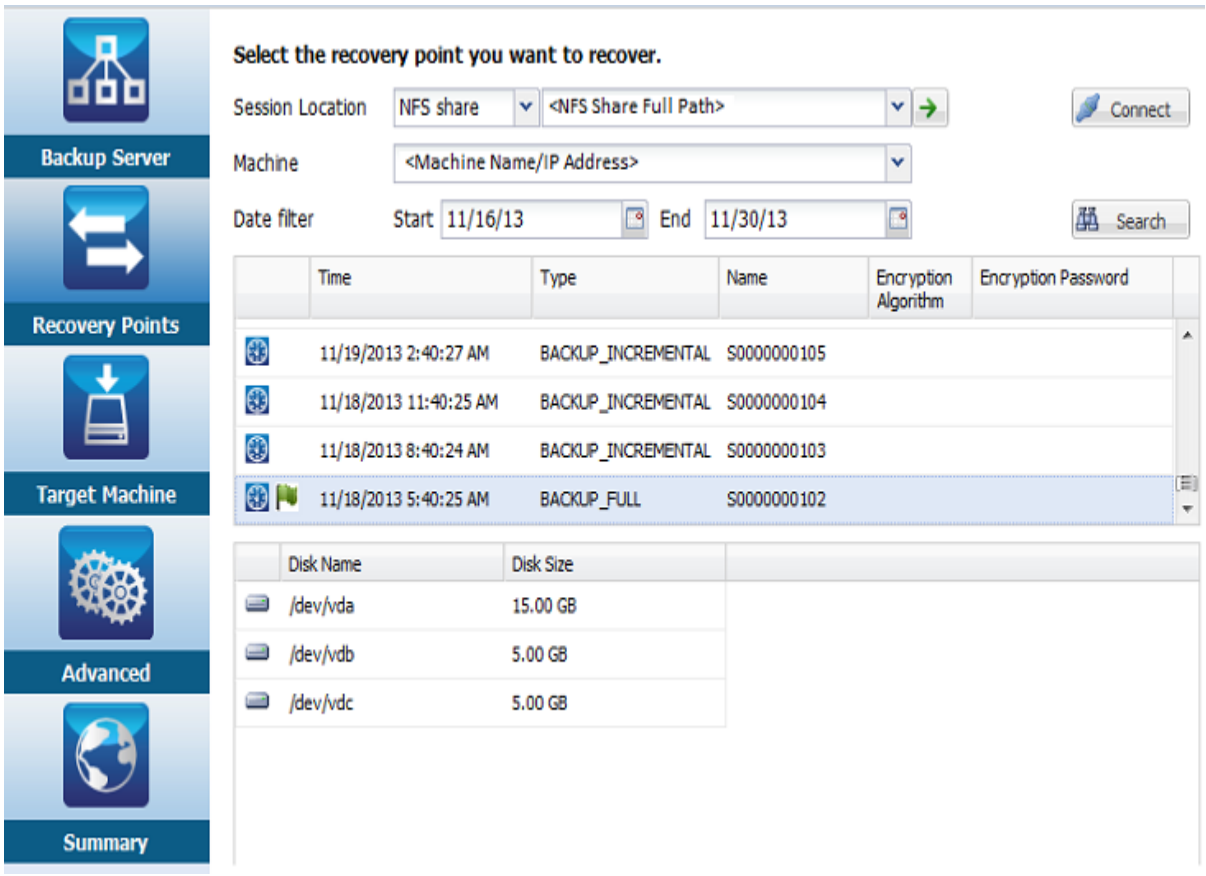
Effettuare le operazioni seguenti:

1. Eseguire una delle operazioni riportate di seguito in base all'archiviazione di backup utilizzata.
   - Eseguire le operazioni seguenti per accedere ai punti di ripristino archiviati su una periferica mobile:
     a. Avviare il computer di destinazione utilizzando Live CD.
     b. Accedere all'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux dal Live CD.
     c. Aprire la **procedura guidata di ripristino bare metal**.
     d. Accedere alla pagina **Punti di ripristino**.
     e. Selezionare **Locale** come **Percorso di sessione** nella pagina **Punti di ripristino** della **procedura guidata di ripristino bare metal**.
   - Eseguire le operazioni seguenti se la posizione di sessione corrisponde a una condivisione NFS o CIFS:
     a. Selezionare una sessione dall'elenco a discesa **Percorso di sessione**, quindi specificare il percorso completo della condivisione.

        Ad esempio, si utilizza il percorso della sessione come condivisione NFD, xxx.xxx.xxx.xxx come indirizzo IP della condivisione NFS e la cartella viene denominata *Data.* Sarà necessario immettere xxx.xxx.xxx.xxx:/Data come percorso di condivisione NFS.

        Nota: se i dati di backup vengono archiviati nell'origine locale, sarà necessario convertire il nodo di origine in un server NFS, quindi con-

dividere il percorso della sessione.



2. Fare clic su **Connetti**.

   Tutti i nodi di cui è stato eseguito il backup per il percorso specificato saranno contenuti nell'elenco a discesa **Computer.**

3. Selezionare il nodo di cui si desidera eseguire il ripristino dall'elenco a discesa **Computer**.

   Verrà creato un elenco contenente tutti i punti di ripristino per il nodo selezionato.

4. Applicare il filtro data per visualizzare i punti di ripristino generati tra le date specificate e fare clic su **Cerca**.

   Valore predefinito: ultime due settimane.

   Vengono visualizzati tutti i punti di ripristino disponibili tra le date specificate.

5. Selezionare il punto di ripristino di cui si desidera eseguire il ripristino e fare clic su **Avanti**.

   Verrà visualizzata la pagina **Computer di destinazione**.

   Il punto di ripristino viene specificato.

Definizione dei dettagli relativi al computer di destinazione

Specificare i dettagli relativi al computer di destinazione in modo che i dati vengano ripristinati su tale computer. Un computer di destinazione è un computer bare metal su cui verrà eseguito un ripristino bare metal. Se si esegue il ripristino mediante l'indirizzo IP, sarà necessario disporre dell'indirizzo IP del computer di destinazione registrato precedentemente all'inizio del processo. Se il ripristino viene eseguito mediante un indirizzo MAC, sarà necessario disporre di tale indirizzo per il computer di destinazione.

Effettuare le operazioni seguenti:

1. Immettere l'indirizzo MAC o IP del computer di destinazione nel campo **Indirizzo MAC/IP**.
2. Specificare un nome per il campo **Nome host**.

   Il computer di destinazione utilizzerà questo nome come nome host al completamento del processo di ripristino.
3. Selezionare una delle opzioni seguenti come rete:

   DHCP

   Configura automaticamente l'indirizzo IP. Questa è l'opzione predefinita. Utilizzare questa opzione se si desidera eseguire il ripristino di un server DHCP (Dynamic Host Configuration Protocol) su una rete DHCP.

   IP statico

   Configura manualmente l'indirizzo IP. Se si seleziona questa opzione, è necessario specificare l'**indirizzo IP**, la **subnet mask** e il **gateway predefinito** del computer di destinazione.

   Importante. Verificare che l'IP statico non sia in uso da altri computer durante il processo di ripristino.
4. (Facoltativo) Selezionare l'opzione **Abilita ripristino bare metal immediato** in modo da poter utilizzare istantaneamente il computer di destinazione.

   Quando si abilita questa opzione, l'Agente Arcserve Unified Data Protection per Linux recupera innanzitutto tutti i dati necessari per avviare il computer. Dopo aver avviato il computer di destinazione, i dati rimanenti vengono ripristinati. La connessione di rete deve essere costantemente disponibile durante il ripristino bare metal immediato.

Esempio: Se si dispone di 100 GB di dati e si desidera eseguire un ripristino bare metal e *non* si seleziona questa opzione, prima vengono ripristinati tutti i 100 GB di dati, quindi è possibile utilizzare il computer di destinazione. Tuttavia, è necessario solo 1 GB di dati circa per avviare il computer. Quando si abilita questa opzione, viene ripristinato innanzitutto 1 GB di dati richiesti in modo che sia possibile avviare e utilizzare il computer. Dopo aver avviato il computer, i rimanenti 99 GB di dati vengono ripristinati automaticamente.

Nota: I dati necessari per avviare il computer dipendono dalla configurazione del sistema operativo. Inoltre, è possibile sospendere o riprendere il ripristino automatico dei dati se l'opzione **Non eseguire il recupero automatico dei dati dopo l'avvio del computer** non è selezionata.

5. (Facoltativo) Selezionare l'opzione **Non eseguire il recupero automatico dei dati dopo l'avvio del computer** per interrompere il ripristino automatico dei dati quando il computer di destinazione viene avviato.

   Quando si seleziona l'opzione **Abilita ripristino bare metal immediato**, il comportamento predefinito prevede innanzitutto il ripristino dei dati necessari e poi l'avvio del computer. Dopo aver avviato il computer, i dati rimanenti vengono ripristinati automaticamente. Se si aggiornano i dati di origine durante il ripristino e poi si seleziona questa opzione, i dati vengono recuperati fino al punto prima dell'aggiornamento.

6. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Impostazioni avanzate**.

   Vengono specificati i dettagli relativi al computer di destinazione.

Definizione delle impostazioni avanzate

Specificare le impostazioni avanzate per eseguire un ripristino bare metal pianificato dei dati. Il ripristino bare metal pianificato garantisce che i dati vengano ripristinati all'ora specificata anche in caso di assenza dell'utente.

Effettuare le operazioni seguenti:

1. Impostare la data e l'ora di inizio selezionando una delle seguenti opzioni:

   Esegui ora

   Avvia il processo di ripristino dopo l'invio del processo.

   Imposta ora speciale

   Avvia il processo di ripristino all'ora specificata dopo l'invio del processo.

2. (Facoltativo) Selezionare uno script dall'opzione **Impostazioni script pre/post backup** per il server di backup e il computer di destinazione.

   Questi script eseguono comandi di script per le azioni da eseguire prima dell'inizio del processo e/o al completamento del processo.

   Nota: i campi **Impostazioni pre/post script** vengono popolati solamente se un file di script è già stato creato e collocato nel percorso seguente:

   /opt/Arcserve/d2dserver/usr/prepost

   Nota: per ulteriori informazioni sulla creazione di pre/post script, consultare la sezione *Gestione di pre/post script per l'automazione*.

3. (Facoltativo) Fare clic su **Mostra altre impostazioni** per visualizzare ulteriori impostazioni relative al ripristino bare metal.

4. (Facoltativo) Reimpostare la password per il nome utente specificato per il computer di destinazione di cui è stato eseguito il recupero.

5. (Facoltativo) Immettere il percorso completo del percorso di archiviazione di backup dei punti di ripristino in **Accesso locale al punto di ripristino**.

6. (Facoltativo) Immettere il nome completo del disco nel campo **Dischi** per escludere tali dischi sul computer di destinazione dal processo di recupero.

7. (Facoltativo) Selezionare l'opzione **Abilita riattivazione LAN** se viene eseguito un ripristino bare metal basato su PXE (Preboot Execution Environment).

   Nota: l'opzione **Abilita riattivazione LAN** è applicabile solamente ai computer fisici. Assicurarsi di avere abilitato le impostazioni di riattivazione LAN nelle impostazioni BIOS del computer fisico.

8. (Facoltativo) Selezionare l'opzione di **riavvio** per riavviare automaticamente il nodo di destinazione al completamento del processo di ripristino bare metal.
9. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Riepilogo**.

   Vengono specificate le impostazioni avanzate.

(Facoltativo) Gestione di pre/post script per l'automazione

Gli script di pre/post esecuzione consentono di eseguire regole di business a intervalli specifici di un processo in esecuzione. È possibile specificare quando eseguire gli script nelle **Impostazioni pre/post script** della **Procedura guidata di backup** e della **Procedura guidata di ripristino** dell'interfaccia utente. È possibile eseguire gli script sul server di backup in base alle impostazioni dell'utente.

La gestione del pre/post script è un processo costituito da due passaggi: la creazione del pre/post script e la sua collocazione nella cartella prepost.

Creazione di pre/post script

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare un file di script mediante le variabili di ambiente nel linguaggio di scripting preferito.

   Variabili di ambiente del pre/post script

   Per creare lo script, utilizzare le variabili di ambiente seguenti:

   D2D_JOBNAME

   Indica il nome del processo.

   D2D_JOBID

   Identifica l'ID del processo. L'ID di processo è un numero attribuito al processo durante la sua esecuzione. Se si esegue lo stesso processo nuovamente, verrà fornito un nuovo numero di processo.

   D2D_TARGETNODE

   Identifica il nodo di cui viene eseguito il backup o il ripristino.

   D2D_JOBTYPE

   Identifica il tipo di processo in esecuzione. I valori seguenti identificano la variabile D2D_JOBTYPE:

   backup.full

   Identifica il processo come backup completo.

   backup.incremental

   Identifica il processo come backup incrementale.

   backup.verify

Identifica il processo come backup di verifica.

restore.bmr

Identifica il processo come ripristino bare metal (BMR). Si tratta di un processo di ripristino.

restore.file

Identifica il processo come ripristino a livello di file. Si tratta di un processo di ripristino.

D2D_SESSIONLOCATION

Identifica la posizione in cui vengono archiviati i punti di ripristino.

D2D_PREPOST_OUTPUT

Identifica un file temp. Il contenuto della prima linea del file temp viene visualizzato nel registro attività.

D2D_JOBSTAGE

Indica la fase del processo. I valori seguenti identificano la variabile D2D_ JOBSTAGE:

pre-job-server

Identifica lo script eseguito sul server di backup prima dell'avvio del processo.

post-job-server

Identifica lo script eseguito sul server di backup dopo il completamento del processo.

pre-job-target

Identifica lo script eseguito sul computer di destinazione prima dell'avvio del processo.

post-job-target

Identifica lo script eseguito sul computer di destinazione dopo il completamento del processo.

pre-snapshot

Identifica lo script eseguito sul computer di destinazione prima dell'acquisizione della snapshot.

post-snapshot

Identifica lo script eseguito sul computer di destinazione dopo l'acquisizione della snapshot.

D2D_TARGETVOLUME

Identifica il volume di cui viene eseguito il backup durante un processo di backup. Questa variabile è adatta per gli script di snapshot di pre/post automazione per un processo di backup.

D2D_JOBRESULT

Identifica il risultato di uno script del processo di post-esecuzione. I valori seguenti identificano la variabile di D2D_JOBRESULT:

success

Identifica il risultato come corretto.

fail

Identifica il risultato come non corretto.

D2DSVR_HOME

Identifica la cartella in cui è installato il server di backup. È possibile applicare la variabile agli script in esecuzione sul server di backup.

Lo script viene creato.

Nota: per tutti gli script, un valore restituito pari a zero indica un'operazione riuscita, mentre un valore restituito diverso da zero indica la presenza di un errore.

Collocare lo script nella cartella prepost ed eseguire la verifica

Tutti gli script di pre/post per un server di backup sono gestiti centralmente dalla cartella prepost nella posizione seguente:

/opt/Arcserve/d2dserver/usr/prepost

Effettuare le operazioni seguenti:

1. Collocare il file nella posizione seguente del server di backup:

   /opt/Arcserve/d2dserver/usr/prepost
2. Fornire le autorizzazioni di esecuzione per il file di script.
3. Accedere all'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux.
4. Aprire la procedura guidata di **backup** o **ripristino** ed accedere alla scheda **Impostazioni avanzate**.
5. Selezionare il file di script nell'elenco del menu a discesa **Impostazioni di pre/post script**, quindi inviare il processo.
6. Fare clic sul **Registro attività** e verificare che lo script venga eseguito per il processo di backup specificato.

Lo script viene eseguito.

I pre/post script vengono creati correttamente e inseriti nella cartella prevista.

Creazione ed esecuzione del processo di ripristino

Creare e eseguire il processo di ripristino in modo da poter avviare il processo di ripristino bare metal. Prima di eseguire un ripristino bare metal, verificare le informazioni relative al punto di ripristino. Se necessario, è possibile tornare indietro e modificare le impostazioni di ripristino.

Effettuare le operazioni seguenti:

1. Verificare i dettagli relativi al ripristino nella pagina **Riepilogo** della **Procedura guidata di ripristino**.
2. (Facoltativo) Fare clic su **Indietro** per modificare le impostazioni di ripristino da una qualsiasi delle pagine della **Procedura guidata di ripristino**.
3. Immettere un nome per il del processo e fare clic su **Invia**.

   Il campo **Nome processo** è associato a un nome predefinito. È possibile specificare un nuovo nome per il processo ma non è possibile lasciare il campo vuoto.

   La **Procedura guidata di ripristino** viene chiusa. È possibile visualizzare il processo nella scheda **Stato processo**. Se si utilizza l'indirizzo IP per il ripristino bare metal, il computer di destinazione verrà riavviato automaticamente sullo stesso sistema operativo dell'origine di backup al completamento del processo di ripristino bare metal.

   Se si utilizza l'indirizzo MAC per il ripristino bare metal, lo stato della scheda **Stato processo** verrà modificato in *In attesa dell'avvio del nodo di destinazione*.
4. (Facoltativo) Affinché il ripristino bare metal utilizzi l'indirizzo MAC, avviare il computer di destinazione se viene visualizzato il messaggio *In attesa dell'avvio del nodo di destinazione nella scheda* della scheda **Stato processo**.

   Nota: Se il computer di destinazione viene avviato prima dell'invio del processo di ripristino, sarà necessario riavviare il computer di destinazione. Verificare che BIOS sia configurato per l'avvio dalla rete.

   Lo stato della colonna **Stato processo** viene modificato in **Ripristino del volume in corso**. Ciò indica che il ripristino è in corso. Al completamento del processo di ripristino, il computer di destinazione verrà riavviato automaticamente con lo stesso sistema operativo dell'origine di backup.

   Il processo di ripristino viene creato ed eseguito correttamente.

(Facoltativo) Esecuzione di operazioni successive al ripristino bare metal

Gli argomenti riportati di seguito fanno riferimento a impostazioni di configurazione facoltative che possono essere eseguite dopo il ripristino bare metal:

Configurazione di X Windows

In caso di ripristino bare metal su hardware diversi, il sistema X Windows del sistema operativo ripristinato non funziona correttamente, pertanto il nodo di destinazione mostra una finestra di dialogo di errore. La finestra di dialogo di errore viene visualizzata a causa della modifica della configurazione di visualizzazione. Per risolvere questo errore, attenersi alle istruzioni riportate nella finestra dialogo di errore per configurare la scheda grafica. Una volta completate tali operazioni, sarà possibile visualizzare l'interfaccia utente X Windows e il desktop.

Configurazione del nome completo di dominio del sistema (FQDN)

Per utilizzare un FQDN, configurare l'FQDN. Il processo di ripristino bare metal non esegue la configurazione automatica dell'FQDN.

Numero massimo di caratteri per FQDN: 63

Attenersi alla procedura seguente per configurare l'FQDN:

1. Modificare il file */etc/hosts* e specificare l'indirizzo IP, il nome FQDN e il nome del server.

   #vi /etc/hosts

   ip_of_system servername.domainname.com servername

2. Riavviare il servizio di rete.

   #/etc/init.d/network restart

3. Verificare il nome host e il nome FQDN.

   #hostname

   servername

   #hostname -f

   servername.domainname.com

   L'FQDN è stato configurato.

Estensione del volume di dati in seguito al ripristino bare metal su dischi diversi

Se si esegue il ripristino bare metal su un disco di maggiori dimensioni rispetto al disco sul nodo originale, lo spazio su disco non verrà utilizzato

completamente. L'operazione di ripristino bare metal non elabora automaticamente lo spazio su disco inutilizzato. È possibile formattare lo spazio su disco su una partizione separata oppure ridimensionare la partizione esistente con lo spazio su disco inutilizzato. Il volume che si desidera ridimensionare deve essere inutilizzato. Si consiglia quindi di non eseguire il ridimensionamento di un volume di sistema. La presente sezione descrive la procedura di estensione di un volume di dati con spazio su disco inutilizzato.

Nota: Per evitare la perdita di dati, ridimensionare i volumi immediatamente dopo il ripristino bare metal. Inoltre, è possibile eseguire il backup del nodo prima di avviare il ridimensionamento del volume.

In seguito al corretto riavvio del computer di destinazione dopo il ripristino bare metal, è possibile eseguire l'estensione del volume di dati.

Volume di partizione raw

Ad esempio, il ripristino di un disco da 2GB nella sessione viene eseguito su un disco da 16GB denominato */dev/sdb* con una partizione. La partizione raw */dev/sdb1* viene montata direttamente nella directory */data.*

Questo esempio viene utilizzato per descrivere la procedura di estensione di un volume di partizione raw.

Effettuare le operazioni seguenti:

1. Verificare lo stato del volume /dev/sdb1.

   # df –h /dev/sdb1

   /dev/sdb1 2.0G 40M 1.9G 3% /data

2. Smontare il volume /dev/sdb1.

   # umount /data

3. Ridimensionare /dev/sdb1 per occupare tutto lo spazio su disco utilizzando il comando fdisk.

   Per eseguire questa operazione, eliminare la partizione esistente e ricrearla utilizzando lo stesso numero di settore di inizio. L'utilizzo dello stesso numero di settore di inizio consente di evitare la perdita di dati.

   # fdisk -u /dev/sdb

   Command (m for help): p

   Disk /dev/sdb: 17.1 GB, 17179869184 bytes

   255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

   *Units = sectors of 1 * 512 = 512 bytes*

Device Boot Start End Blocks Id System

/dev/sdb1 63 4192964 2096451 83 Linux

Command (m for help): d

Selected partition 1

Command (m for help): n

Command action

e extended

p primary partition (1-4)

p

Partition number (1-4): 1

First sector (63-33554431, default 63):

Using default value 63

Last sector or +size or +sizeM or +sizeK (63-33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdb: 17.1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

*Units = sectors of 1 * 512 = 512 bytes*

Device Boot Start End Blocks Id System

/dev/sdb1 63 33554431 16777184+ 83 Linux

Command (m for help): w

La partizione adotta lo stesso numero di settore di inizio della partizione originale e il numero di settore di fine è 33554431.

4. Ridimensionare il volume utilizzando il comando resize2fs. Se necessario, eseguire prima il comando e2fsck.

   # e2fsck -f /dev/sdb1

   # resize2fs /dev/sdb1

5. Montare il volume sul punto di montaggio e verificare nuovamente lo stato del volume.

   # mount /dev/sdb1 /data

   # df –h /dev/sdb1

/dev/sdb1 16G 43M 16G 1% /data

Il volume viene esteso a 16 GB ed è pronto per essere utilizzato.

Volume LVM:

Ad esempio, il ripristino di un disco da 8GB nella sessione viene eseguito su un disco da 16GB denominato */dev/sdb* con una partizione. La partizione raw */dev/sdc1* viene utilizzata come unico volume fisico del volume logic LVM */dev/mapper/VGTest-LVTest* con punto di montaggio */lvm*.

Questo esempio viene utilizzato per descrivere la procedura di estensione di un volume di partizione LVM.

Effettuare le operazioni seguenti:

1. Selezionare lo stato del volume /dev/mapper/VGTest-LVTest.

   # lvdisplay –m /dev/mapper/VGTest-LVTest

   --- Logical volume ---

   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

   ---Segments---

   Logical extent 0 to 2017:

   Type linear

   Physical volume /dev/sdc1

   Physical extents 0 to 2017

   Il volume fisico è */dev/sdc1*, il gruppo di volume è *VGTest* e il volume logico è */dev/VGTest/LVTest oppure /dev/mapper/VGTest-LVTest*.

2. Smontaggio del volume /dev/mapper/VGTest-LVTest.

   # umount /lvm

3. Disabilitare il gruppo di volume in cui risiede il volume fisico /dev/sdc1.

   # vgchange -a n VGTest

4. Creare una partizione per occupare lo spazio su disco inutilizzato mediante il comando fdisk.

   # fdisk -u /dev/sdc

   Command (m for help): p

   Disk /dev/sdc: 17.1 GB, 17179869184 bytes

   255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

   *Units = sectors of 1 * 512 = 512 bytes*

   Device Boot Start End Blocks Id System

   /dev/sdc1 63 16777215 8388576+ 83 Linux

   Command (m for help): n

   Command action

   e extended

   p primary partition (1-4)

   p

   Partition number (1-4): 2

   First sector (16777216-33554431, default 16777216):

   Using default value 16777216

   Last sector or +size or +sizeM or +sizeK (16777216-33554431, default 33554431):

   Using default value 33554431

   Command (m for help): p

   Disk /dev/sdc: 17.1 GB, 17179869184 bytes

   255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

   *Units = sectors of 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

Command (m for help): w

La partizione /dev/sdc2 viene creata.

5. Creare un nuovo volume fisico.

   # pvcreate /dev/sdc2

6. Estendere le dimensioni di gruppo del volume.

   # vgextend VGTest /dev/sdc2

7. Abilitare il gruppo di volume disabilitato.

   # vgchange -a y VGTest

8. Estendere le dimensioni del volume logico utilizzando il comando lvextend.

   # lvextend -L +8G /dev/VGTest/LVTest

9. Ridimensionare il volume utilizzando il comando resize2fs. Se necessario, eseguire prima il comando e2fsck.

   # e2fsck -f /dev/mapper/VGTest-LVTest

   # resize2fs /dev/mapper/VGTest-LVTest

10. Montare il volume sul punto di montaggio e verificare nuovamente lo stato del volume.

    # mount /dev/mapper/VGTest-LVTest /lvm

    # lvdisplay -m /dev/mapper/VGTest-LVTest

    ---Logical volume---

    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

--- Segments ---

Logical extent 0 to 2046:

Type linear

Physical volume /dev/sdc1

Physical extents 0 to 2046

Logical extent 2047 to 4065:

Type linear

Physical volume /dev/sdc2

Physical extents 0 to 2018

Il volume LVM viene esteso a 16 GB ed è pronto per essere utilizzato.

Verifica del ripristino del nodo di destinazione

Al completamento del processo di ripristino, verificare che il nodo di destinazione sia stato ripristinato e contenga i dati rilevanti.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione di cui è stato eseguito il ripristino.
2. Verificare che il computer di destinazione contenga tutte le informazioni di cui è stato eseguito il backup.

   La verifica del computer di destinazione viene eseguita correttamente.

   Il ripristino bare metal è stato eseguito correttamente per i computer Linux.

Esecuzione di un ripristino bare metal di migrazione per computer Linux

Il ripristino bare metal di migrazione è un processo composto da due fasi che prevede il ripristino dei dati prima su un computer temporaneo e, quindi, su quello effettivo. Quando è abilitata l'opzione di ripristino bare metal immediato, è possibile recuperare i dati su un computer temporaneo. Il computer temporaneo si può utilizzare finché non è pronto il computer effettivo. Quando è disponibile il computer effettivo, il ripristino bare metal di migrazione permette di trasferire i dati dal computer temporaneo a quello effettivo. Quando si esegue un ripristino bare metal di migrazione, tutti i dati creati sul computer temporaneo vengono trasferiti nel computer effettivo.

Nota: È possibile eseguire un ripristino bare metal di migrazione soltanto con i backup basati su agente. I backup senza agente non supportano il ripristino bare metal di migrazione.

È possibile eseguire un ripristino bare metal mediante l'indirizzo IP o l'indirizzo MAC del computer di destinazione. Se il computer di destinazione viene avviato mediante il Live CD dell'Agente Arcserve Unified Data Protection per Linux, è possibile ottenere l'indirizzo IP del computer di destinazione.

Nota: È possibile avviare il computer. È stata configurata una sola scheda NIC.

Per effettuare un ripristino bare metal di migrazione, completare le attività seguenti:

- Verifica dei prerequisiti per il ripristino bare metal di migrazione
- Esecuzione del ripristino bare metal sul computer temporaneo
- Esecuzione del ripristino bare metal di migrazione
- Verifica del ripristino del computer di destinazione

Verifica dei prerequisiti per il ripristino bare metal di migrazione

Prima di eseguire un ripristino bare metal di migrazione, controllare i seguenti punti:

- Si dispone di un punto di ripristino valido e della password di crittografia per il ripristino.
- Si dispone di un computer di destinazione valido per il ripristino bare metal.
- È stato creato Live CD dell'Agente Arcserve Unified Data Protection per Linux.
- Se si desidera eseguire il ripristino bare metal con l'indirizzo IP, è necessario acquisire l'indirizzo IP del computer di destinazione utilizzando Live CD.
- Se si desidera eseguire il ripristino bare metal PXE con l'indirizzo MAC, è necessario acquisire l'indirizzo MAC del computer di destinazione.
- È necessario che il punto di ripristino sia creato dal backup basato su agente Linux.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Esecuzione di un ripristino bare metal su un computer temporaneo

Prima di eseguire un ripristino bare metal di migrazione, è necessario ripristinare i dati dall'origine su un computer temporaneo. Per ripristinare i dati in modo temporaneo, è possibile eseguire il ripristino bare metal sul computer temporaneo. Una volta preparato il computer temporaneo, si può continuare a utilizzarlo.

Quando è pronto il computer effettivo, si può eseguire il ripristino bare metal di migrazione dal computer temporaneo a quello effettivo.

Nota: Per ulteriori informazioni sull'esecuzione del ripristino bare metal, consultare la sezione Esecuzione di un ripristino bare metal (BMR) per computer Linux.

Effettuare le operazioni seguenti:

1. Accedere alla procedura guidata di ripristino in uno dei modi seguenti:

   Da Arcserve UDP :

   a. Accedere ad Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata l'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux. La finestra di dialogo di selezione del tipo di ripristino viene visualizzata nell'interfaccia utente dell'agente.

   f. Selezionare il tipo di ripristino e fare clic su **OK**.

      Nota: si accede automaticamente al nodo agente e la **Procedura guidata di ripristino** viene visualizzata dal nodo agente.

   Dall'Agente Arcserve Unified Data Protection per Linux:

   a. Aprire l'interfaccia Web dell'Agente Arcserve Unified Data Protection per Linux.

      Nota: durante l'installazione dell'Agente Arcserve Unified Data Protection per Linux, l'URL per l'accesso e la gestione del server viene fornito all'utente.

   b. Accedere all'Agente Arcserve Unified Data Protection per Linux.

2. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Ripristino bare metal (BMR)**.

   Viene visualizzata la pagina **Server di backup** della **Procedura guidata di ripristino - Ripristino bare metal**.

3. Inserire i dettagli richiesti nella finestra **Procedura guidata di ripristino - Ripristino bare metal** e salvare.

4. Verificare che sia selezionata la casella di controllo **Abilita ripristino bare metal immediato** nella pagina **Computer di destinazione** della procedura guidata.

5. Verificare che sia selezionata la casella di controllo **Non eseguire il recupero automatico dei dati dopo l'avvio del computer** nella pagina **Computer di destinazione** della procedura guidata.

6. Eseguire il processo di ripristino bare metal.

   Il computer temporaneo viene recuperato utilizzando il ripristino bare metal con l'opzione di ripristino bare metal immediato abilitata. Il computer temporaneo si può utilizzare finché non è pronto il computer effettivo.

Esecuzione del ripristino bare metal di migrazione

Quando il computer effettivo è pronto, è possibile eseguire un ripristino bare metal di migrazione. Il ripristino bare metal di migrazione consente di ripristinare i dati originali dalla sessione di backup e i nuovi dati dal computer temporaneo sul computer effettivo.

Effettuare le operazioni seguenti:

1. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Ripristino bare metal di migrazione**.

   Viene visualizzata la pagina **Server di backup** della **Procedura guidata di ripristino - Ripristino bare metal di migrazione**.

2. Fornire tutti i dettagli nella **Procedura guidata di ripristino - Ripristino bare metal di migrazione**.

   Nota: Per ulteriori informazioni sull'esecuzione del ripristino bare metal, consultare la sezione Esecuzione di un ripristino bare metal (BMR) per computer Linux.

3. Verificare che nella pagina **Server di Backup** della procedura guidata vengano fornite le seguenti informazioni.

   a. Selezionare il processo di ripristino del computer virtuale istantaneo o il processo di ripristino bare metal immediato.

      Server locale

      indica che il server di backup è gestito localmente. Il processo di ripristino bare metal per il computer temporaneo viene eseguito sul server locale.

      Server remoto

      Indica che il server di backup è gestito in remoto. Il processo di ripristino bare metal per il computer temporaneo viene eseguito sul server remoto. Per la connessione al server remoto, è necessario fornire i dettagli relativi al server interessato.

   b. Selezionare il processo di ripristino dall'elenco a discesa Nome processo.

      Una volta pronto per l'uso, nell'elenco viene visualizzato il processo di ripristino di computer virtuale istantaneo o il processo di ripristino bare metal immediato il cui stato è pronto per l'uso o disattivato.

4. Salvare il processo di ripristino bare metal.

Nella pagina principale, la voce **Job Phase (Fase processo)** nella scheda **Stato processo** viene modificata in **Click here to migrate data (Fare clic qui per migrare i dati)**.

5. (Facoltativo) Quando il tipo di processo selezionato è un ripristino bare metal immediato, avviare il computer temporaneo utilizzando un Live CD.
6. Dalla scheda **Stato processo**, selezionare **Fare clic qui per eseguire la migrazione dei dati**.

   La migrazione dei dati viene avviata.

   Il ripristino bare metal di migrazione è stato eseguito correttamente.

Verifica del ripristino del nodo di destinazione

Al completamento del processo di ripristino, verificare che il nodo di destinazione sia stato ripristinato e contenga i dati rilevanti.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione di cui è stato eseguito il ripristino.
2. Verificare che il computer di destinazione contenga tutte le informazioni del computer temporaneo, inclusi tutti i nuovi dati creati sul computer temporaneo.

   La verifica del computer di destinazione viene eseguita correttamente.

   La migrazione del ripristino bare metal è stata eseguita correttamente per i computer Linux basati sull'agente.

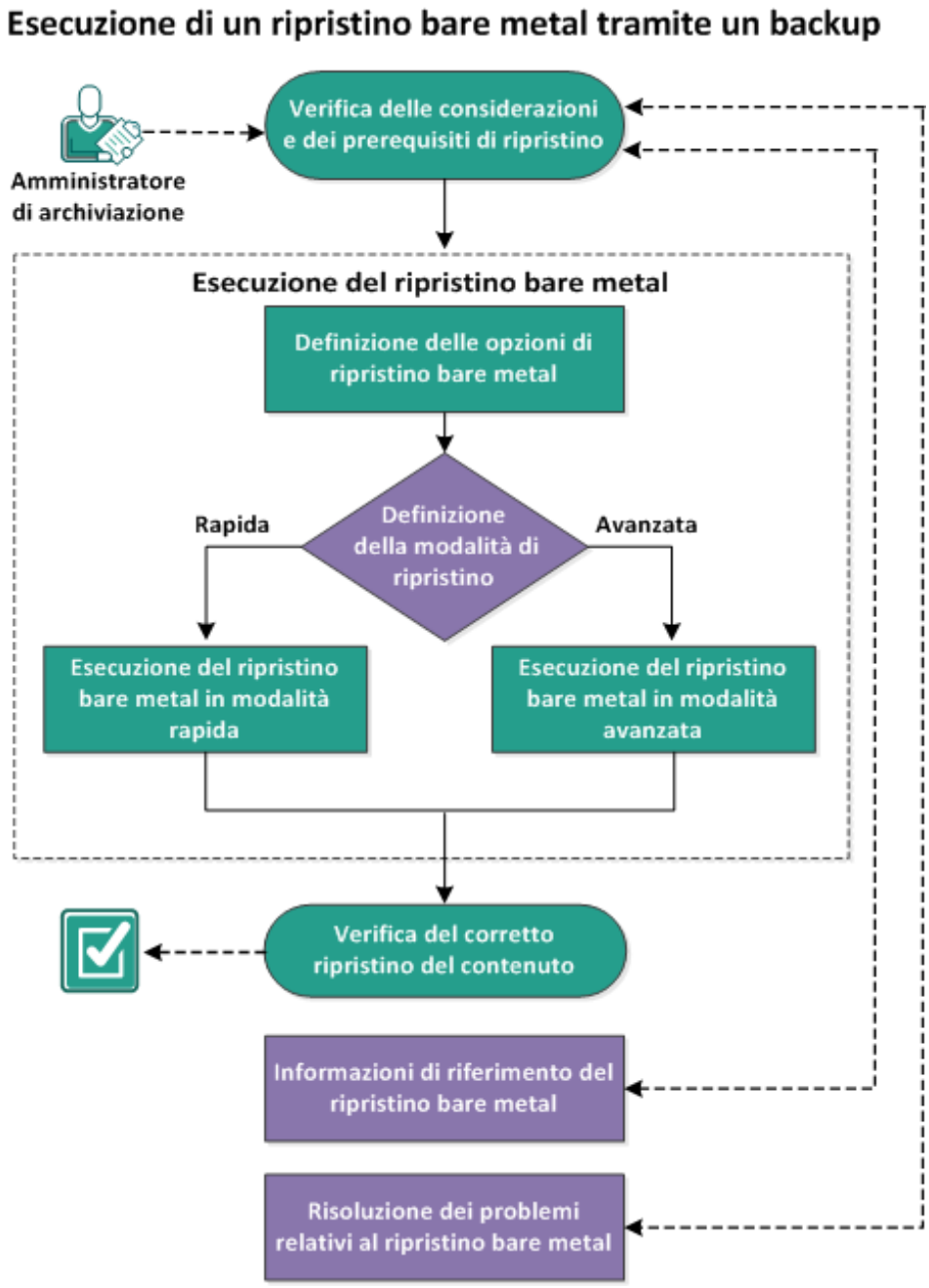
Esecuzione di un ripristino bare metal mediante un backup

Il processo di ripristino bare metal (BMR) consiste nel ripristino di interi sistemi ed include la reinstallazione del sistema operativo e delle applicazioni software nonché il ripristino di dati e impostazioni. Il processo di ripristino bare metal consente di eseguire facilmente il ripristino completo di un computer, incluso in caso di hardware diverso. È possibile eseguire il ripristino bare metal poiché durante il processo di backup a livello di blocco, l'agente Arcserve UDP (Windows) acquisisce non solo i dati, ma anche tutte le informazioni relative alle seguenti applicazioni:

- Sistema operativo
- Applicazioni installate
- Impostazioni di configurazione
- Driver necessari

Le informazioni necessarie per l'esecuzione di una ricostruzione completa di interi sistemi da bare metal vengono sottoposte a backup in una serie di blocchi ed archiviate nella posizione di backup.

Nel diagramma seguente viene illustrato il processo di esecuzione di un ripristino bare metal mediante backup:



Completare le attività seguenti per eseguire un ripristino bare metal mediante backup:

1. Verifica delle considerazioni e dei prerequisiti del ripristino bare metal
2. Definizione delle opzioni di ripristino bare metal
   - Esecuzione del ripristino bare metal in modalità rapida
   - Esecuzione del ripristino bare metal in modalità avanzata
3. Verifica della corretta esecuzione del ripristino bare metal

4. Informazioni di riferimento del ripristino bare metal
5. Risoluzione dei problemi relativi al ripristino bare metal

Verifica delle considerazioni e dei prerequisiti del ripristino bare metal

Verificare l'esistenza dei seguenti prerequisiti prima di procedere a un ripristino bare metal:

- È necessario disporre di una delle seguenti immagini:
  - Un'immagine ISO di ripristino bare metal masterizzata su un CD/DVD
  - Un'immagine ISO di ripristino bare metal masterizzata su una periferica USB portatile

  Nota: L'agente Arcserve UDP (Windows) consente di utilizzare un'utilità di kit di avvio per combinare un'immagine WinPE e un'immagine dell'agente Arcserve UDP (Windows) per la creazione di un'immagine ISO di ripristino bare metal. Tale immagine viene quindi masterizzata su un supporto di avvio. Sarà quindi possibile utilizzare tali supporti di avvio (CD/DVD o periferica USB) per avviare il nuovo sistema del computer e consentire l'avvio del processo di ripristino bare metal. Al fine di garantire che l'immagine salvata corrisponda sempre alla versione più recente, creare una nuova immagine ISO per ogni aggiornamento dell'agente Arcserve UDP (Windows).
- Almeno un backup completo.
- Almeno 2 GB di RAM installati sul computer virtuale e il server di origine di cui si sta eseguendo il recupero.
- Se si desidera eseguire il recupero di computer virtuali VMware su computer virtuali VMware configurati come server fisici, verificare che gli strumenti VMware siano installati sul computer virtuale di destinazione.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Verificare le seguenti considerazioni sul ripristino:

- Il processo di ripristino bare metal non cambia, indipendentemente dal metodo utilizzato per la creazione dell'immagine del kit di avvio.

  Nota: Il processo di ripristino bare metal non è in grado di creare spazi di archiviazione. Se il computer di origine dispone di spazi di archiviazione, durante il ripristino bare metal non sarà possibile creare spazi di archiviazione sul computer di destinazione. È inoltre possibile eseguire il ripristino di tali volumi su dischi o volumi regolari oppure creare manualmente spazi di archiviazione prima dell'esecuzione del ripristino bare metal ed eseguire il ripristino dei dati negli spazi di archiviazione creati.

- Il ripristino dei dischi dinamici viene eseguito solo a livello del disco. Se il backup dei dati avviene su un volume locale che risiede su un disco dinamico, tale disco non potrà essere ripristinato durante il ripristino bare metal. In tal caso, per eseguire il ripristino durante il ripristino bare metal è necessario eseguire una delle attività seguenti e quindi eseguire il ripristino bare meta dal punto di ripristino copiato:
  - Eseguire il backup su un volume di un'altra unità.
  - Eseguire il backup su una condivisione remota.
  - Copiare un punto di ripristino su una destinazione diversa.

  Nota: se si esegue il ripristino bare metal con dischi dinamici multipli, il ripristino potrà non riuscire a causa di alcuni errori imprevisti (come errori di avvio, volumi dinamici non riconosciuti, eccetera). Se ciò si verifica, sarà necessario eseguire il ripristino del disco mediante ripristino bare metal quindi, una volta riavviato il computer, sarà possibile ripristinare i volumi dinamici in un ambiente normale.
- (Facoltativo) Verificare le informazioni di riferimento del ripristino bare metal. Per ulteriori informazioni, consultare i seguenti argomenti:
  - Funzionamento del ripristino bare metal
  - Sistemi operativi che supportano la conversione UEFI/BIOS
  - Gestione del menu delle operazioni di ripristino bare metal

Verificare le seguenti considerazioni:

- Se si esegue l'aggiornamento a una versione o release più recente di Arcserve UDP, è necessario ricreare l'immagine ISO di ripristino bare metal secondo il livello di Windows AIK o ADK appropriato per includere il supporto delle funzionalità e delle correzioni di errori più recenti. Tuttavia, una volta creata un'immagine ISO di ripristino bare metal, è possibile utilizzare il file .ISO per lo stesso livello di sistema operativo. I seguenti livelli di sistema operativo possono utilizzare la stessa immagine ISO:
  - ISO creata mediante Windows 7 WAIK (valido per Windows 2003, Vista, 2008, 2008 R2)
  - ISO creato mediante Windows 8/8.1 ADK (valido per Windows 8, 8.1, Server 2012, Server 2012 R2)
  - ISO creata mediante Windows 10 ADK (valido per Windows 10, Windows Server 2016 e Windows Server 2019)

Definizione delle opzioni di ripristino bare metal

Prima di avviare il processo di ripristino bare metal, è necessario specificare alcune opzioni preliminari relative al ripristino.

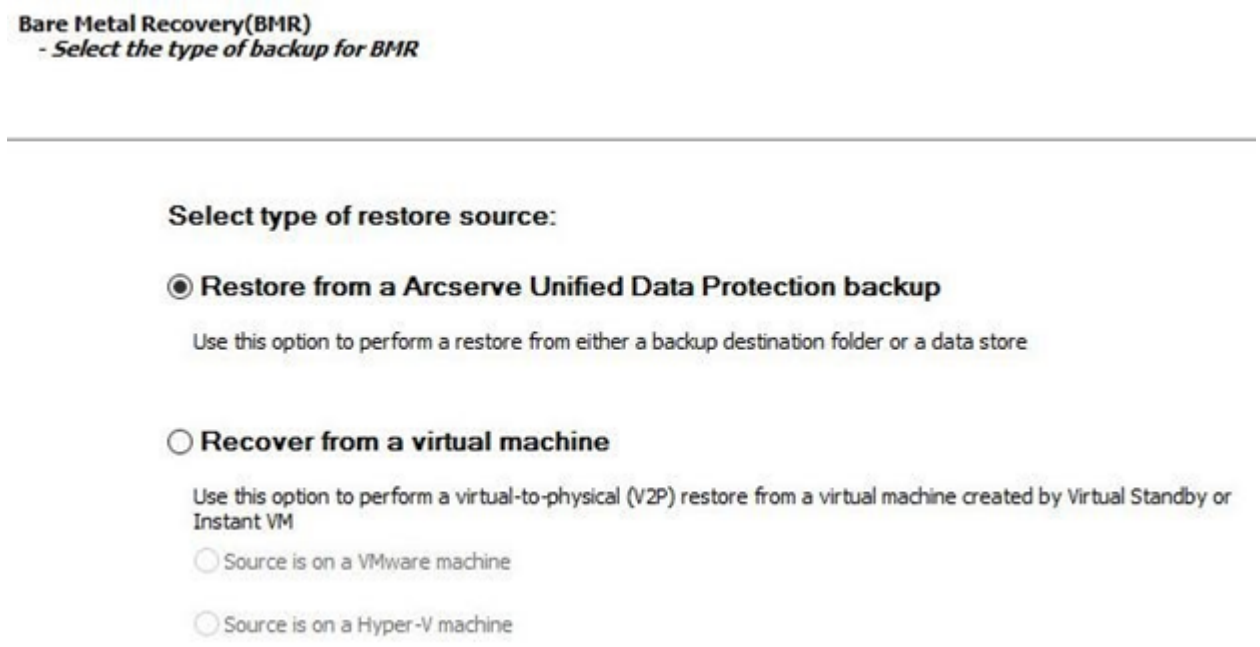
Effettuare le operazioni seguenti:

1. Inserire il supporto contenente l'immagine del kit di avvio salvata e avviare il computer.
   - Se si utilizza un'immagine ISO di ripristino bare metal masterizzata su CD/DVD, inserire il CD/DVD salvato.
   - Se si utilizza un'immagine ISO di ripristino bare metal masterizzata su una periferica USB, inserire la periferica USB salvata.

   Verrà visualizzata la schermata dell'**utilità di installazione BIOS**.
2. In questa schermata, selezionare l'opzione dell'**utilità di installazione BIOS** o l'opzione USB per inizializzare il processo di avvio. Selezionare un'architettura (x86/-x64) e premere **Invio** per continuare.
3. Viene visualizzata la schermata di selezione della lingua dell'agente Arcserve UDP (Windows). Selezionare una lingua e fare clic su **Avanti** per continuare.



Il processo di ripristino bare metal viene avviato e viene visualizzata la schermata della procedura guidata di ripristino bare metal.



La schermata della procedura guidata del ripristino bare metal consente di selezionare il tipo di ripristino bare metal che si desidera eseguire:

- **Ripristino da un backup di Arcserve Unified Data Protection**

  Utilizzare questa opzione per eseguire il ripristino da una cartella di destinazione del backup o da un archivio dati.

  Questa opzione consente di ripristinare i dati di cui è stato eseguito il backup mediante l'agente Arcserve UDP (Windows). Questa opzione viene utilizzata nel caso di sessioni di backup eseguite con l'agente Arcserve UDP (Windows) oppure con l'applicazione Arcserve UDP Host-Based VM Backup.

  Se si seleziona questa opzione, continuare questa procedura da questo punto.

- **Recupera da computer virtuale**

  Utilizzare questa opzione per eseguire un ripristino virtual-to-physical (V2P) da un computer virtuale Virtual Standby. Virtual-to-physical (V2P) è un termine che fa riferimento alla migrazione di un sistema operativo, dei programmi applicativi e dei dati da un computer virtuale o una partizione del disco al disco rigido principale di un computer. La destinazione può essere uno o più computer.

- **L'origine è su un computer VMware**

  Consente di eseguire il recupero dei dati per un computer la cui conversione virtuale viene eseguita da un computer virtuale VMware. Questa opzione viene utilizzata per l'applicazione Arcserve Central Virtual Standby.

  Nota: l'opzione consente di eseguire il recupero dei dati solo se la conversione virtuale a file VMDK (per VMware) è stata eseguita mediante Arcserve Central Virtual Standby.

  Se si seleziona questa opzione, consultare la sezione Recupero mediante computer virtuale Virtual Standby VMware per continuare la procedura.

  Per ulteriori informazioni, consultare la sezione Ripristino mediante computer virtuale Virtual Standby VMware nella Guida in linea dell'agente per Windows.

- **L'origine è su un computer Hyper-V**

  Consente di eseguire il recupero dei dati per un computer la cui conversione virtuale viene eseguita da un computer virtuale Hyper-V. Questa opzione viene utilizzata per l'applicazione Arcserve Central Virtual Standby.

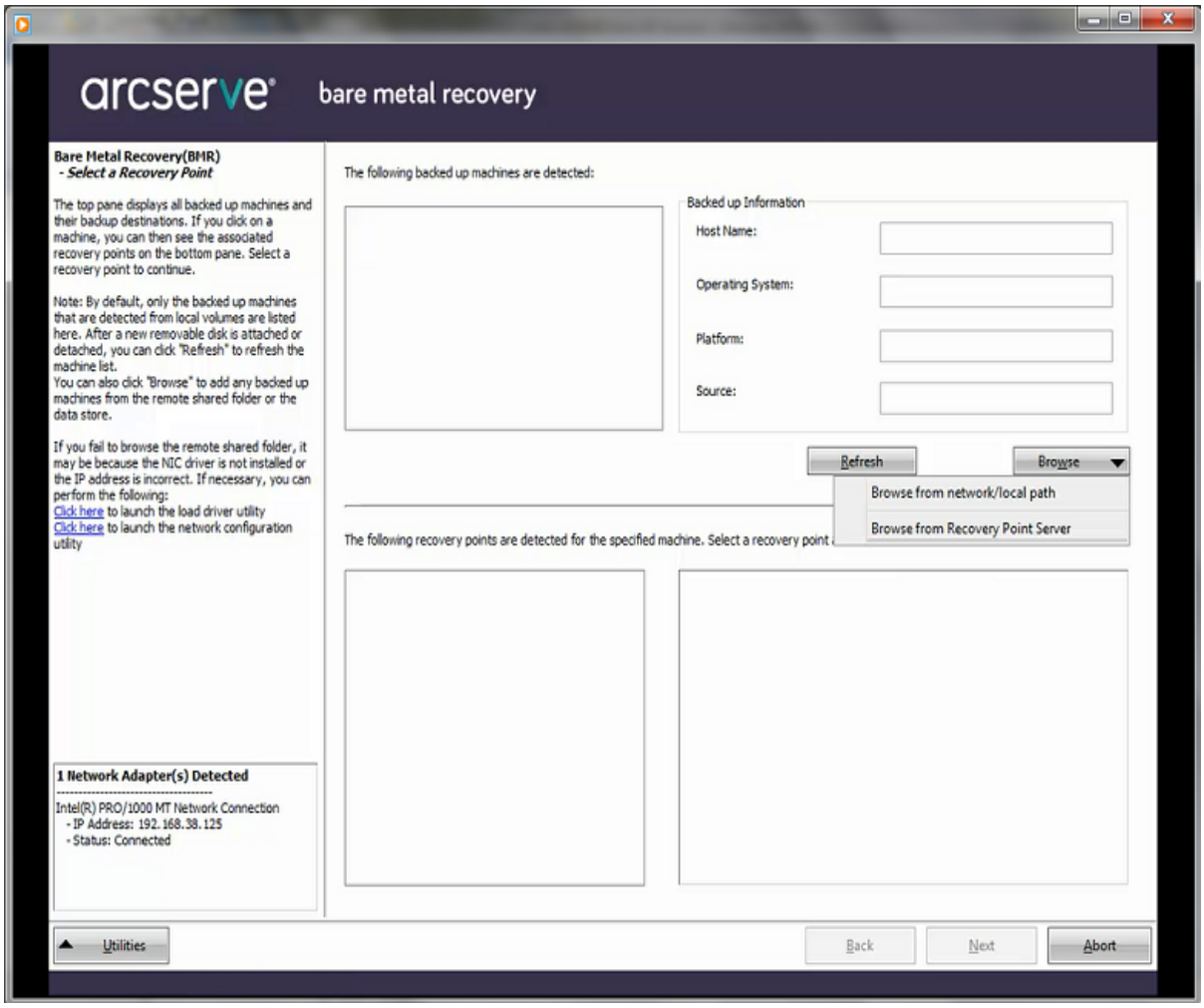
  Nota: l'opzione consente di eseguire il recupero dei dati solo se la conversione virtuale a file VHD (per Hyper-V) è stata eseguita mediante Arcserve Central Virtual Standby.

  Se si seleziona questa opzione, consultare la sezione Recupero mediante computer virtuale Virtual Standby Hyper-V per continuare la procedura.

  Per ulteriori informazioni, consultare la sezione Ripristino mediante computer virtuale Virtual Standby Hyper-V nella Guida in linea dell'agente per Windows.

4. Selezionare **Ripristino da un backup di Arcserve Unified Data Protection** e fare clic su **Avanti**.

   Viene visualizzata la schermata della procedura guidata **Seleziona punto di ripristino**.



5. Dalla schermata della procedura guidata **Selezionare un punto di ripristino**, fare clic su **Sfoglia** e selezionare **Sfoglia da rete/percorso locale** o **Sfoglia da Recovery Point Server**.

    a. Se si seleziona **Sfoglia** da rete/percorso locale, selezionare il computer o il volume con i punti di ripristino per l'immagine di backup.

    L'agente Arcserve UDP (Windows) consente di eseguire il ripristino da un'unità locale o da una condivisione di rete.

    - Se si esegue il recupero da un backup locale, la procedura guidata di ripristino bare metal individua e visualizza automaticamente tutti i volumi che contengono punti di ripristino.
    - Se si sta eseguendo il recupero da una condivisione remota, individuare la posizione remota di archiviazione dei punti di ripristino. Se i punti di ripristino sono contenuti su più computer, verranno visualizzati tutti i computer.

Potrebbe essere necessario disporre delle informazioni di accesso (nome utente e password) del computer remoto.

Nota: per poter individuare i punti di ripristino remoti, la rete deve essere attiva e in esecuzione. Se necessario, è possibile verificare o aggiornare le informazioni relative alla configurazione di rete oppure caricare i driver mancanti dal menu Utilità.

- Se il modulo di ripristino bare metal non è in grado di individuare alcun volume di destinazione locale, viene visualizzata automaticamente la finestra di dialogo **Selezionare una cartella**. Specificare la condivisione remota su cui risiede il backup.
- Se si esegue il ripristino da una destinazione iSCSI, il modulo di ripristino bare metal potrebbe non rilevare la destinazione. Pertanto, potrebbe essere necessario eseguire le seguenti operazioni:

  1. Fare clic su **Utilità**, selezionare **Esegui** dal menu pop-up, digitare **cmd**, quindi fare clic su **OK**.

  2. Nella finestra del prompt dei comandi, utilizzare i seguenti comandi Windows iSCSI per impostare le connessioni iSCSI:

  > net start msiscsi

  > iSCSICLI QAddTargetPortal <TargetPortalAddress>

  > iSCSICLI QLoginTarget <TargetName > [CHAP username] [CHAP password]

  Nota: CHAP = Challenge-Handshake Authentication Protocol

  Per ulteriori informazioni sulle opzioni della riga di comando di Windows iSCSI, consultare il seguente collegamento.

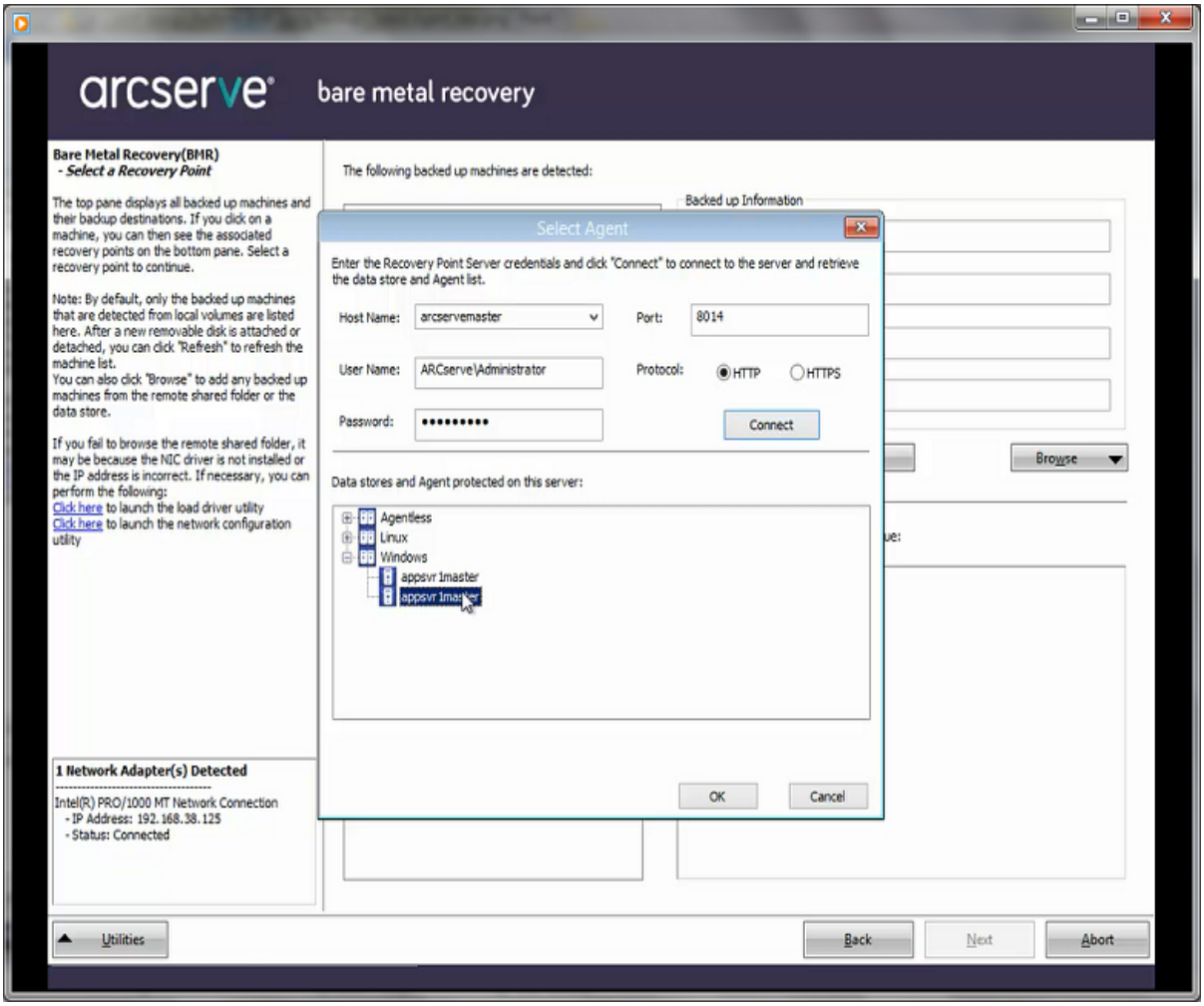
  Nota: potrebbero essere necessarie ulteriori operazioni in base al software di destinazione iSCSI utilizzato. Per ulteriori informazioni, consultare il manuale del software di destinazione iSCSI.

  3. La schermata di ripristino bare metal dovrebbe contenere i dischi/volumi connessi mediante il disco iSCSI. È ora possibile utilizzare il disco iSCSI come volume di origine o volume di destinazione del backup.

  Nota: il ripristino bare metal non supporta l'installazione del sistema operativo su un disco iSCSI. Sono supportati soltanto i dischi di dati.

b. Se si sceglie di accedere dal **Recovery Point Server**, viene visualizzata la finestra di dialogo di **selezione dell'agente.** Immettere il **nome host del Reco-**

very Point Server, il **nome utente**, la **password**, la **porta** e il **protocollo**. Fare clic su **Connetti**.



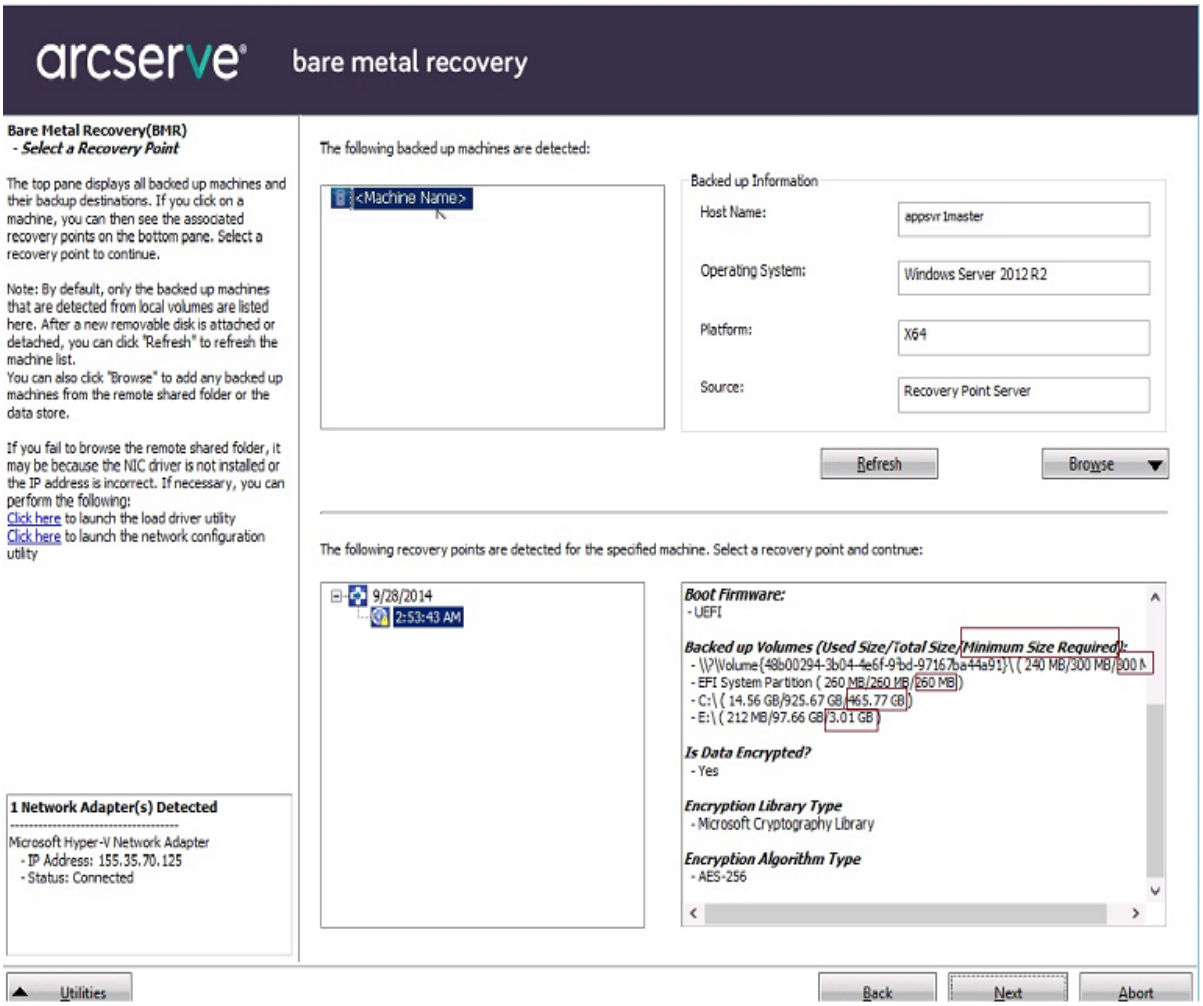
6. Selezionare la cartella o il nome dell'agente nell'archivio dati in cui sono archiviati i punti di ripristino per il backup, quindi fare clic su **OK**.

   La schermata della procedura guidata di ripristino bare metal visualizza le informazioni seguenti:

   - Nome computer (nel riquadro in alto a sinistra).
   - Informazioni di backup (riquadro destro superiore).
   - Punti di ripristino corrispondenti (riquadro sinistro inferiore).

     Nota: i sistemi operativi supportati consentono di eseguire un ripristino bare metal a partire a un backup eseguito su un computer UEFI su un computer BIOS e da un computer BIOS su un computer UEFI. Consultare la sezione Sistemi operativi che supportano la conversione UEFI/BIOS per un elenco completo di sistemi supportati per la conversione firmware.

- Per sistemi operativi che non supportano la conversione firmware, è necessario avviare il computer in modalità UEFI per l'esecuzione di un ripristino bare metal per un sistema UEFI. Il ripristino bare metal non supporta il ripristino di un computer con firmware diverso. Per verificare che il firmware di avvio utilizzato corrisponde a UEFI e non BIOS, fare clic su **Utilità** e selezionare **Informazioni**.
- Per sistemi operativi che supportano la conversione firmware, dopo aver selezionato il punto di ripristino, se il computer di origine non corrisponde al firmware del sistema, verrà richiesto se si desidera convertire il sistema UEFI in un sistema compatibile con BIOS o il sistema BIOS in un sistema compatibile con UEFI.



Nota: Arcserve UDP Versione 5.0 Aggiornamento 2 supporta soltanto ripristini bare metal su un disco più piccolo quando viene eseguito il backup delle sessioni da tale aggiornamento. Fare riferimento al campo **Dimensioni minime richieste** per la dimensione del disco di destinazione. Il ripristino

bare metal su un disco più piccolo è supportato soltanto in **modalità avanzata**.

7. Selezionare il punto di ripristino da ripristinare.

   Vengono visualizzate le informazioni relative al punto di ripristino selezionato (riquadro destro inferiore). La visualizzazione include informazioni quali il tipo di backup eseguito (e salvato), la destinazione di backup e i volumi di cui è stato eseguito il backup.

   Se il punto di ripristino contiene sessioni crittografate, l'icona del punto di ripristino con forma di orologio presenta un lucchetto e viene visualizzata una schermata per l'immissione della password. Immettere la password di sessione, quindi fare clic su **OK**.

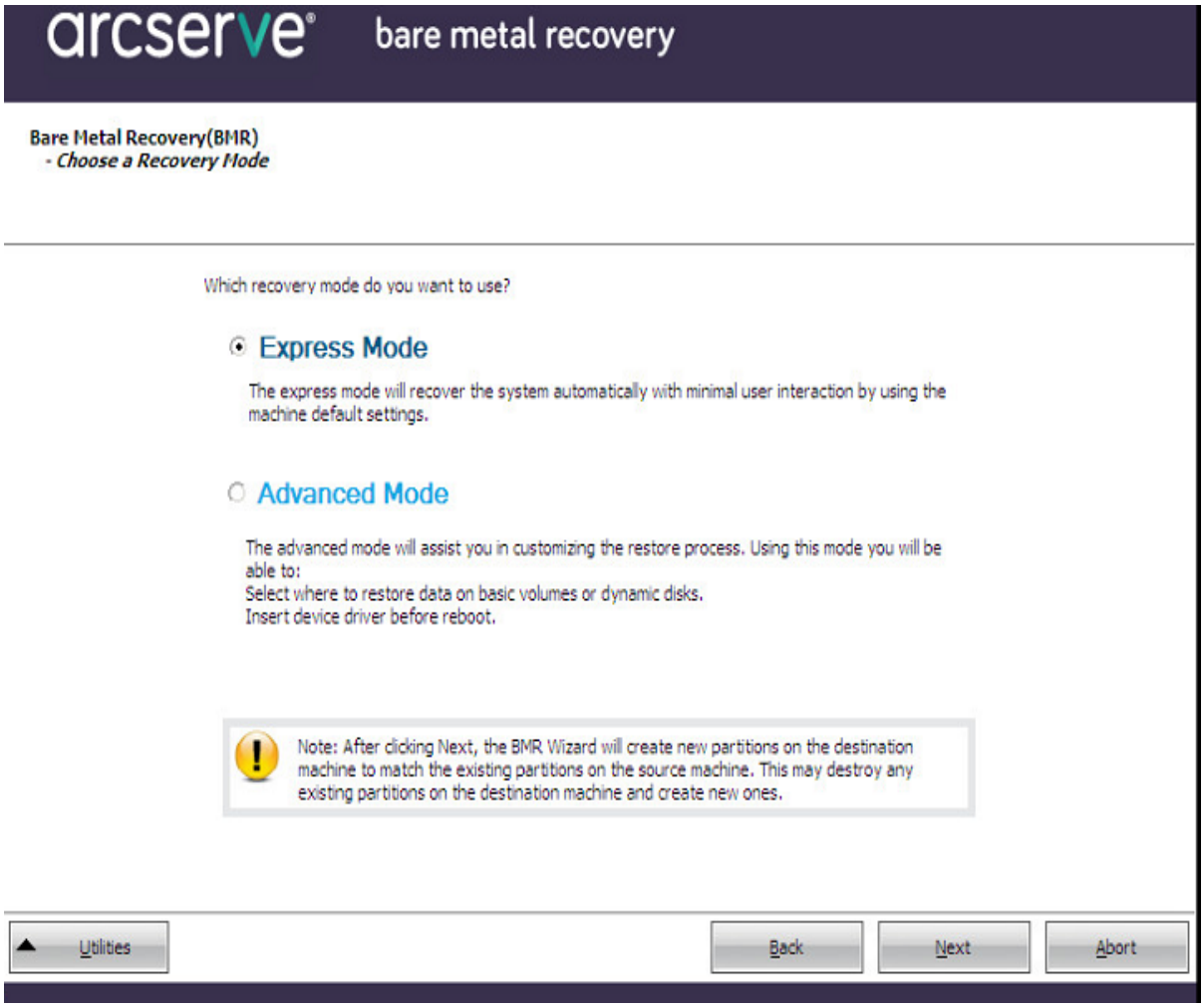
   Note:

   In caso di ripristino da un Recovery Point Server di Arcserve UDP, viene richiesto di fornire una password di sessione.

   Se il computer in uso è un controller di dominio, l'agente Arcserve UDP (Windows) supporta il ripristino non autorevole del file del database Active Directory durante il ripristino bare metal. (Non supporta il ripristino di cluster MSCS).

8. Verificare che il punto di ripristino selezionato sia corretto, quindi selezionare **Avanti**.

   Viene visualizzata la schermata della procedura guidata di ripristino bare metal e le opzioni della modalità di recupero.



Le opzioni disponibili sono **Modalità avanzata** e **Modalità rapida**.

- Selezionare Modalità rapida se si desidera intervenire in modo limitato nel processo di recupero.
- Selezionare Modalità avanzata per personalizzare il processo di recupero.

  Impostazione predefinita: Modalità rapida.

Esecuzione del ripristino bare metal in modalità rapida

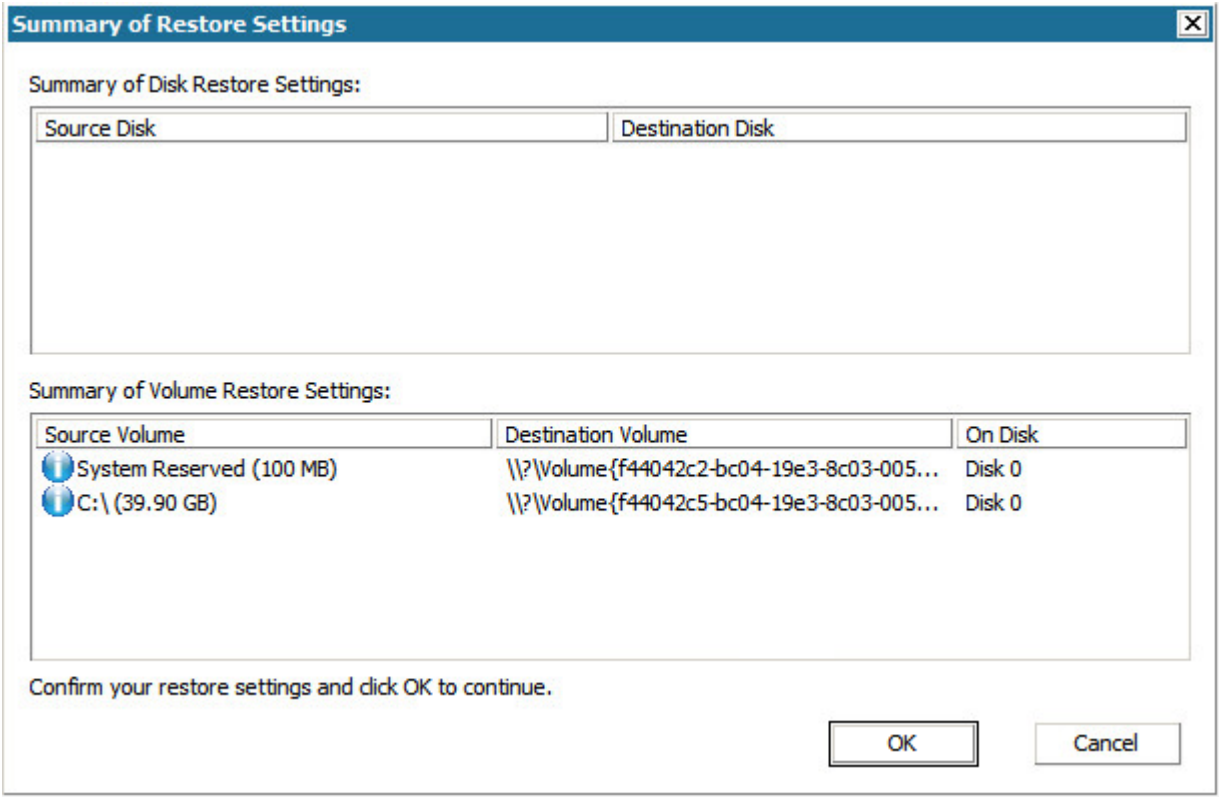
La Modalità rapida richiede un'interazione minima durante il processo di recupero.

Effettuare le operazioni seguenti:

1. Dalla finestra di dialogo **Selezionare una modalità di recupero**, selezionare **Modalità rapida** e fare clic su **Avanti**.

   Verrà visualizzata la schermata **Riepilogo delle impostazioni di ripristino del disco** contenente un riepilogo dei volumi da ripristinare.

   Nota: nella parte superiore della finestra Riepilogo ripristino, le lettere corrispondenti alle unità elencate nella colonna **Volume di destinazione** vengono generate automaticamente dall'Ambiente di preinstallazione di Windows (WinPE). È possibile che tali lettere di unità non corrispondano alle lettere elencate nella colonna **Volume di origine**. Tuttavia, il ripristino dei dati verrà eseguito sul volume appropriato anche se le lettere di unità sono diverse.

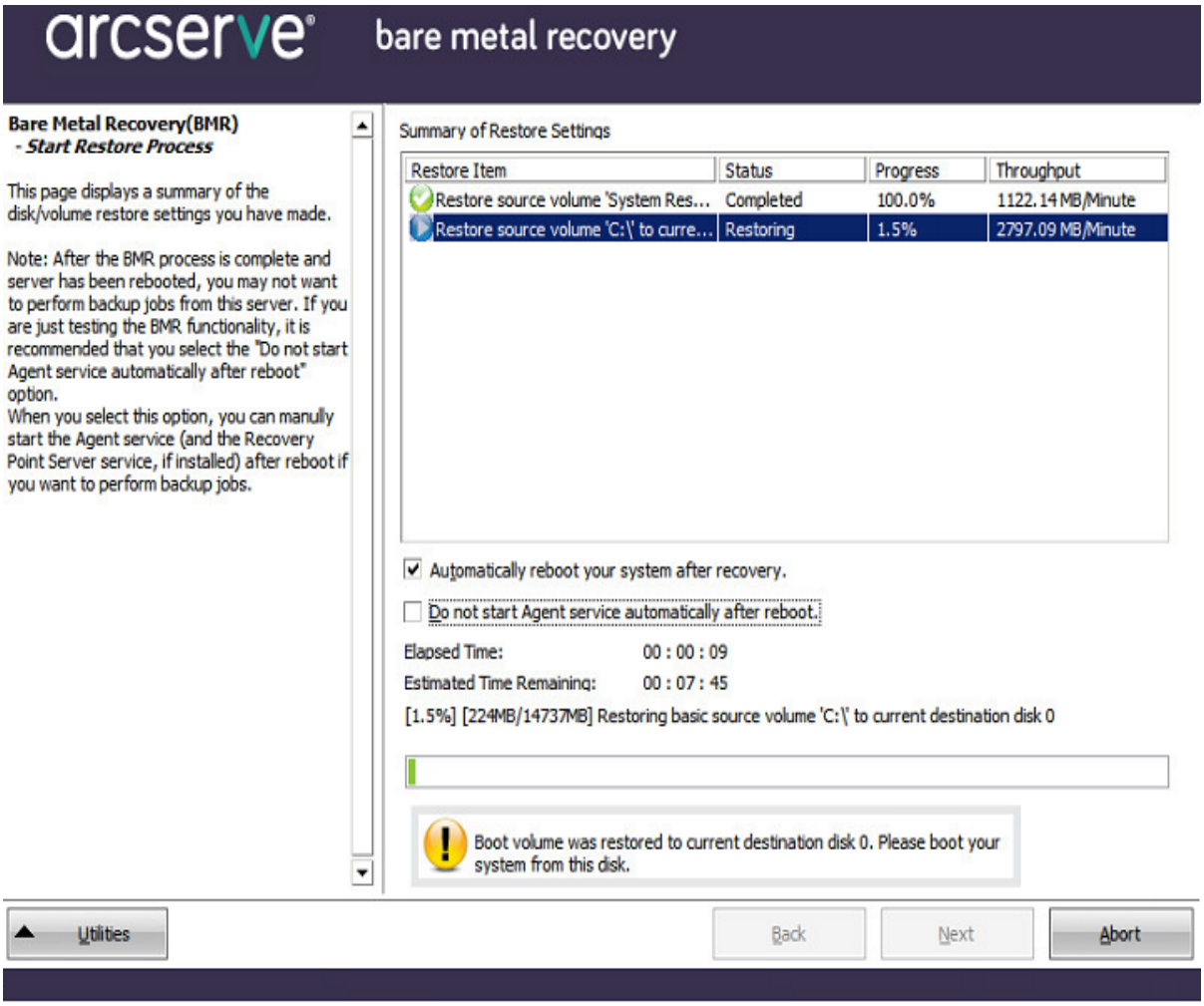


2. Verificare che le informazioni di riepilogo siano corrette, quindi fare clic su **OK**.

   Verrà avviato il processo di ripristino. La schermata della procedura guidata di ripristino bare metal visualizza lo stato di ripristino per ciascun volume.

- Il tempo necessario per l'esecuzione di questa operazione dipende dalle dimensioni del volume da ripristinare.
- Durante questo processo viene eseguito il ripristino blocco per blocco di tutti i dati di backup di tale punto di ripristino e viene creata una replica del computer di origine sul computer di destinazione.
- L'opzione di riavvio automatico del sistema in seguito al recupero è selezionata per impostazione predefinita. Se lo si desidera, è possibile deselezionare questa opzione ed eseguire il riavvio manuale in un secondo momento.

  Importante: se è in corso il recupero autorevole di Active Directory dopo un ripristino bare metal, è necessario deselezionare l'opzione di **riavvio automatico del sistema in seguito al ripristino**. Per ulteriori informazioni, consultare la sezione Ripristino autorevole di Active Directory dopo un ripristino bare metal.
- Se necessario, è possibile selezionare di non avviare automaticamente il servizio Agente dopo il riavvio.
- Se necessario, è possibile annullare o interrompere l'operazione in qualsiasi momento.



3. Dal menu **Utilità**, è possibile accedere al **registro attività** del ripristino bare metal e utilizzare l'opzione **Salva** per salvare il registro attività.

   Per impostazione predefinita, il salvataggio del registro attività viene effettuato nella posizione seguente:

   X:\windows\system32\dr\log

   Nota: per evitare la generazione di un errore Windows, si consiglia di non utilizzare l'opzione **Salva con nome** della finestra di dialogo del registro attività del ripristino bare metal per salvare il registro attività sul desktop o per creare una nuova cartella sul desktop.

4. Se si sta eseguendo il ripristino su hardware diversi (la scheda SCSI/FC utilizzata per la connessione ai dischi rigidi potrebbe essere stata modificata) e non viene rilevato nessun driver compatibile nel sistema originale, viene visualizzata la pagina di inserimento del driver per consentire all'utente di specificare i driver necessari per le periferiche.

È possibile individuare e selezionare i driver da inserire nel sistema ripristinato. In tal modo è possibile eseguire il ripristino su un computer con hardware diversi.

Una volta completato il processo di ripristino bare metal, viene visualizzata una notifica di conferma.

Esecuzione del ripristino bare metal in modalità avanzata

La **Modalità avanzata** consente di personalizzare il processo di recupero.

Effettuare le operazioni seguenti:

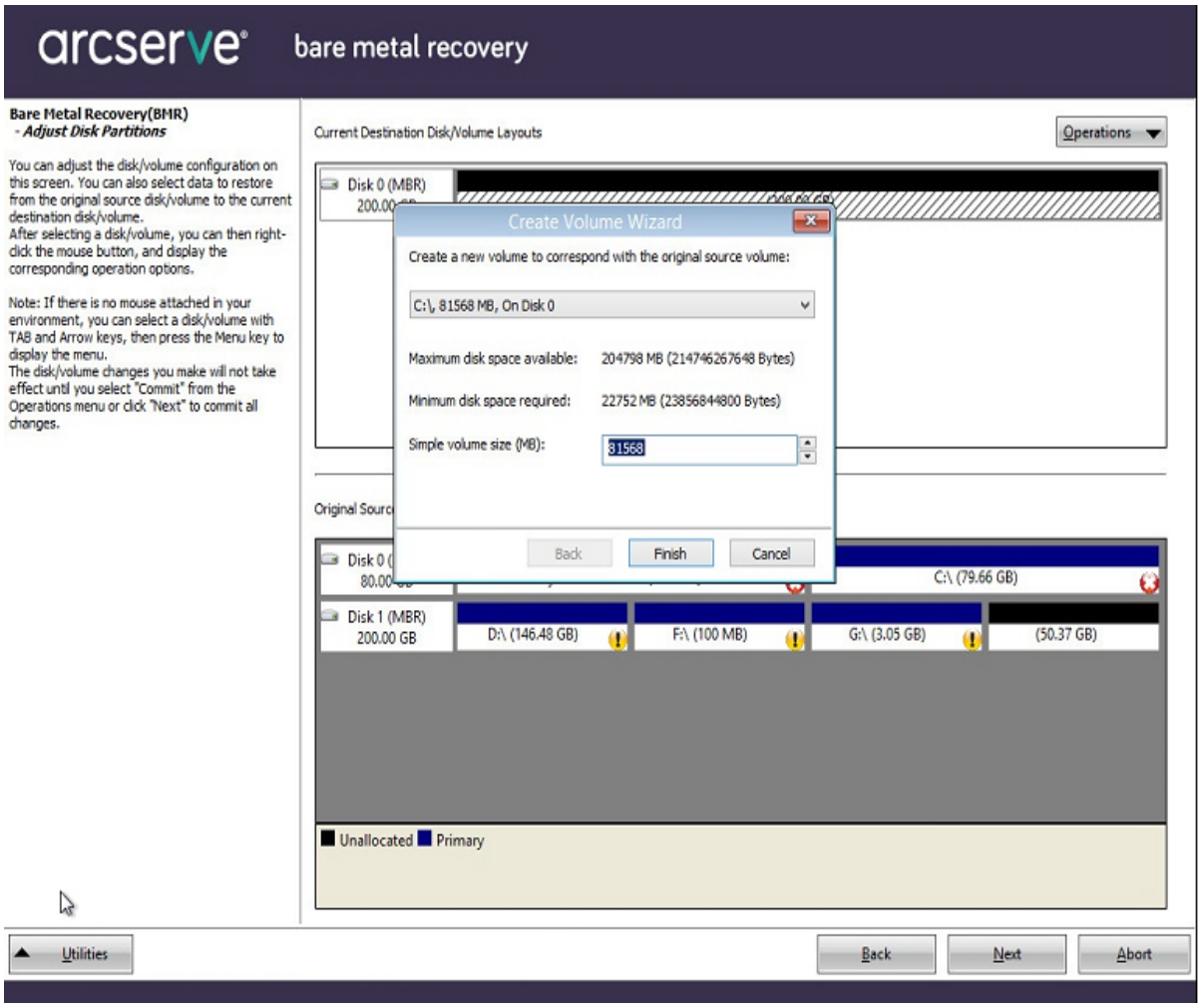
1. Dalla finestra di dialogo **Selezionare una modalità di recupero**, selezionare **Modalità avanzata** e fare clic su **Avanti**.

   L'utilità di ripristino bare metal esegue la ricerca del computer da recuperare e visualizza le informazioni relative alla partizione del disco corrispondente.

   Il riquadro superiore mostra la configurazione del disco presente sul computer corrente (destinazione), mentre il riquadro inferiore mostra le informazioni relative alla partizione del disco del computer originale (origine).

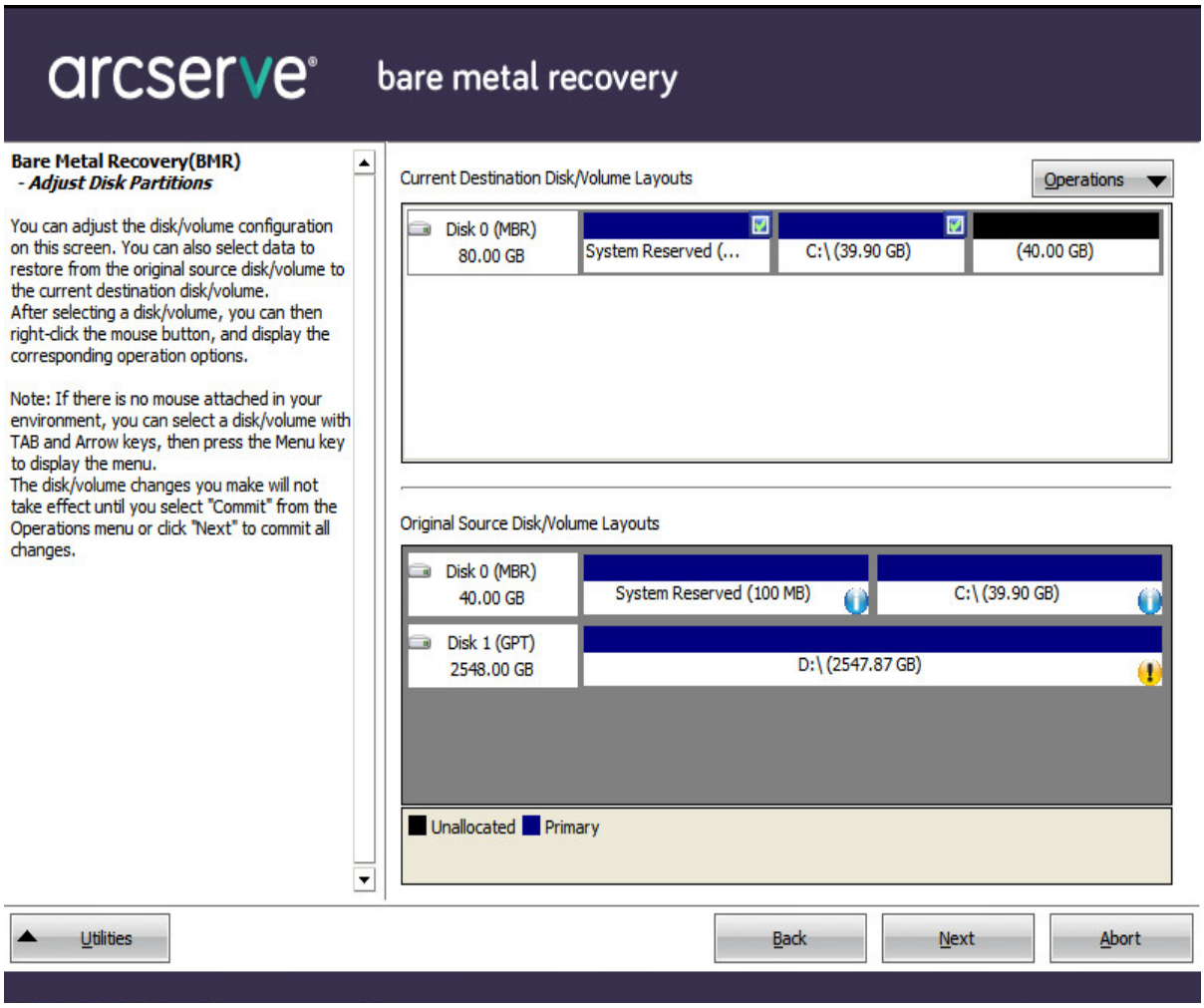
   Importante! Se nel riquadro inferiore il volume di origine viene contrassegnato da una X rossa, significa che tale volume contiene informazioni di sistema e che non è stato assegnato (mappato) al volume di destinazione. Il volume contenente le informazioni di sistema dovrà essere assegnato dal disco di origine al disco di destinazione e ripristinato durante il processo di ripristino bare metal. In caso contrario, non sarà possibile eseguire il riavvio.

   È possibile creare volumi in un disco più piccolo a seconda del valore consigliato di **spazio su disco minimo richiesto**. Nell'esempio, le dimensioni originali del volume sono pari a 81568 MB. Quando si crea il volume sul disco di destinazione, le dimensioni minime consigliate sono pari a 22752 MB. In questo caso, è possibile creare il volume originale con dimensioni di 22752 MB.



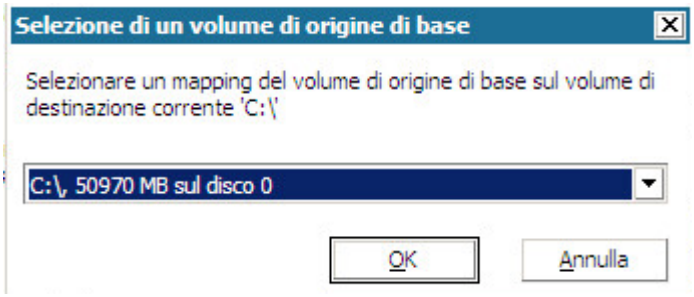
Nota: Se si esegue il ripristino bare metal del volume di sistema su un disco non configurato come disco di avvio, non sarà possibile avviare il computer in seguito al completamento del ripristino bare metal. Assicurarsi di eseguire il ripristino del volume di sistema su un disco di avvio configurato correttamente.

Nota: In caso di ripristino su un altro disco/volume, la capacità del nuovo disco/-volume può essere delle stesse dimensioni, maggiore o minore rispetto al disco/-volume originale. Inoltre, il ridimensionamento del volume non si applica ai dischi dinamici.



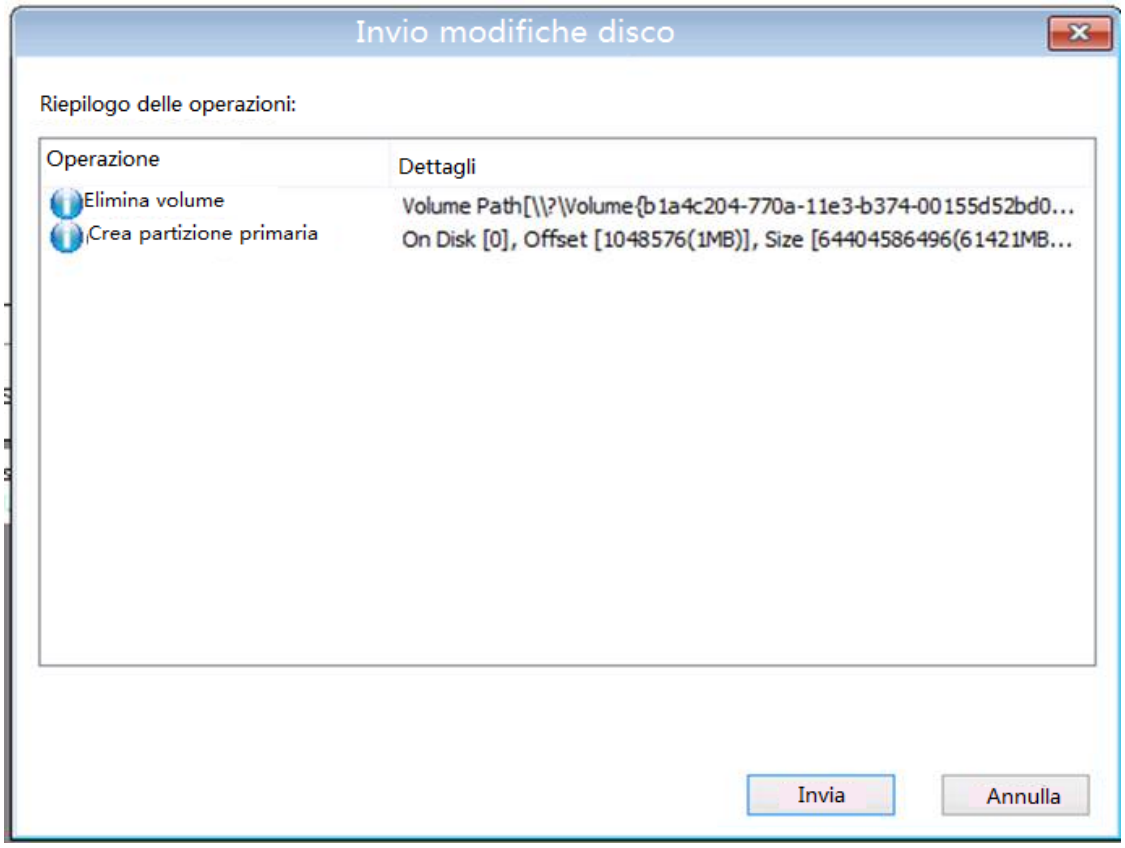
2. Se le informazioni del disco non vengono visualizzate correttamente, accedere al menu **Utilità** e verificare se sono richiesti driver mancanti.
3. Se necessario, nel riquadro del disco/volume di destinazione, è possibile fare clic sul menu a discesa **Operazioni** e visualizzare le opzioni disponibili. Per ulteriori informazioni sulle opzioni, consultare la sezione Gestione del menu delle operazioni di ripristino bare metal.
4. Per assegnare un volume di origine al volume di destinazione, fare clic su ciascun volume di destinazione e, dal menu di scelta rapida, selezionare l'opzione **Esegui mapping del volume da**.

   Verrà visualizzata la finestra di dialogo **Selezione di un volume di origine di base**.



5. Nella finestra di dialogo **Selezione di un volume di origine di base**, fare clic sul menu a discesa e selezionare il volume di origine disponibile da assegnare al volume di destinazione specificato. Fare clic su **OK**.
   - Il volume di destinazione viene contrassegnato da un'icona con il segno di spunta, a indicare che il mapping del volume di destinazione è stato eseguito.
   - Nel volume di origine, l'icona con forma di X rossa viene sostituita da un'icona verde, a indicare che il volume di origine è stato assegnato a un volume di destinazione.
6. Verificare che tutti i volumi da ripristinare e che i volumi contenenti informazioni di sistema siano assegnati a un volume di destinazione, quindi fare clic su **Avanti**.

   Verrà visualizzata la schermata **Invia modifiche disco** contenente un riepilogo delle operazioni selezionate. Per ciascun nuovo volume creato, vengono visualizzate le informazioni corrispondenti.



7. Verificare che le informazioni di riepilogo siano corrette, quindi fare clic su **Invia**. Se le informazioni non sono corrette, fare clic su **Annulla**.

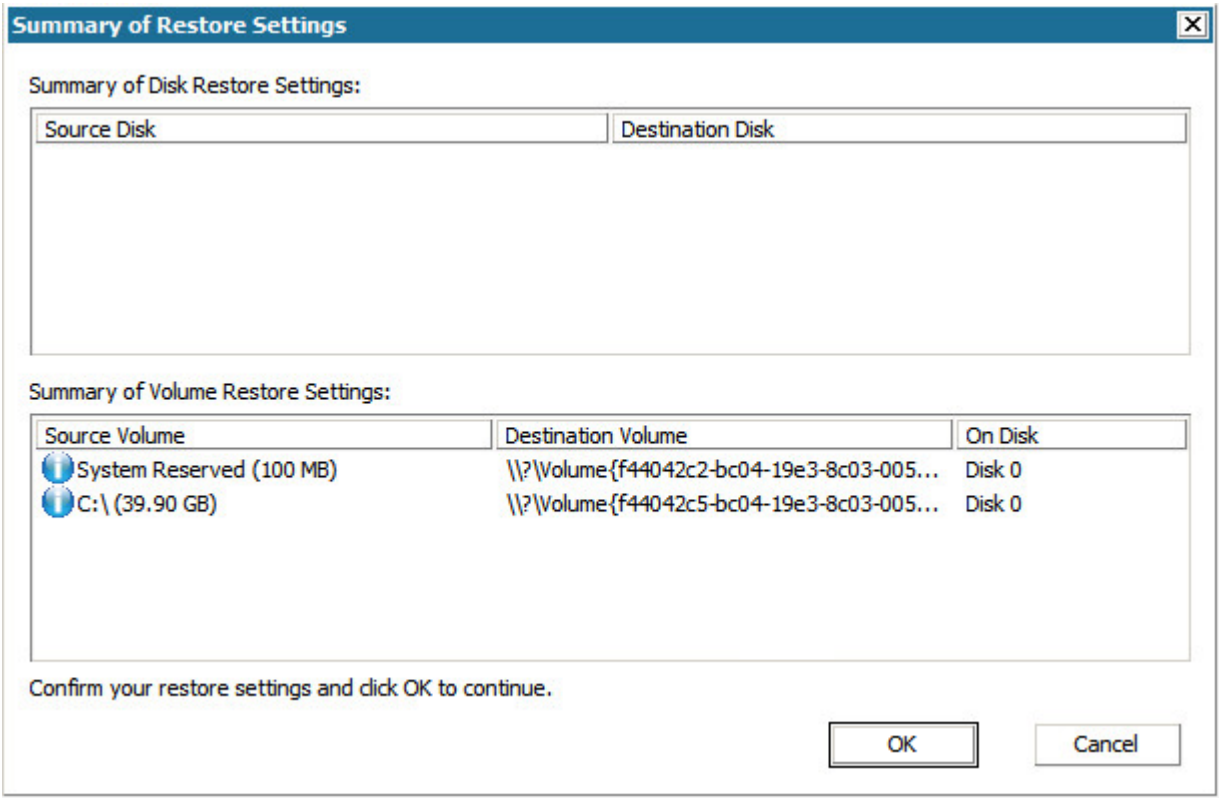
   Nota: tutte le operazioni eseguite sul disco rigido verranno implementate solo in seguito all'invio.

   I nuovi volumi vengono creati sul computer di destinazione e mappati sul computer di origine corrispondente.

8. Una volta completate le modifiche, fare clic su **OK**.

   Verrà visualizzata la schermata Riepilogo delle impostazioni di ripristino del disco contenente un riepilogo dei volumi da ripristinare.

   Nota: Nella parte superiore della pagina Riepilogo ripristino, le lettere corrispondenti alle unità elencate nella colonna Volume di destinazione vengono generate automaticamente dall'Ambiente di preinstallazione di Windows (WinPE). È possibile che tali lettere di unità non corrispondano alle lettere elencate nella colonna Volume di origine. Tuttavia, il ripristino dei dati verrà eseguito sul volume appropriato anche se le lettere di unità sono diverse.

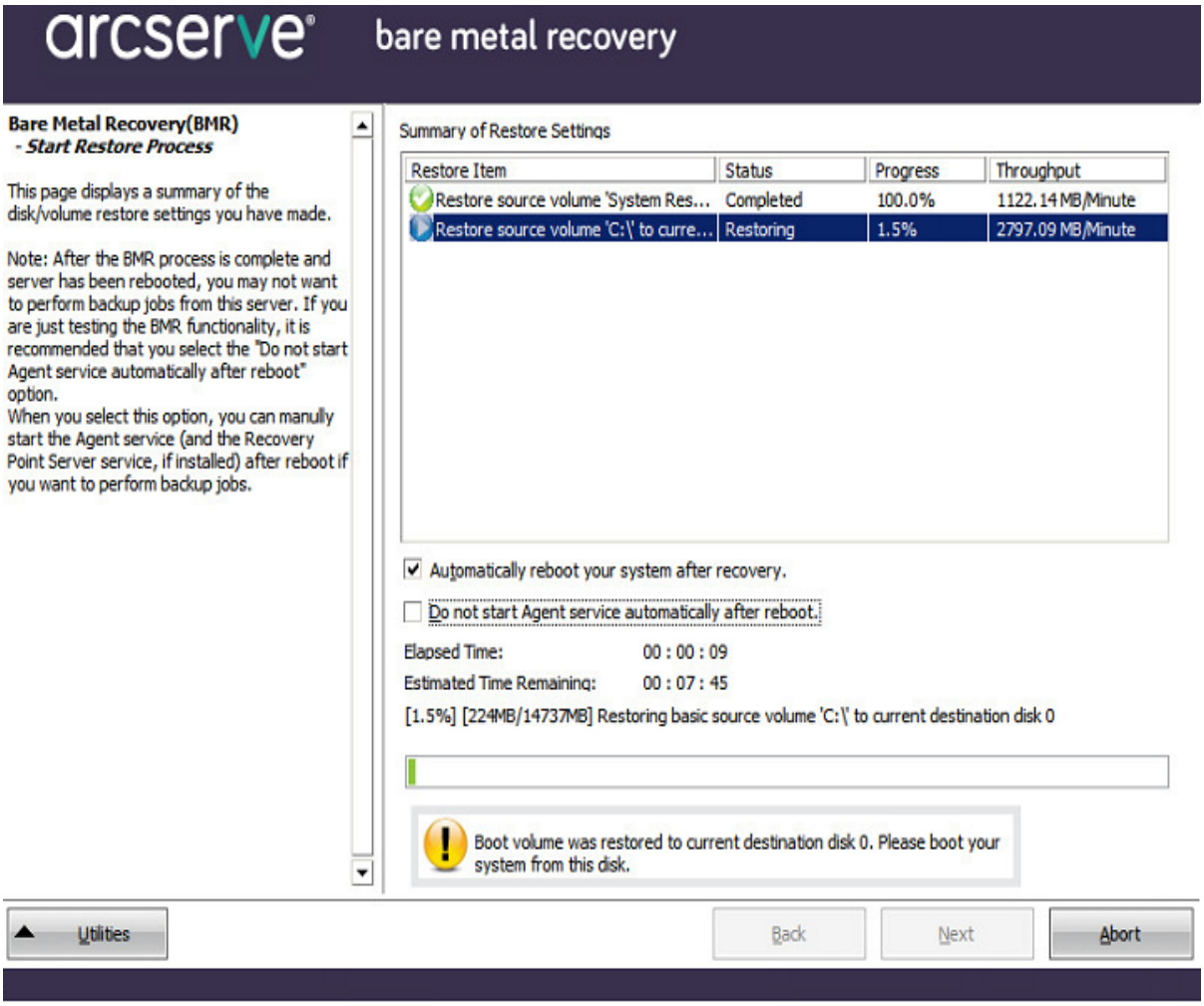


9. Verificare che le informazioni di riepilogo siano corrette, quindi fare clic su **OK**.

   Verrà avviato il processo di ripristino. La schermata della procedura guidata di ripristino bare metal visualizza lo stato di ripristino per ciascun volume.

- Il tempo necessario per l'esecuzione di questa operazione dipende dalle dimensioni del volume da ripristinare.
- Durante questo processo viene eseguito il ripristino blocco per blocco di tutti i dati di backup di tale punto di ripristino e viene creata una replica del computer di origine sul computer di destinazione.
- L'opzione di riavvio automatico del sistema in seguito al recupero è selezionata per impostazione predefinita. Se lo si desidera, è possibile deselezionare questa opzione ed eseguire il riavvio manuale in un secondo momento.

  Importante: se è in corso il recupero autorevole di Active Directory dopo un ripristino bare metal, è necessario deselezionare l'opzione di **riavvio automatico del sistema in seguito al ripristino**. Per ulteriori informazioni, consultare la sezione Ripristino autorevole di Active Directory dopo un ripristino bare metal.
- Se necessario, è possibile selezionare di non avviare automaticamente il servizio Agente dopo il riavvio.
- Se necessario, è possibile annullare o interrompere l'operazione in qualsiasi momento.



10. Dal menu **Utilità**, è possibile accedere al **registro attività** del ripristino bare metal e utilizzare l'opzione **Salva** per salvare il registro attività.

    Per impostazione predefinita, il salvataggio del registro attività viene effettuato nella posizione seguente:

    X:\windows\system32\dr\log.

    Nota: per evitare la generazione di un errore Windows, si consiglia di non utilizzare l'opzione **Salva con nome** della finestra di dialogo del **registro attività** del ripristino bare metal per salvare il registro attività sul desktop o per creare una nuova cartella sul desktop.

11. Se si sta eseguendo il ripristino su hardware diversi (la scheda SCSI/FC utilizzata per la connessione ai dischi rigidi potrebbe essere stata modificata) e non viene rilevato nessun driver compatibile nel sistema originale, viene visualizzata la pagina di inserimento del driver per consentire all'utente di specificare i driver necessari per le periferiche.

È possibile individuare e selezionare i driver da inserire nel sistema ripristinato. In tal modo è possibile eseguire il ripristino su un computer con hardware diversi.

12. Una volta completato il processo di ripristino bare metal, viene visualizzata una notifica di conferma.

Verifica della corretta esecuzione del ripristino bare metal

Per verificare che il ripristino bare metal sia avvenuto correttamente, eseguire le attività seguenti:

- Riavviare il sistema operativo.
- Verificare che tutti i sistemi e tutte le applicazioni funzionino correttamente.
- Verificare che tutte le impostazioni di rete siano state configurate correttamente.
- Verificare che il BIOS sia configurato per l'avvio dal disco utilizzato per il ripristino del volume di avvio.
- Quando il ripristino bare metal viene completato, occorre considerare le condizioni seguenti:
  - Il primo backup eseguito dopo il ripristino bare metal è un backup di verifica.
  - Dopo aver riavviato il computer, potrebbe essere necessario configurare manualmente le schede di rete, nel caso in cui sia stato eseguito il ripristino su hardware differenti.

    Nota: Durante il riavvio di un computer, potrebbe essere visualizzata la schermata Ripristino da errori di Windows indicante che l'arresto di Windows non è avvenuto correttamente. Se ciò si verifica, è possibile ignorare l'avviso e avviare Windows normalmente.
  - In caso di dischi dinamici, se il disco è in modalità Non in linea, è possibile modificare manualmente lo stato a In linea, accedendo all'interfaccia di gestione del disco mediante l'utilità di controllo Diskmgmt.msc.
  - In caso di dischi dinamici, se lo stato del volume è Ridondanza non riuscita, è possibile eseguire la sincronizzazione manuale dei volumi, accedendo all'interfaccia di gestione del disco mediante l'utilità di controllo Diskmgmt.msc.

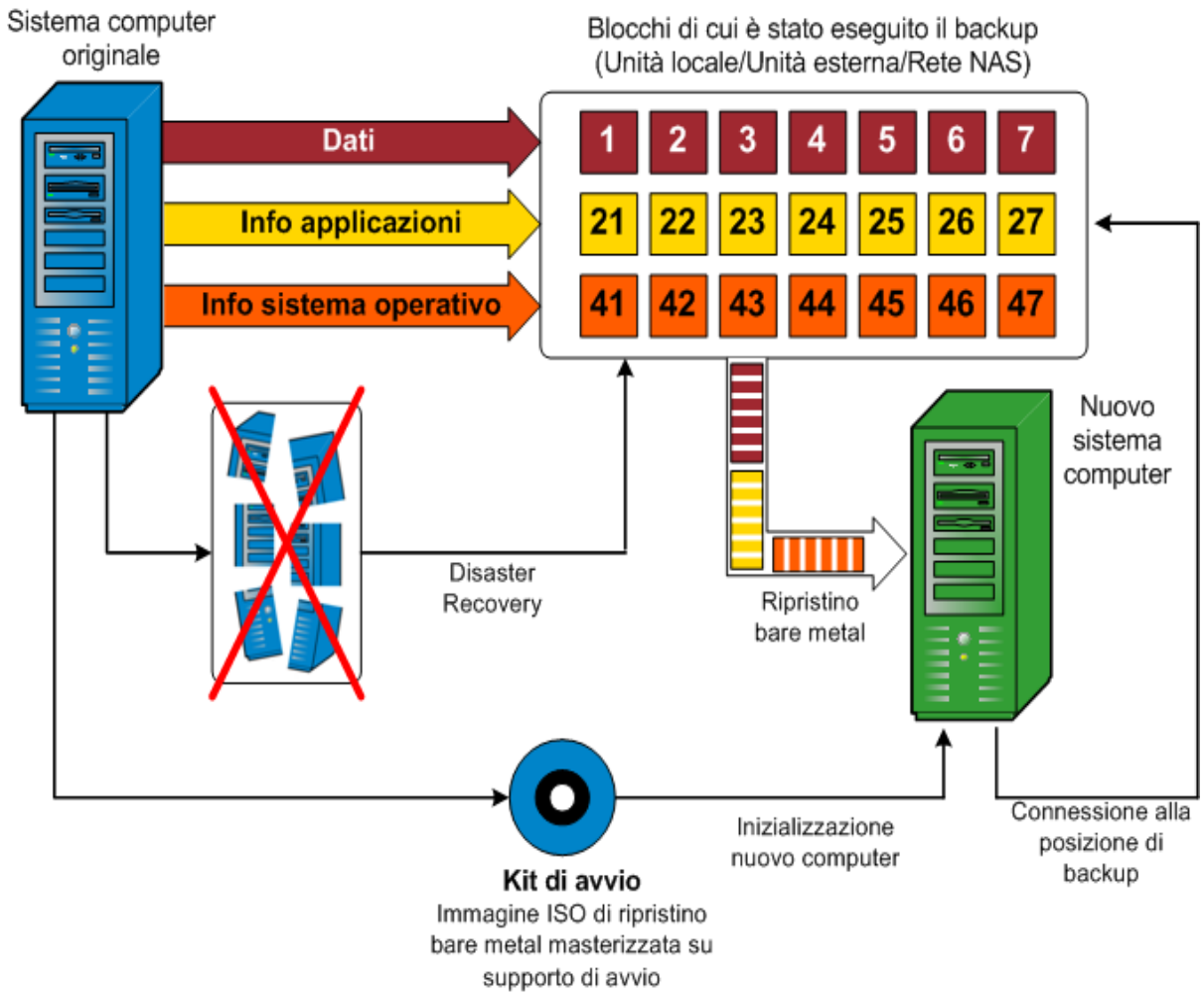
Informazioni di riferimento del ripristino bare metal

- Funzionamento del ripristino bare metal
- Sistemi operativi che supportano la conversione UEFI/BIOS
- Gestione del menu delle operazioni di ripristino bare metal

Funzionamento del ripristino bare metal

Il ripristino bare metal è il processo di ripristino di interi sistemi mediante la reinstallazione del sistema operativo, delle applicazioni software e mediante il ripristino di dati e impostazioni. Il ripristino bare metal di solito viene eseguito perché si verifica un errore nel disco rigido o perché il disco rigido è pieno e si desidera eseguire un aggiornamento (migrazione) a un'unità di dimensioni maggiori o una migrazione a un hardware più recente. È possibile eseguire un ripristino bare metal poiché durante il processo di backup a livello di blocco, l'agente Arcserve UDP (Windows) acquisisce non solo i dati, ma anche le informazioni relative al sistema operativo, alle applicazioni installate, alle impostazioni di configurazione, ai driver necessari e così via. Le informazioni necessarie per l'esecuzione di una ricostruzione completa di interi sistemi da bare metal vengono sottoposte a backup in una serie di blocchi ed archiviate nella posizione di backup.

Nota: il ripristino dei dischi dinamici viene eseguito solo a livello del disco. Se è stato eseguito il backup di dati in un volume o in un disco dinamico, non sarà possibile eseguire il ripristino di tale disco (compresi i volumi corrispondenti) durante il ripristino bare metal.



Quando si esegue un ripristino bare metal, il disco di avvio dell'agente Arcserve UDP (Windows) viene utilizzato per inizializzare il nuovo sistema e consentire l'avvio del processo di ripristino bare metal. Una volta avviato il ripristino bare metal, l'agente Arcserve UDP (Windows) richiederà di selezionare o specificare una posizione valida per il recupero dei blocchi sottoposti a backup, nonché del punto di ripristino da ripristinare. Il nuovo sistema potrebbe inoltre richiedere l'immissione di driver validi. Quando vengono fornite le informazioni di connessione e configurazione, l'agente Arcserve UDP (Windows) avvia l'estrazione dell'immagine di backup specificata dalla posizione di backup e ripristina tutti i blocchi sottoposti a backup sul nuovo sistema (i blocchi vuoti non verranno ripristinati). Una volta eseguito il ripristino completo dell'immagine bare metal sul nuovo sistema, lo stato del computer verrà ripristinato a quello dell'ultima esecuzione del backup e i backup dell'agente Arcserve UDP (Windows) potranno procedere in base alla pianificazione. (una volta completato il ripristino bare metal, il primo backup corrisponderà a Backup di verifica).

Sistemi operativi che supportano la conversione UEFI/BIOS

Se il sistema operativo del computer di origine non corrisponde al firmware del sistema, verrà richiesto se si desidera convertire il sistema UEFI in un sistema compatibile con BIOS o viceversa. La seguente tabella classifica ciascun sistema operativo e il tipo di conversione supportato:

Sistema operativo	CPU	UEFI a BIOS	BIOS a UEFI
Windows Vista (senza SP)	x86	No	No
Windows Vista (senza SP)	x64	No	No
Windows Vista SP1	x86	No	No
Windows Vista SP1	x64	Sì	Sì
Windows Server 2008	x86	No	No
Windows Server 2008	x64	Sì	Sì
Windows Server 2008 R2	x64	Sì	Sì
Windows 7	x86	No	No
Windows 7	x64	Sì	Sì
Windows 8	x86	No	No
Windows 8	x64	Sì	Sì
Windows Server 2012	x64	Sì	Sì
Windows 8.1	x86	No	No
Windows 8.1	x64	Sì	Sì
Windows 10	x86	No	No
Windows 10	x64	Sì	Sì
Windows Server 2012 R2	x64	Sì	Sì
Windows Server 2016	x64	Sì	Sì
Windows Server 2019	x64	Sì	Sì

Gestione del menu delle operazioni di ripristino bare metal

Il menu Operazioni di ripristino bare metal comprende i seguenti tre tipi di operazioni:

- Operazioni specifiche del disco
- Operazioni specifiche di volume/partizione
- Operazioni specifiche di ripristino bare metal

Operazioni specifiche del disco:

Per eseguire operazioni specifiche del disco, selezionare l'intestazione del disco e fare clic su **Operazioni**.

Pulitura disco

Questa operazione viene utilizzata per la pulitura di tutte le partizioni di un disco:

- Si tratta di un metodo alternativo per l'eliminazione di tutti i volumi di un disco. L'operazione di **pulitura disco** consente di non eliminare ogni volume singolarmente.
- Viene utilizzata per l'eliminazione di partizioni non-Windows. A causa di una limitazione di VDS, non è possibile eliminare la partizione non-Windows dall'interfaccia utente. Sarà tuttavia possibile utilizzare l'operazione per eseguire la pulitura completa.

  Nota: durante il ripristino bare metal, se il disco di destinazione dispone di partizioni non-Windows o di partizioni OEM, non sarà possibile selezionare la partizione ed eliminarla dall'interfaccia utente di ripristino bare metal. Solitamente, questo problema si verifica se è stato installato Linux/Unix sul disco di destinazione. Per risolvere il problema, eseguire una delle seguenti attività:
- Selezionare l'intestazione del disco nell'interfaccia utente di ripristino bare metal, fare clic su **Operazioni**, quindi utilizzare l'operazione **Pulitura disco** per eliminare tutte le partizioni presenti sul disco.
- Aprire un prompt dei comandi e digitare **Diskpart** per aprire la console del comando Diskpart. Digitare quindi "select disk x" (x corrisponderà al numero di disco) e "clean" per eliminare tutte le partizioni sul disco.

Converti in MBR

Questa operazione consente di convertire un disco in MBR (Master Boot Record, Record di avvio principale). L'operazione è disponibile solamente quando il disco selezionato è un disco GPT (tabella di partizione GUID) e non sono presenti volumi sul disco.

Converti in GPT

Questa operazione viene utilizzata per convertire un disco in GPT. L'operazione è disponibile solamente quando il disco selezionato è un disco MBR e non sono presenti volumi sul disco.

Converti in disco di base

Questa operazione viene utilizzata per convertire un disco in un disco di base. L'operazione è disponibile solamente quando il disco selezionato è un disco dinamico e non sono presenti volumi sul disco.

Converti in disco dinamico

Questa operazione viene utilizzata per convertire un disco in un disco dinamico. L'operazione è disponibile soltanto quando il disco selezionato è un disco di base.

Disco in linea

Questa operazione viene utilizzata per rendere un disco in linea. L'operazione è disponibile soltanto quando il disco selezionato è in stato Non in linea.

Proprietà disco

Questa operazione viene utilizzata per visualizzare proprietà del disco dettagliate. L'operazione è sempre disponibile. Quando viene selezionata, verrà visualizzata la finestra di dialogo **Proprietà disco**.

Operazioni specifiche di volume/partizione:

Per eseguire operazioni di volume/partizione, selezionare l'area di testo del disco, quindi fare clic su **Operazioni**. Questo menu consente di creare nuove partizioni corrispondenti alle partizioni di disco del volume di origine.

Crea partizione primaria

Questa operazione consente di creare una partizione su un disco di base. È disponibile solamente quando l'area selezionata è uno spazio su disco non allocato.

Crea partizione logica

Questa operazione consente di creare una partizione logica su un disco MBR di base. È disponibile solamente quando l'area selezionata è una partizione estesa.

Crea partizione estesa

Questa operazione viene utilizzata per creare una partizione estesa su un disco MBR di base. È disponibile solamente quando il disco è un disco MBR e l'area selezionata è uno spazio su disco non allocato.

Crea partizione di sistema riservato

Questa operazione consente di creare la partizione di sistema riservato su un sistema firmware BIOS e genera una relazione di mapping con la partizione di sistema EFI di origine. L'operazione è disponibile soltanto quando viene eseguito il ripristino di un sistema UEFI in un sistema BIOS.

Nota: se precedentemente è stata eseguita una conversione da UEFI a un sistema compatibile con BIOS, utilizzare l'opzione Crea partizione di sistema riservato per il ridimensionamento del disco di destinazione.

Crea partizione del sistema EFI

Questa operazione viene utilizzata per creare la partizione di sistema EFI su un disco GPT di base. È disponibile solamente quando il firmware del computer di destinazione è UEFI e il disco selezionato è un disco GPT di base.

Nota: se precedentemente è stata eseguita la conversione da BIOS a un sistema compatibile con UEFI, utilizzare l'opzione Crea partizione del sistema EFI per il ridimensionamento del disco di destinazione.

Nota: i sistemi che supportano UEFI richiedono che la partizione di avvio sia anche presente su un disco GPT (Tabella di partizione GUID). Se si utilizza un disco MBR (record di avvio principale), è necessario eseguire la conversione del disco in un disco GPT, quindi utilizzare l'operazione Crea partizione del sistema EFI per il ridimensionamento del disco.

Ridimensiona volume

Questa operazione consente di ridimensionare un volume. Si tratta di un metodo alternativo di Windows Estendi volume/Riduci volume. È disponibile solamente quando l'area selezionata è una partizione di disco valida.

Elimina volume

Questa operazione consente di eliminare un volume. È disponibile solamente quando l'area selezionata è un volume valido.

Elimina partizione estesa

Questa operazione viene utilizzata per eliminare la partizione estesa. È disponibile solamente quando l'area selezionata è una partizione estesa.

Proprietà volume

Questa operazione viene utilizzata per visualizzare le proprietà del volume dettagliate. Quando viene selezionata questa operazione, viene visualizzata la finestra di dialogo **Proprietà volume**.

Operazioni specifiche di ripristino bare metal:

Queste operazioni sono specifiche del ripristino bare metal. Per eseguire operazioni di ripristino bare metal, selezionare l'intestazione del disco o l'area di testo del disco, quindi fare clic su **Operazioni**.

Esegui mapping del disco da

Questa operazione viene utilizzata per stabilire una relazione di mapping tra i dischi dinamici di origine e di destinazione. L'opzione è disponibile soltanto quando il disco selezionato è un disco dinamico.

Nota: quando viene eseguito il mapping su un altro disco, la capacità di ciascun volume di destinazione mappato deve essere uguale o superiore alla capacità del volume di origine corrispondente.

Esegui mapping del volume da

Questa operazione viene utilizzata per stabilire una relazione di mapping tra i volumi di base di origine e di destinazione. L'opzione è disponibile soltanto quando il volume selezionato è un volume di base.

Nota: quando viene eseguito il mapping su un altro disco, la capacità di ciascun volume di destinazione mappato deve essere uguale o superiore alla capacità del volume di origine corrispondente.

Conferma

Questa operazione è sempre disponibile. Tutte le operazioni vengono memorizzate nella cache e non modificano i dischi di destinazione fino alla selezione dell'operazione **Conferma**.

Reimposta

Questa operazione è sempre disponibile. L'operazione **Reimposta** viene utilizzata per abbandonare le operazioni e ripristinare il layout del disco sullo stato predefinito. Viene così eseguita la pulitura di tutte le operazioni memorizzate nella cache. Per reimpostazione si intende ricaricare le informazioni di layout del disco di origine e di destinazione dal file di configurazione e dal sistema operativo corrente, annullando le modifiche apportate dall'utente alle informazioni di layout del disco.

Risoluzione dei problemi relativi al ripristino bare metal

Quando viene rilevato un problema, l'agente Arcserve UDP (Windows) genera un messaggio che consente di identificare e risolvere il problema. Questi messaggi sono contenuti nel **Registro attività** dell'agente Arcserve UDP (Windows). Per accedere a questo registro, utilizzare l'opzione **Visualizza registri** dell'interfaccia utente della pagina principale. Inoltre, in caso di un'azione non corretta, l'agente Arcserve UDP (Windows) visualizza solitamente un messaggio popup che consente all'utente di identificare e risolvere rapidamente il problema.

- Velocità effettiva bassa durante il ripristino bare metal
- I volumi dinamici non sono riconosciuti dal sistema operativo dopo il ripristino bare metal.
- Impossibile eseguire il riavvio del computer virtuale Hyper-V in seguito al ripristino bare metal
- Impossibile eseguire il riavvio del computer virtuale VMware in seguito al ripristino bare metal
- Impossibile avviare il server dopo avere eseguito un ripristino bare metal.
- Errore di invio del processo di ripristino bare metal al Recovery Point Server

Velocità effettiva bassa durante il ripristino bare metal

Questo problema potrebbe essere causato dai controller SATA con AHCI abilitato.

Durante il ripristino bare metal, l'agente Arcserve UDP (Windows) installa i driver per le periferiche sconosciute critiche. Se la periferica dispone già dei driver installati, l'agente Arcserve UDP (Windows) non aggiornerà nuovamente il driver. Windows 7PE contiene già i driver necessari per alcune periferiche, tuttavia, tali driver potrebbero non essere i più indicati e rallentare il processo di ripristino bare metal.

Per risolvere il problema, completare una delle seguenti attività:

- Verificare se la cartella di pool dei driver contiene i driver del disco più recenti. In tal caso, se si sta eseguendo il ripristino sul computer originale, installare il nuovo driver contenuto nella cartella di pool dei driver. In caso di ripristino in un computer alternativo, scaricare i driver del disco più recenti da Internet, e caricarli prima di avviare il recupero dei dati. Per caricare il driver, utilizzare l'utilità drvload.exe, fornita con Windows PE.
- Modificare la modalità operativa della periferica da AHCI (Advanced Host Controller Interface) alla modalità di compatibilità. La modalità di compatibilità consente di ottenere una velocità effettiva superiore.

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Volumi dinamici non riconosciuti dal sistema operativo dopo il ripristino bare metal

Per mantenere lo stato coerente dei dischi dinamici, il sistema operativo Windows esegue la sincronizzazione automatica dei metadati della Gestione dischi logici (LDM) su ciascun disco dinamico. Quando si esegue il ripristino bare metal di un disco dinamico e il disco viene messo in linea, i metadati LDM del disco vengono aggiornati automaticamente dal sistema operativo. In seguito a questa operazione, è possibile che il sistema operativo non sia in grado di riconoscere il disco dinamico che risulta mancante dopo il riavvio del computer.

Per risolvere il problema, quando si esegue il ripristino bare metal con più dischi dinamici, non eseguire operazioni di disco prima della procedura BMR (quali pulizia, eliminazione del volume, e così via).

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Impossibile eseguire il riavvio del computer virtuale Hyper-V in seguito al ripristino bare metal

Se è stato eseguito il ripristino bare metal su un computer Hyper-V costituito da più dischi collegati a un controller IDE (Integrated Drive Electronics) e non è possibile eseguire il riavvio del server, eseguire la seguente procedura per la risoluzione del problema:

1. Verificare che il disco contenente il volume di sistema corrisponda al disco master.

   La BIOS Hyper-V esegue la ricerca del volume di sistema sul disco principale (disco 1) connesso al canale principale. Se il volume di sistema non viene individuato sul disco principale, non sarà possibile eseguire il riavvio del computer virtuale.

   Nota: Verificare che il disco contenente il volume di sistema sia connesso a un controller di IDE. Impossibile riavviare Hyper-V da un disco SCSI.

2. Se necessario, modificare le impostazioni Hyper-V, per connettere il disco contenente il volume di sistema al canale principale IDE e riavviare nuovamente il computer virtuale.

   Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Impossibile eseguire il riavvio del computer virtuale VMware in seguito al ripristino bare metal

Se è stato eseguito il ripristino bare metal su un computer VMware costituito da più dischi connessi a un controller IDE (Integrated Drive Electronics) o a una scheda SCSI e non è possibile eseguire il riavvio del server, attenersi alla seguente procedura per la risoluzione del problema:

1. Verificare che il disco contenente il volume di sistema corrisponda al disco master.

   La BIOS VMware esegue la ricerca del volume di sistema sul disco principale (disco 0) connesso al canale principale. Se il volume di sistema non viene individuato sul disco principale, non sarà possibile eseguire il riavvio del computer virtuale.

2. Se necessario, modificare le impostazioni del computer VMware, per connettere il disco contenente il volume di sistema al canale master di IDE e riavviare nuovamente il computer virtuale.

3. Se si tratta di un disco SCSI, verificare che il disco contenente il volume di avvio sia il primo disco ad eseguire la connessione alla scheda SCSI. In caso contrario, assegnare il disco di avvio dal BIOS VMware.

4. Verificare che il disco contenente il volume di avvio sia incluso negli 8 dischi precedenti, in quanto il BIOS VMware è in grado di individuare un numero massimo di 8 dischi durante l'avvio. Se il disco contenente i volumi di sistema connessi alla scheda SCSI è preceduto da più di 7 dischi, non sarà possibile eseguire l'avvio del computer virtuale.

   Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Impossibile avviare il server dopo avere eseguito un ripristino bare metal.

Sintomo

Se il computer di origine è un server Active Directory su cui è in esecuzione un ripristino bare metal verso un computer fisico con hardware differente o un computer virtuale su un server Hyper-v, il server non si avvia e viene visualizzata una schermata blu con il messaggio seguente:

STOP: c00002e2 Directory Services could not start because of the following error: a device attached to the system is not functioning. Stato di errore: 0xc0000001.

Soluzione

Riavviare il sistema nell'ambiente PE di ripristino bare metal, rinominare tutti i file *.log nella cartella C:\Windows\NTDS e riavviare il sistema. Ad esempio, rinominare il file edb.log in edb.log.old e riavviare il sistema.

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Errore di invio del processo di ripristino bare metal al Recovery Point Server

È supportato soltanto un processo di ripristino bare metal per l'esecuzione di un ripristino dallo stesso server RPS per lo stesso nodo (backup agente o backup basato su host). L'operazione è controllata dal monitoraggio del processo del server RPS.

Se il computer su cui è in esecuzione il processo di ripristino bare metal viene interrotto o riavviato in maniera imprevista, il monitoraggio del processo sul lato server RPS attenderà 10 minuti per poi scadere. In questi 10 minuti non sarà possibile avviare un altro ripristino bare metal per lo stesso nodo dallo stesso server RPS.

Se il ripristino bare metal viene interrotto dall'interfaccia utente di ripristino bare metal, il problema non si verifica.

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Avvio del computer di destinazione di ripristino bare metal nella schermata delle opzioni del ripristino di sistema in seguito all'esecuzione di un ripristino bare metal

Sintomo

Se si esegue un ripristino bare metal su un computer virtuale su un server ESX, a volte il computer virtuale di destinazione di ripristino bare metal viene avviato nella schermata delle opzioni del ripristino di sistema.

Soluzione

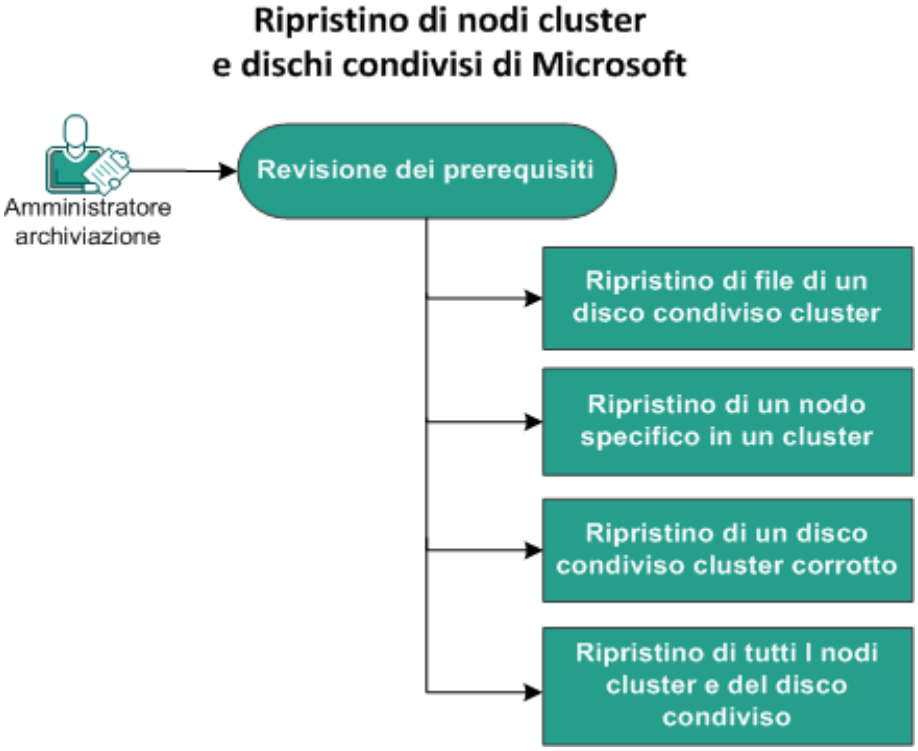
Per risolvere questo problema, disabilitare i writer VSS specifici con gli strumenti VMware sul computer virtuale istantaneo, quindi eseguire nuovamente un ripristino bare metal.

Ripristino di dischi condivisi e nodi del cluster Microsoft

Se si dispone di un ambiente cluster e i nodi del cluster e il disco condiviso non funzionano correttamente, è possibile recuperare facilmente nodi e dischi. È possibile ripristinare gli elementi seguenti:

- Singoli file e cartelle in un disco condiviso
- Nodi specifici in un cluster
- Disco condiviso intero
- Configurazione intera del cluster (tutti i dischi condivisi e i nodi del cluster)

Il diagramma seguente illustra la procedura per ripristinare i dischi condivisi e i nodi del cluster:



Completare questi passaggi per ripristinare i dischi condivisi e i nodi del cluster Microsoft:

- Verifica dei prerequisiti
- Ripristino di file di un disco condiviso del cluster
- Ripristino di un nodo specifico in un cluster
- Ripristino di un disco condiviso corrotto del cluster
- Ripristino di tutti i dischi condivisi e nodi del cluster

Verifica dei prerequisiti

Verificare di aver completato i seguenti passaggi preliminari:

- È disponibile un punto di ripristino valido.
- È disponibile un'immagine ISO valida per un ripristino bare metal.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Ripristino di file di un disco condiviso del cluster

Il disco condiviso è compreso in un nodo del cluster. Quando si recuperano i file dal disco condiviso (non dal disco quorum del cluster), è necessario individuare il nodo padre del disco condiviso. Una volta identificato, è possibile recuperare i file nel nodo padre dal disco condiviso.

Nota: Dopo un failover, è necessario accedere al punto di ripristino di un agente diverso per trovare il punto di ripristino desiderato.

Effettuare le operazioni seguenti:

1. Accedere all'agente proprietario del disco condiviso.
2. Aprire la procedura guidata di ripristino e selezionare Trova file/cartelle da ripristinare.

   Nota: Per ulteriori informazioni sul ripristino di file e cartelle, consultare la sezione Ripristino di file e cartelle.
3. Dalla procedura guidata di ripristino, selezionare tutti i file che si desiderano ripristinare nella posizione originale.
4. Completare le configurazioni della procedura guidata di ripristino e inoltrare il processo.

   I file vengono recuperati.
5. Accedere al nodo padre del disco condiviso e verificare che i file siano stati recuperati.

   Il recupero dei file del disco condiviso è completato.

Ripristino di un nodo specifico in un cluster

Se un nodo specifico di un cluster non funziona, è possibile eseguire un ripristino bare metal soltanto per tale nodo. Generalmente, in questo scenario il disco condiviso funziona correttamente e non necessita di un ripristino.

Effettuare le operazioni seguenti:

1. Preparare l'immagine di ripristino bare metal (CD/DVD o periferica USB).
2. Rimuovere tutte le connessioni tra il nodo che si desidera recuperare e i dischi condivisi.

   Esempio: Scollegare la connessione con canale a fibre.
3. Eseguire un ripristino bare metal per il nodo del cluster.

   Nota: Per ulteriori informazioni sull'esecuzione di un ripristino bare metal, consultare la sezione Esecuzione di un ripristino bare metal mediante un backup.

   Il nodo specifico in un cluster è stato recuperato.
4. Selezionare lo stato del nodo recuperato nella console di gestione cluster e verificare che funzioni come componente del cluster.

   Il nodo specifico in un cluster è stato recuperato.

Ripristino di un disco condiviso corrotto del cluster

Il disco condiviso è compreso in un nodo del cluster. Se il disco condiviso è danneggiato o rotto, è possibile ripristinare specifici file o cartelle del disco condiviso, senza recuperare i nodi del cluster. Generalmente, in questo scenario il disco quorum e tutti i nodi del cluster funzionano correttamente.

Effettuare le operazioni seguenti:

1. Sostituire il disco danneggiato manualmente e riconfigurare il disco condiviso del cluster.
2. Identificare l'agente proprietario del disco condiviso e accedervi.
3. Aprire la procedura guidata di ripristino e selezionare Trova file/cartelle da ripristinare.

   Nota: Per ulteriori informazioni sul ripristino di file e cartelle, consultare la sezione Ripristino di file e cartelle.
4. Dalla procedura guidata di ripristino, selezionare tutti i file che si desiderano ripristinare nella posizione originale.
5. Completare le configurazioni della procedura guidata di ripristino e inoltrare il processo.

   Il disco condiviso è stato recuperato.
6. Selezionare lo stato del disco condiviso nella console di gestione cluster e verificare che funzioni come componente del cluster.

   Il disco condiviso è stato recuperato.

Ripristino di tutti i dischi condivisi e nodi del cluster

Se l'intera configurazione del cluster risulta danneggiata o non funzionante, è possibile recuperare il cluster intero. Il recupero del cluster intero comprende due fasi. Primo, recuperare i singoli nodi del cluster mediante ripristino bare metal. Quindi, recuperare i file e le cartelle del disco condiviso.

Nota: Per i dischi quorum, ricompilare il disco mediante la console di gestione cluster invece di recuperarlo con la procedura guidata di ripristino nell'agente Arcserve UDP (Windows).

Effettuare le operazioni seguenti:

1. Preparare l'immagine di ripristino bare metal (CD/DVD o periferica USB).
2. Rimuovere tutte le connessioni tra il nodo che si desidera recuperare e i dischi condivisi.

   Esempio: Scollegare la connessione con canale a fibre.
3. Eseguire un ripristino bare metal per il nodo del cluster.

   Nota: Per ulteriori informazioni sull'esecuzione di un ripristino bare metal, consultare la sezione Esecuzione di un ripristino bare metal mediante un backup.

   Il nodo specifico in un cluster è stato recuperato.
4. Selezionare lo stato del nodo recuperato nella console di gestione cluster e verificare che funzioni come componente del cluster.

   Il nodo specifico in un cluster è stato recuperato.
5. Ripetere i passaggi per recuperare tutti i nodi del cluster.

   Tutti i nodi del cluster sono stati recuperati. Passare al recupero del disco condiviso.
6. Sostituire il disco danneggiato manualmente e riconfigurare il disco condiviso del cluster.
7. Identificare l'agente proprietario del disco condiviso e accedervi.
8. Aprire la procedura guidata di ripristino e selezionare Trova file/cartelle da ripristinare.

   Nota: Per ulteriori informazioni sul ripristino di file e cartelle, consultare la sezione Ripristino di file e cartelle.
9. Dalla procedura guidata di ripristino, selezionare tutti i file che si desiderano ripristinare nella posizione originale.

10. Completare le configurazioni della procedura guidata di ripristino e inoltrare il processo.

    Il disco condiviso è stato recuperato.

11. Verificare i file del disco condiviso e controllare che siano stati recuperati.

    Il recupero del cluster intero è completato.

Ripristino di Active Directory

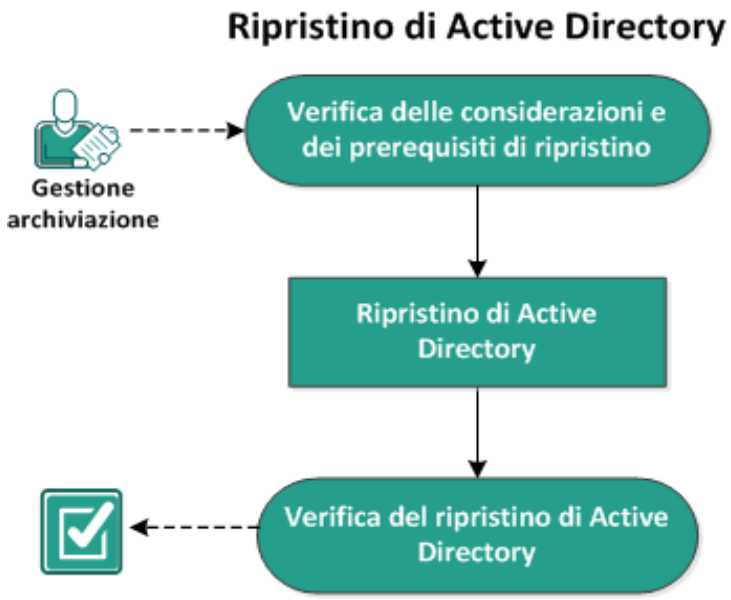
È necessario ripristinare una sessione di Active Directory sottoposta a backup se si presenta uno degli scenari riportati di seguito:

- Si desidera recuperare un attributo dell'oggetto di Active Directory da una qualsiasi delle sessioni disponibili di Active Directory sottoposta a backup (non solo l'ultima sessione sottoposta a backup).
- Si desidera recuperare un oggetto di Active Directory da una qualsiasi delle sessioni disponibili di Active Directory sottoposta a backup (non solo l'ultima sessione sottoposta a backup).
- Si desidera recuperare più attributi oppure oggetti di Active Directory da una qualsiasi delle sessioni disponibili di Active Directory sottoposta a backup (non solo l'ultima sessione sottoposta a backup).

Importante! Per eseguire un ripristino granulare di una Active Directory è necessario un backup basato su agente.

Elenco degli oggetti Active Directory ripristinati dal livello di oggetto		
Unità organizzativa	Sito	Classe persa e trovata
Utente	Contenitore sito	Classe di dominio integrata
Gruppo	Collegamento a un sito	Classe Zona DNS
Computer	Bridge di un collegamento a un sito	Classe di dominio
Contatto	Impostazioni di un sito	Classe di dominio DNS
Connessione	Contenitore subnet	Classe DMD
Cartella condivisa	Dominio attendibile	Classe di unità organizzativa
Stampante	Classe di configurazione	Classe Containerecifiers

Questo scenario descrive il ripristino di Active Directory.



Eseguire le attività seguenti per ripristinare l'Active Directory:

1. Verifica delle considerazioni e dei prerequisiti di ripristino
2. Ripristino di Active Directory
3. Verifica del ripristino di Active Directory

Verifica delle considerazioni e dei prerequisiti di ripristino

Verificare i seguenti prerequisiti prima di procedere al ripristino:

- È già stato eseguito il backup dei volumi che includono la cartella del database di Active Directory e la cartella dei file di registro.
- Si dispone dell'agente Arcserve UDP (Windows) installato sul controller di dominio.
- È stato eseguito un backup basato sull'agente.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Verificare le seguenti considerazioni sul ripristino:

- Per un punto di ripristino che non dispone di un catalogo di file system creato, per far sì che sia possibile accedere e selezionare file/cartelle da ripristinare, prima di eseguire il backup l'account o gruppo dovrebbe avere accesso a tutti i file e cartelle su tutti i volumi con accesso di lettura e elenco.
- È possibile eseguire un ripristino dell'Active Directory solamente sull'agente Arcserve UDP (Windows).

Ripristino di Active Directory

Dopo aver installato l'Active Directory su volumi differenti e aver eseguito un backup per entrambi i volumi, potrebbe essere necessario ripristinare i volumi con l'Active Directory. Questo scenario descrive il ripristino dei volumi di Active Directory sottoposti a backup.

Nota: Verificare il completamento dei prerequisiti e l'esecuzione del backup dei volumi dell'Active Directory.

Effettuare le operazioni seguenti:

1. Accedere alla finestra di dialogo per la selezione del metodo di ripristino in uno dei modi seguenti:

   Da Arcserve UDP:

   a. Accedere ad Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

      Nota: Viene effettuato automaticamente l'accesso al nodo agente e la finestra di dialogo per la selezione del metodo di ripristino viene visualizzata dal nodo agente.

   Dall'agente Arcserve UDP (Windows):

   a. Accedere all'agente Arcserve UDP (Windows).

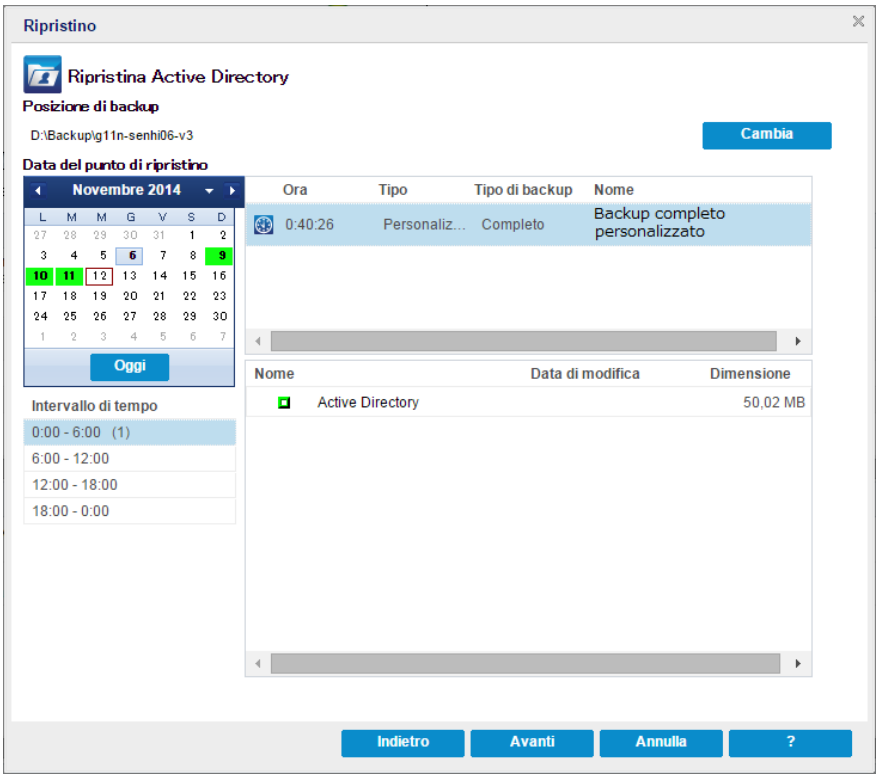
   b. Dalla pagina principale selezionare **Ripristino**.

   Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

2. Dalla schermata Ripristino, fare clic su Ripristina Active Directory.

   Viene visualizzata la finestra di dialogo Ripristina Active Directory.

3. Dalla schermata Ripristina Active Directory, eseguire i passaggi seguenti:



a. Dal calendario, selezionare la data di backup per l'Active Directory che si desidera ripristinare.

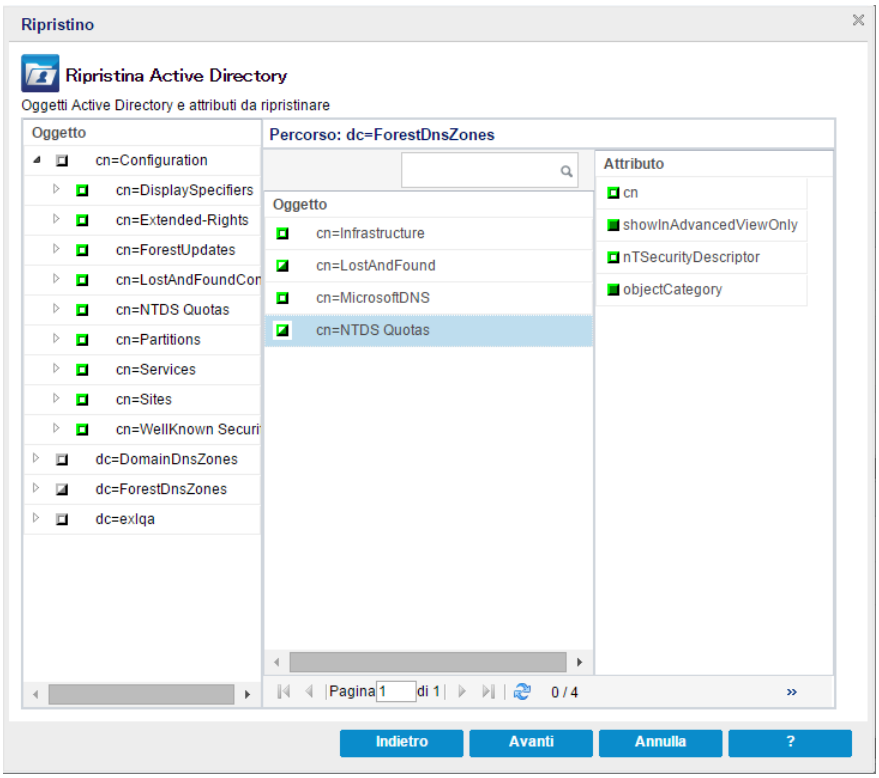
b. Da Intervallo di tempo, selezionare l'ora del backup.

c. Nella schermata Ripristina Active Directory, selezionare un punto di ripristino identificato con Ora, Tipo, Tipo di backup e Nome.

d. Dalla sezione Nome, selezionare una sessione di backup di Active Directory da ripristinare.

4. Fare clic su Avanti.

5. Selezionare le opzioni seguenti per definire meglio gli oggetti, il percorso e gli attributi da ripristinare:



a. Dalla colonna Oggetto, selezionare il nome di un oggetto. Vengono visualizzati i percorsi collegati all'oggetto selezionato.

b. Dalla colonna Percorso, selezionare un percorso. Vengono visualizzati gli attributi collegati al percorso selezionato.

   Nota: È possibile utilizzare l'icona di ricerca per individuare il percorso.

c. Dalla colonna Attributo, selezionare uno o più attributi.

6. Fare clic su Avanti.

   Verrà visualizzata la finestra Opzioni di ripristino.

7. Da Opzioni di ripristino, selezionare gli oggetti seguenti in base alle proprie esigenze:

   a. Se l'oggetto selezionato è stato rinominato dopo il backup, fare clic sull'opzione Restore with original name of Renamed Objects (Ripristina con nome originale degli oggetti rinominati) per ripristinare l'oggetto rinominato.

      Nota: Se questa opzione non viene selezionata, l'oggetto non verrà ripristinato.

   b. Se l'oggetto selezionato è stato spostato in un altro contenitore dopo il backup, fare clic sull'opzione Restore to original location of Moved Objects (Ripri-

stina su posizione originale degli oggetti spostati) per ripristinare l'oggetto spostato.

Nota: Se questa opzione non viene selezionata, l'oggetto non verrà ripristinato.

c. Se l'oggetto selezionato è stato eliminato definitivamente dopo il backup, fare clic sull'opzione Restore with the new object ID of Deleted Objects (Ripristina con il nuovo ID oggetto degli oggetti eliminati) per ripristinare l'oggetto eliminato definitivamente.

Nota: L'utilizzo di questa opzione consente di mantenere l'oggetto ripristinato con il nuovo ID oggetto.

8. Fare clic su Avanti.

   Verrà visualizzata la schermata Riepilogo ripristino.

9. Rivedere i dettagli ed eseguire una delle azioni seguenti:

   - Se si desidera modificare i dettagli, fare clic su Precedente.
   - Per eseguire il ripristino, fare clic su Fine.

   Viene visualizzato un messaggio di stato per informare quando il processo di ripristino è completato. Se il ripristino non è stato effettuato correttamente, visualizzare i registri e riprovare.

Verifica del ripristino di Active Directory

Dopo il completamento del processo di ripristino, è possibile utilizzare l'utilità Utenti e computer di Active Directory per verificare che l'Active Directory (oggetto e/o attributo) sia stata ripristinata nella destinazione specificata.

Nota: L'utilità Active Directory viene installata automaticamente con l'Active Directory.

Ripristino dei dati di Active Directory mediante l'utilità di ripristino a livello di oggetto di Active Directory per Arcserve UDP

Dopo aver installato Active Directory in volumi diversi ed eseguito un backup per entrambi i volumi utilizzando un'attività di backup senza agente basato sull'host, è possibile ripristinare gli oggetti e gli attributi da Active Directory in modo granulare. In questo scenario viene descritto come ripristinare gli oggetti e gli attributi di Active Directory di cui è stato eseguito il backup dai volumi contenitori.

Prima di eseguire un ripristino, assicurarsi che siano disponibili i prerequisiti seguenti:

- L'utilità di ripristino a livello di oggetto di Active Directory è disponibile nel seguente percorso:

  <Arcserve UDP installation path>\Engine\BIN\

  Nota: lo strumento è installato con l'agente Arcserve UDP.
- Il processo di ripristino è impostato per l'esecuzione dal computer proxy di backup basato sull'host.

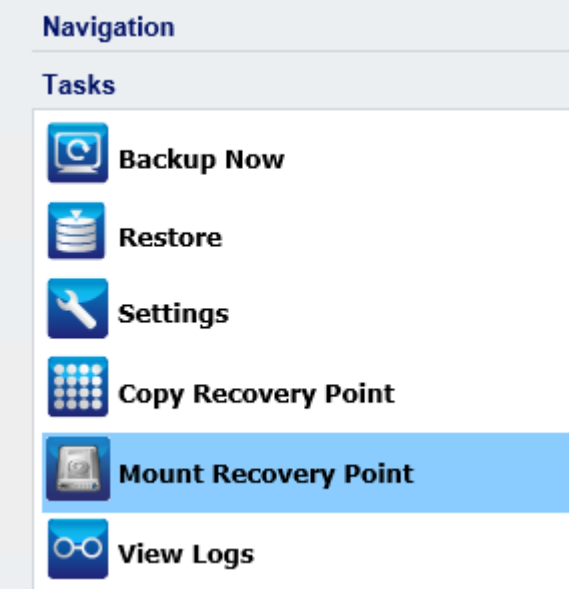
  Nota: per eseguire il processo di ripristino da un altro computer, cercare il punto di ripristino dalla destinazione di backup.
- Il percorso del database di Active Directory (NTDS.dit) viene identificato per eseguire il processo di ripristino.

  Nota: per impostazione predefinita, il percorso a NTDS.dit è C:\Windows\NTDS\NTDS.dit.

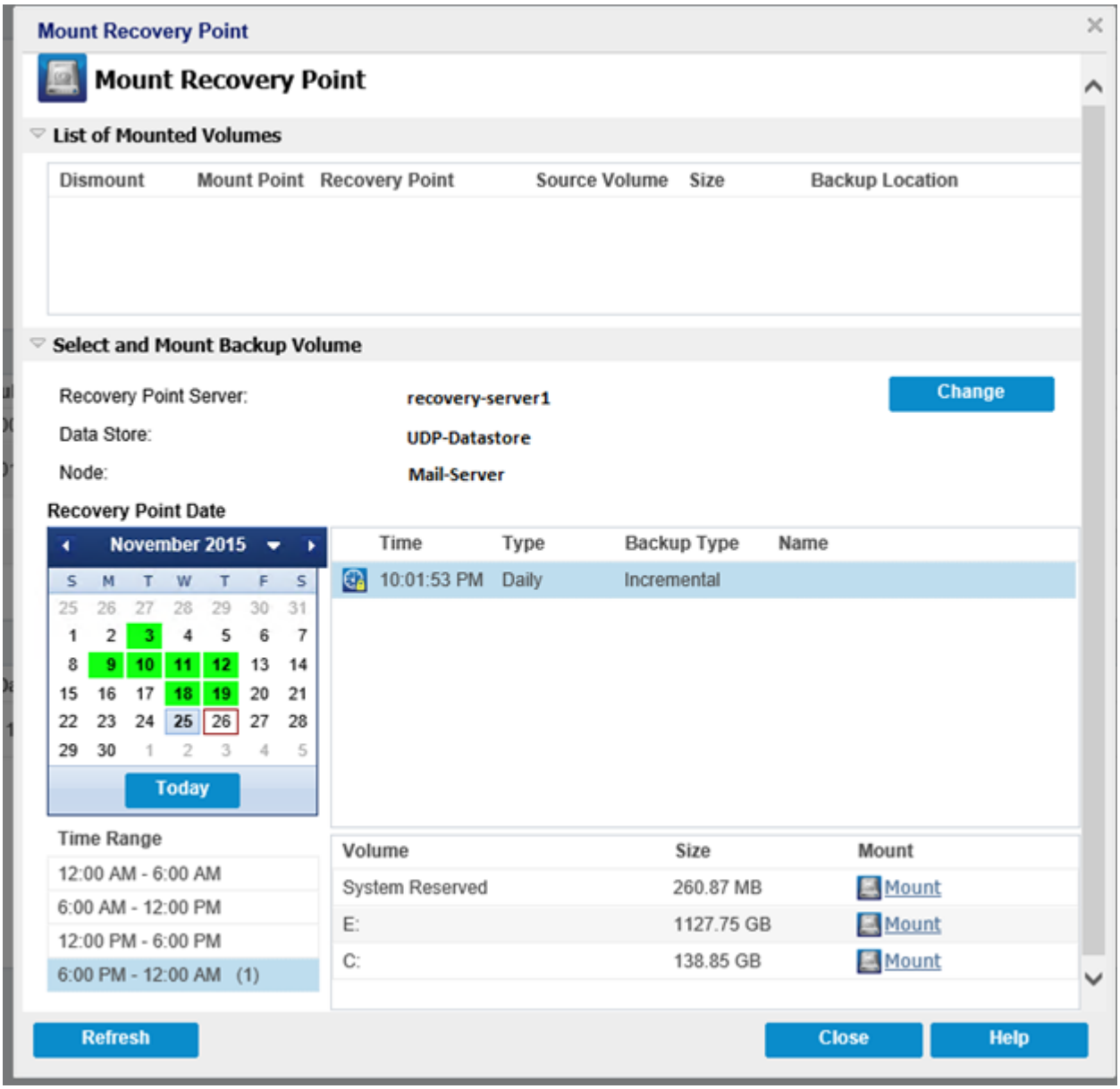
Effettuare le operazioni seguenti:

1. Dalla console dell'agente Arcserve UDP sul computer proxy di backup basato sull'host, selezionare l'attività Monta punto di ripristino. Verrà visualizzata la

finestra di dialogo Monta punto di ripristino.

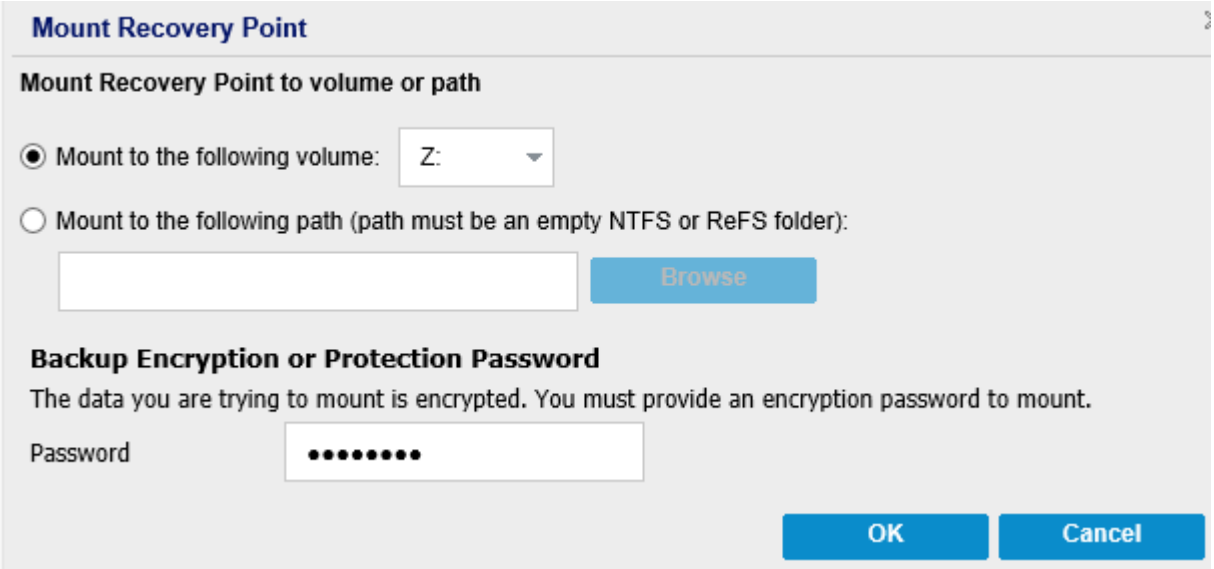


2. Selezionare la data del punto di ripristino.
3. Per il volume contenente il database di Active Directory, fare clic su **Monta**.



Nota: se il server che esegue il processo di ripristino non è un proxy di HBBU, fare clic su **Modifica** per selezionare il Recovery Point Server, l'archivio dati e il server Exchange appropriati.

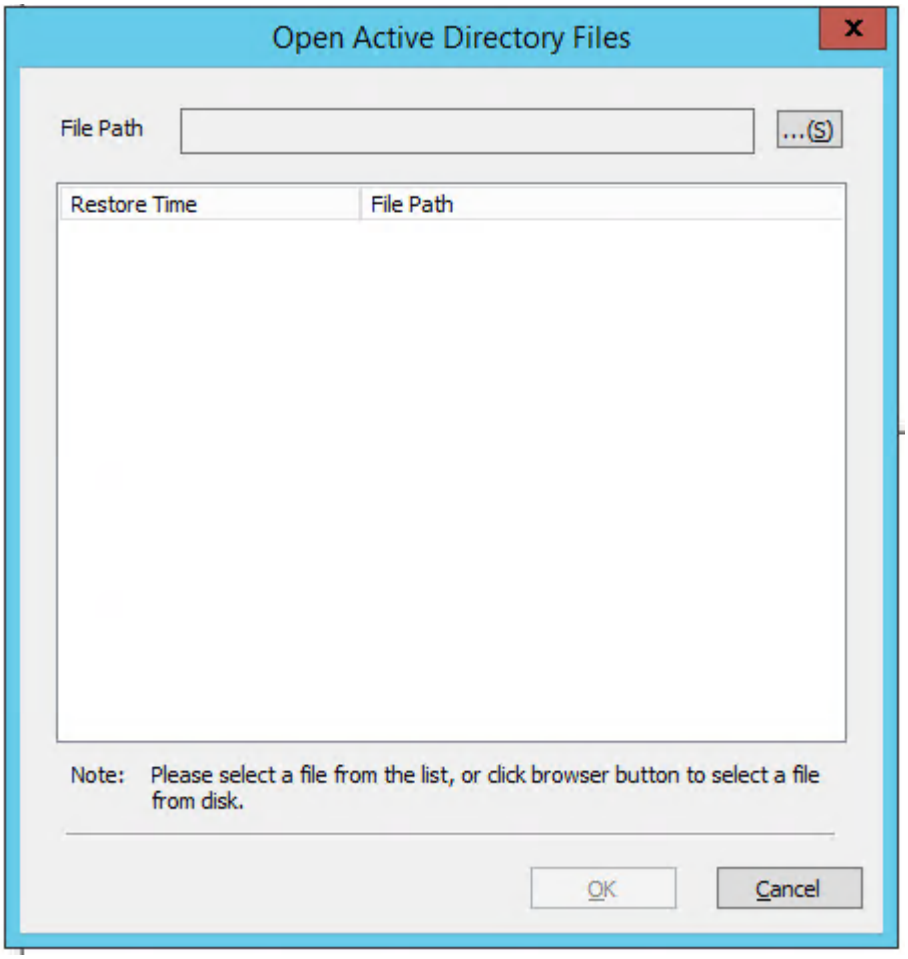
4. Selezionare la lettera di unità per il montaggio del volume e fare clic su **OK**.



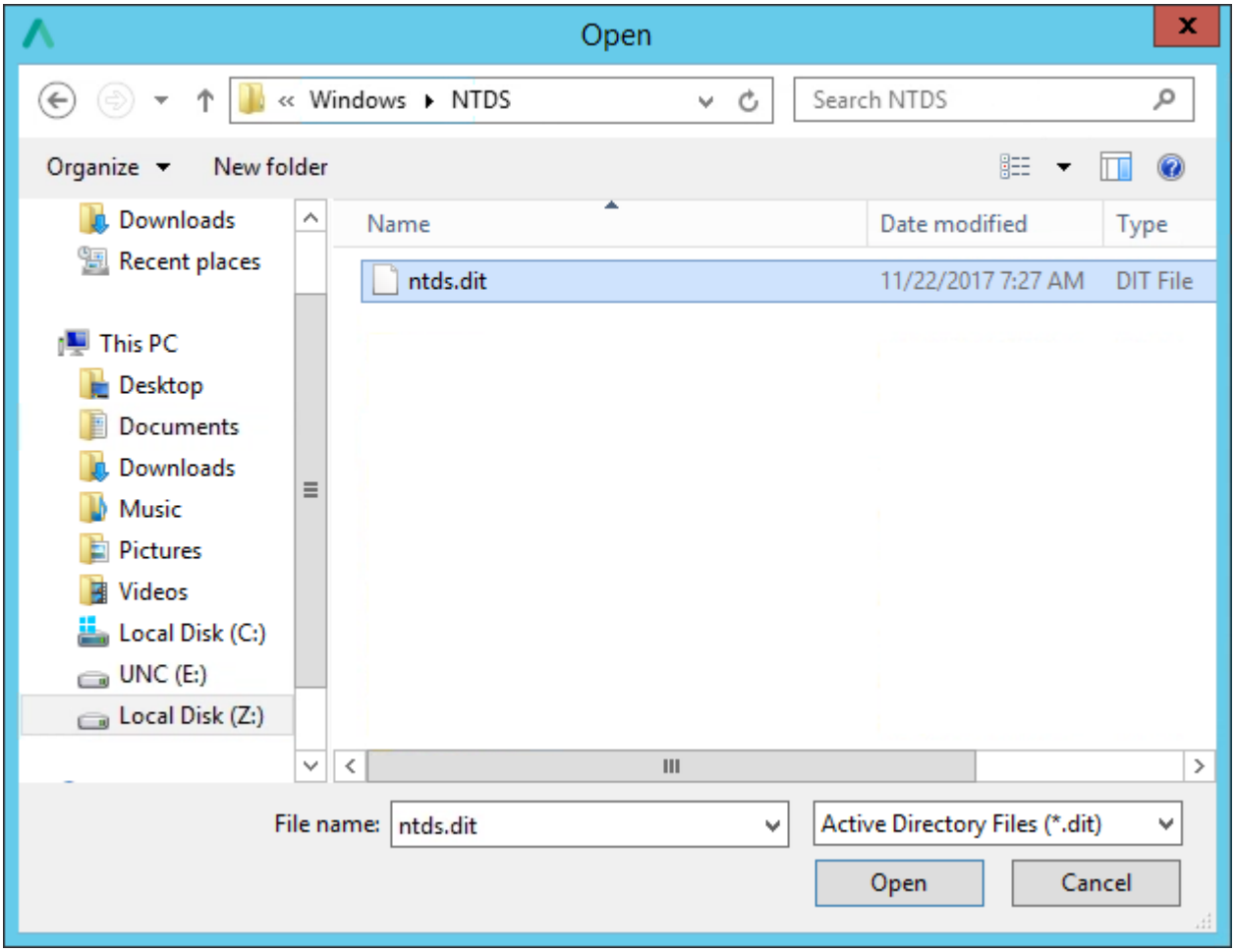
5. Avviare l'utilità di ripristino a livello di oggetto di Active Directory dal seguente percorso:

   <Arcserve UDP installation path>\Engine\BIN\AD_restore.exe

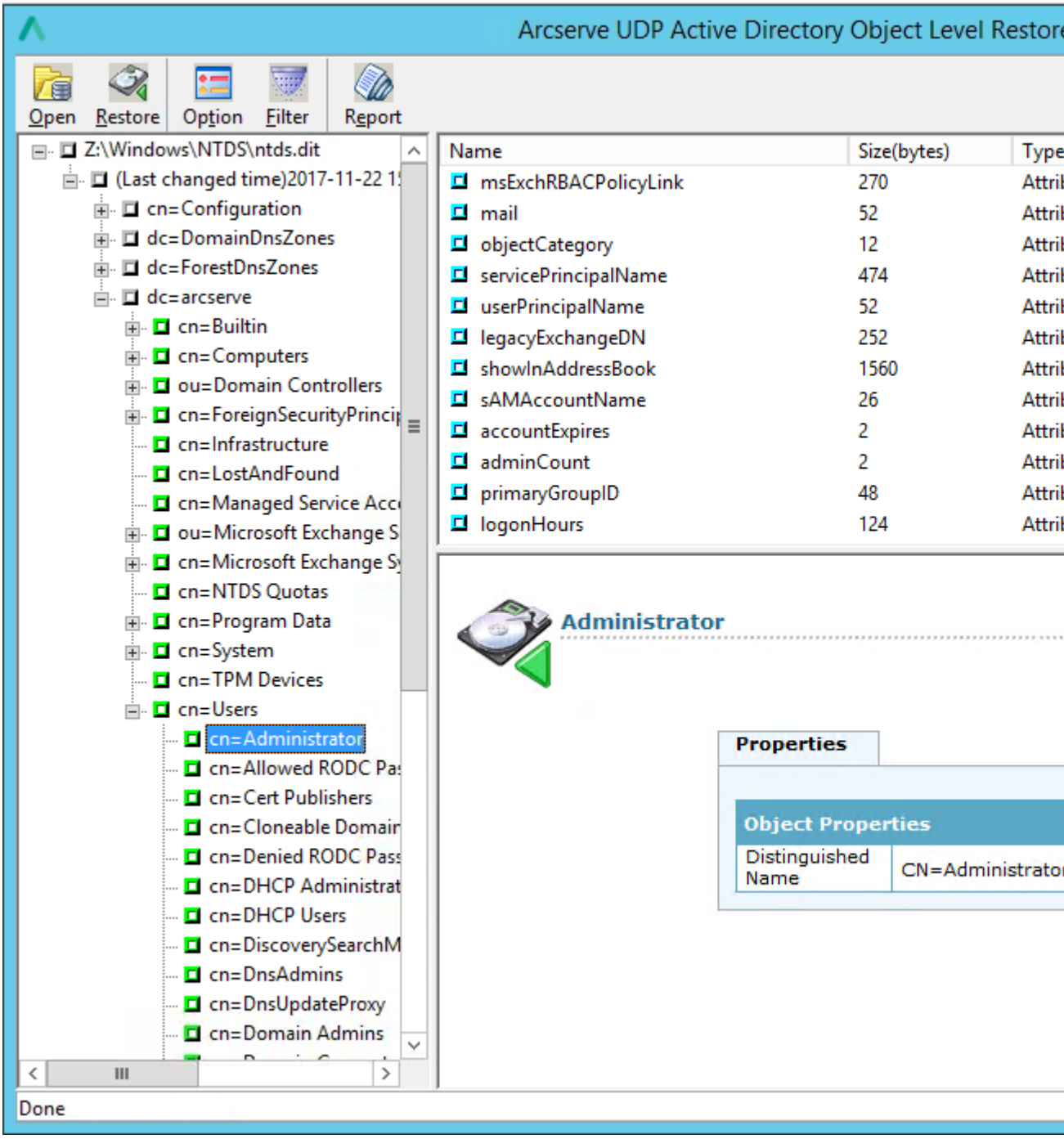
6. Fare clic su **Apri** per aprire la finestra di selezione.



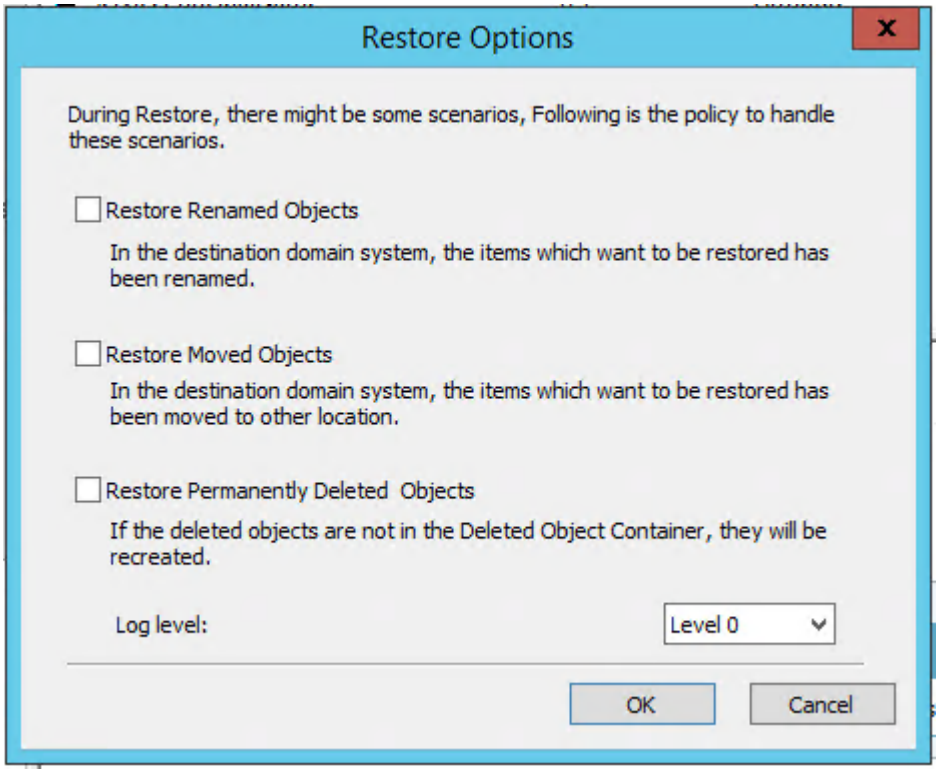
7. Fare clic sull'icona ...(S) e sfogliare il database di Active Directory (NTDS.dit) nel punto di ripristino montato, fare clic su **Apri**, quindi su **OK**.



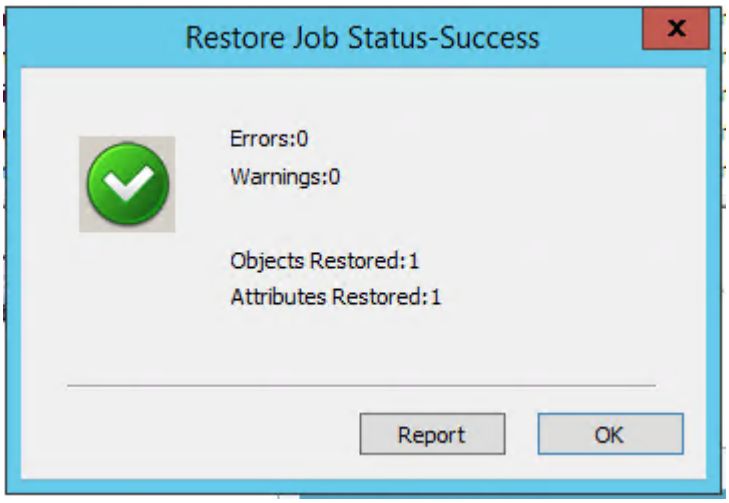
8. Individuare e selezionare gli oggetti o gli attributi di Active Directory che si desidera ripristinare.



9. Fare clic su **Opzioni** per apportare le modifiche necessario al comportamento predefinito, in base alle esigenze.



10. Al termine, fare clic su **OK** per eseguire il processo di ripristino.
11. Al termine del processo di ripristino, viene visualizzata una finestra dei risultati. Fare clic su **Segnala** se si desidera visualizzare i dettagli oppure su **OK** per chiudere.



Note:

- Per impostazione predefinita, l'utilità funziona con l'utente attualmente connesso a Windows per stabilire la connessione.

- Se viene segnalato un errore, l'azione consigliata da eseguire consiste nell'accedere al computer con un account con diritti di amministratore di dominio per eseguire il ripristino.

12. Al termine del processo di ripristino, smontare il volume utilizzato per il ripristino.
13. Per smontare il volume, dalla console dell'agente Arcserve UDP sul computer di backup basato sull'host, fare clic su **Monta punto di ripristino**, quindi su **Smonta**.



Ripristino dei dati di Microsoft Office 365 Exchange

La presente sezione descrive i seguenti argomenti:

Ripristino dei dati della casella di posta di Exchange Online

È possibile ripristinare i dati della casella di posta Exchange Online (messaggi di posta elettronica, calendari, contatti, note, attività e così via) da qualsiasi ambiente cloud Microsoft su qualsiasi computer. È possibile ripristinare i dati dal punto di ripristino nella posizione originale o in una posizione alternativa.

Per eseguire il ripristino dei dati della casella di posta di Exchange Online, procedere come segue:

1. Selezione degli elementi della casella di posta di Exchange Online da ripristinare
2. Definizione delle opzioni di ripristino
3. Ripristino degli elementi recuperabili
4. Ripristino del contenuto del punto di ripristino
5. Verifica del corretto ripristino del contenuto

Selezione degli elementi di posta elettronica di Exchange Online da ripristinare

È possibile ripristinare i dati di posta elettronica di Exchange Online da un punto di ripristino. Quando si seleziona una data di ripristino e poi l'ora, vengono visualizzati tutti i punti di ripristino associati per tale durata. È possibile individuare e selezionare i contenuti di backup (applicazioni incluse) da ripristinare.

Effettuare le operazioni seguenti:

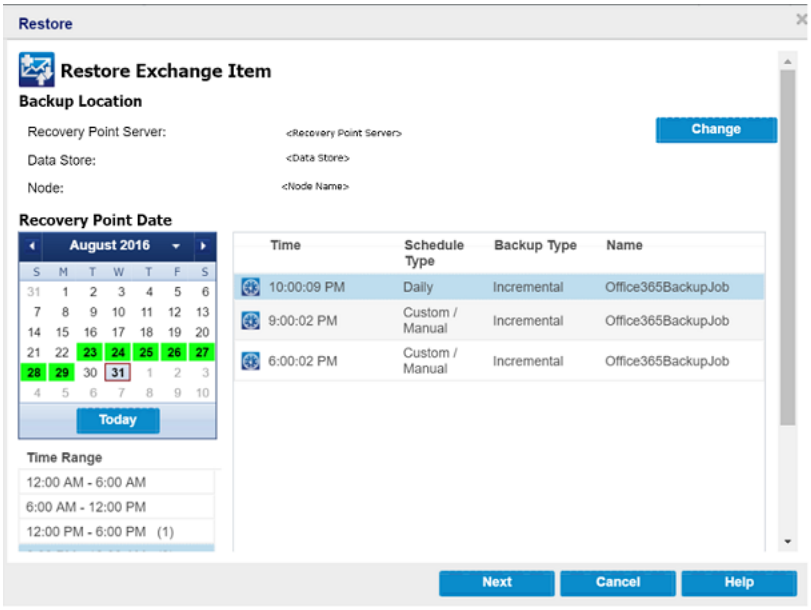
1. Accedere ad Arcserve UDP.
2. Fare clic sulla scheda **Risorse**.
3. Selezionare **Tutti i nodi** nel riquadro sinistro.

   Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.
4. Nel riquadro centrale, selezionare il nodo Exchange Online e fare clic su **Azioni**.
5. Fare clic su **Ripristina** dal menu a discesa Azioni.

   Verrà visualizzata la finestra di dialogo di ripristino della posta di Exchange.

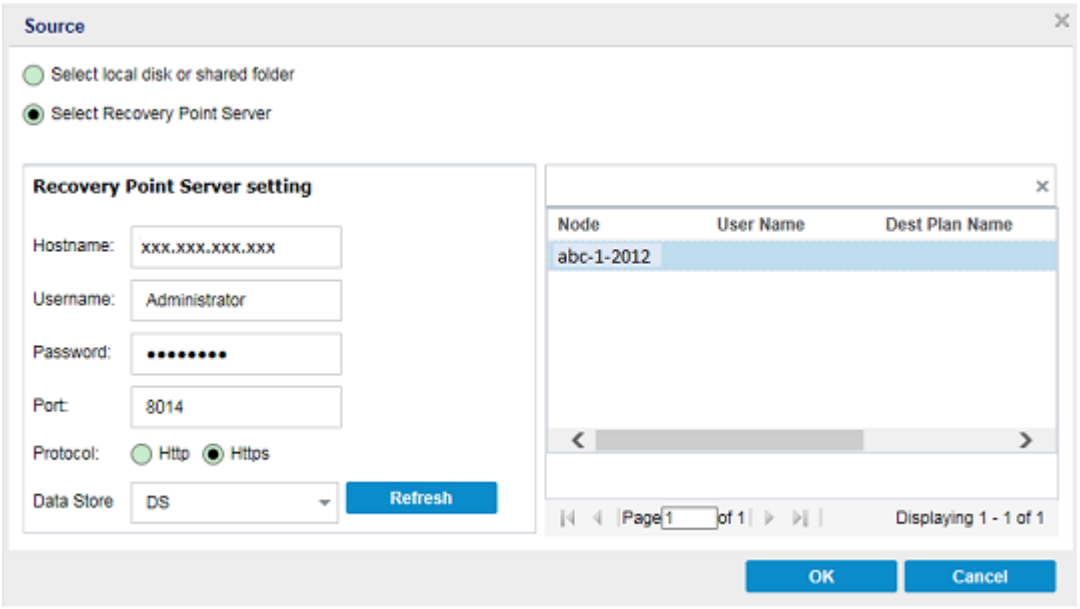
   Nota: L'utente viene connesso automaticamente al nodo dell'agente e viene aperta la finestra di dialogo Ripristina elemento Exchange.

   È possibile visualizzare i dettagli del Recovery Point Server in Posizione di backup.



6. (Facoltativo) Fare clic su **Cambia** per modificare la posizione di backup.

   Viene visualizzata la finestra di dialogo Origine. È possibile selezionare la posizione di backup in questa finestra di dialogo.



   Nota: quando si aggiunge un'attività di copia su nastro al piano e si desidera ripristinare il punto di ripristino del backup di copia su nastro, selezionare il punto di ripristino dal backup di copia su nastro. Per ulteriori informazioni, consultare la sezione Ricerca del punto di ripristino di copia su nastro per il ripristino.

7. Per specificare l'origine, selezionare una delle seguenti opzioni, quindi fare clic su **OK**:

   Selezione di un disco locale o una cartella condivisa

   Nota: In Arcserve UDP non si consiglia di selezionare l'opzione **Seleziona un disco locale o una cartella condivisa**.

   Selezione di un Recovery Point Server

   a. Specificare i dettagli dell'impostazione Recovery Point Server e fare clic su **Aggiorna**.

      Tutti gli agenti vengono elencati nella colonna Data Protection Agent (Agente di protezione dati) nella finestra di dialogo Origine.

   b. Selezionare l'agente dall'elenco visualizzato, quindi fare clic su **OK**.

      I punti di ripristino vengono elencati nella finestra di dialogo di ripristino dell'elemento di Exchange.

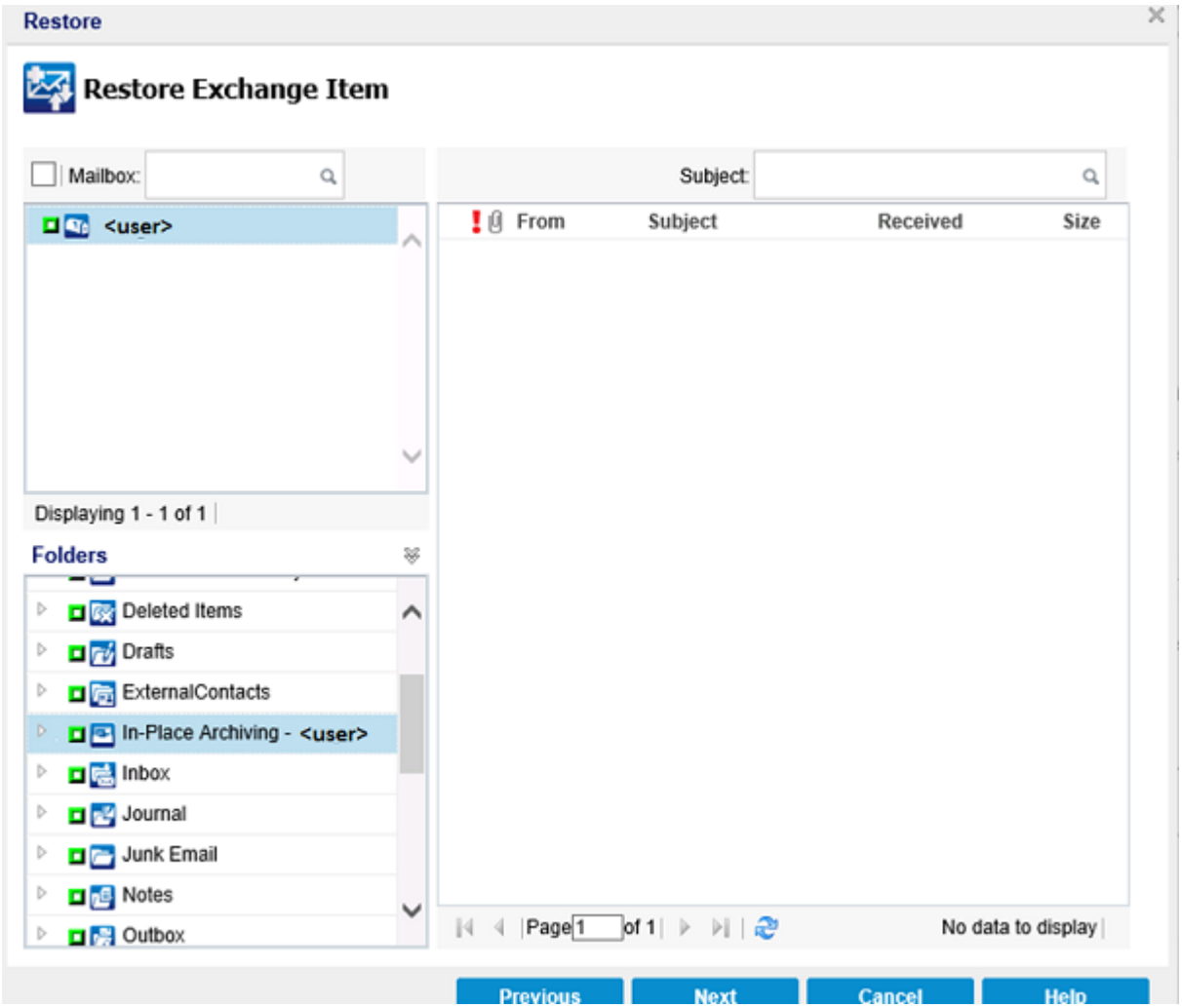
Nota: Dal punto di ripristino Cartella, è possibile che venga visualizzato un numero elevato di cartelle con lo stesso nome con i nodi Exchange Online. Ciò accade poiché il GUID viene modificato e la nuova cartella del punto di ripristino viene creata con l'eliminazione di un nodo e con la sua aggiunta nel piano di verifica.

8. Selezionare la data nel calendario per l'immagine di backup che si desidera ripristinare, quindi fare clic su **Avanti**.

   Tutte le date contenenti punti di ripristino per l'origine di backup specificata sono evidenziate in verde.

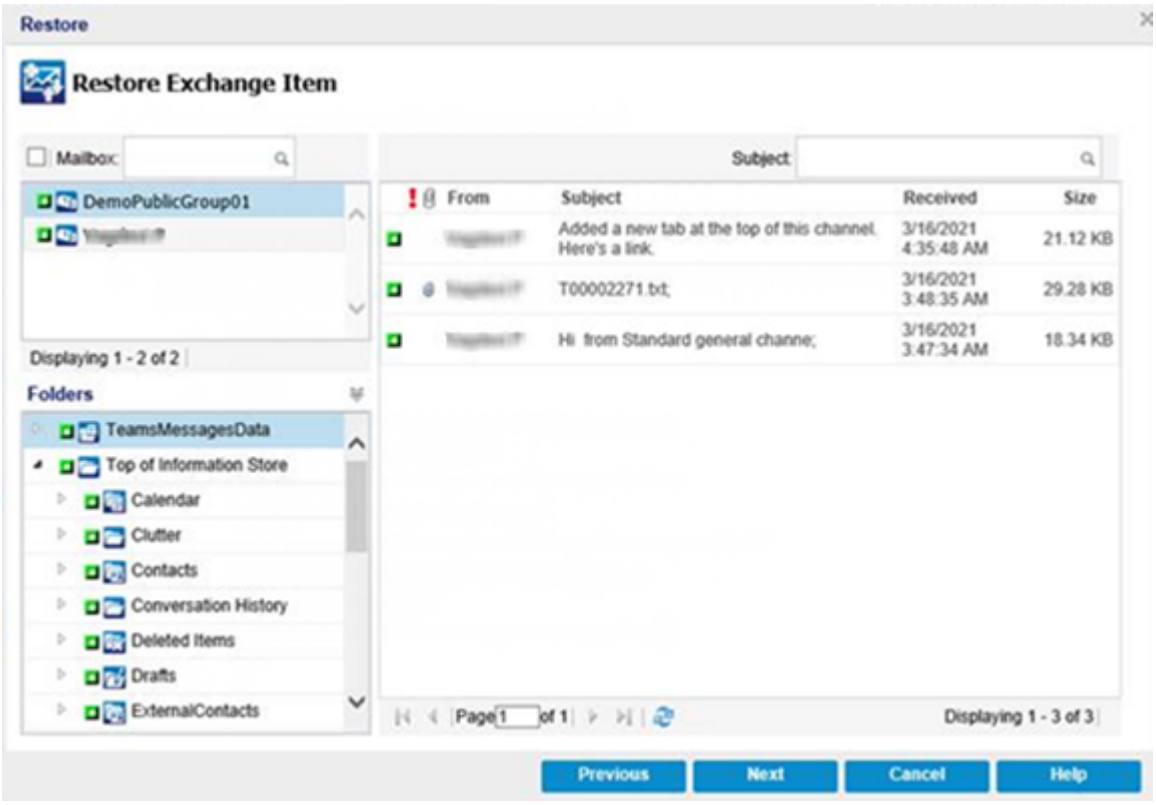
   Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito (completo, incrementale o di verifica) e al nome del backup.

9. Nel riquadro Casella di posta, fare clic sulla casella di posta che si desidera ripristinare.



Nel riquadro Cartelle vengono visualizzati tutti i messaggi di posta corrispondenti.

Nota: per il backup di gruppi di Office 365 Exchange Online, la struttura delle cartelle per la casella di posta del gruppo è diversa dalla casella di posta dell'utente. Le cartelle della casella di posta del gruppo vengono visualizzate nella parte superiore della cartella Archivio informazioni. Ad esempio, quando l'utente esegue il backup delle caselle di posta/elenchi di distribuzione del gruppo AD, tutte le cartelle di cui viene eseguito il backup vengono visualizzate nella parte superiore della cartella Archivio informazioni.



10. Selezionare i messaggi di posta o le cartelle corrispondenti (compresa l'intera casella di posta, i messaggi di posta elettronica, i calendari, i contatti, le note, le attività e così via) che si desiderano ripristinare da Cartelle, quindi fare clic su **Avanti**.

    Note:

    - È possibile selezionare l'intero contenuto oppure parte del contenuto dell'oggetto di Exchange da ripristinare. Per selezionare parte del contenuto, espandere l'oggetto e fare clic sulla casella di controllo del contenuto.
    - È possibile selezionare più oggetti di Exchange da ripristinare.

    Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

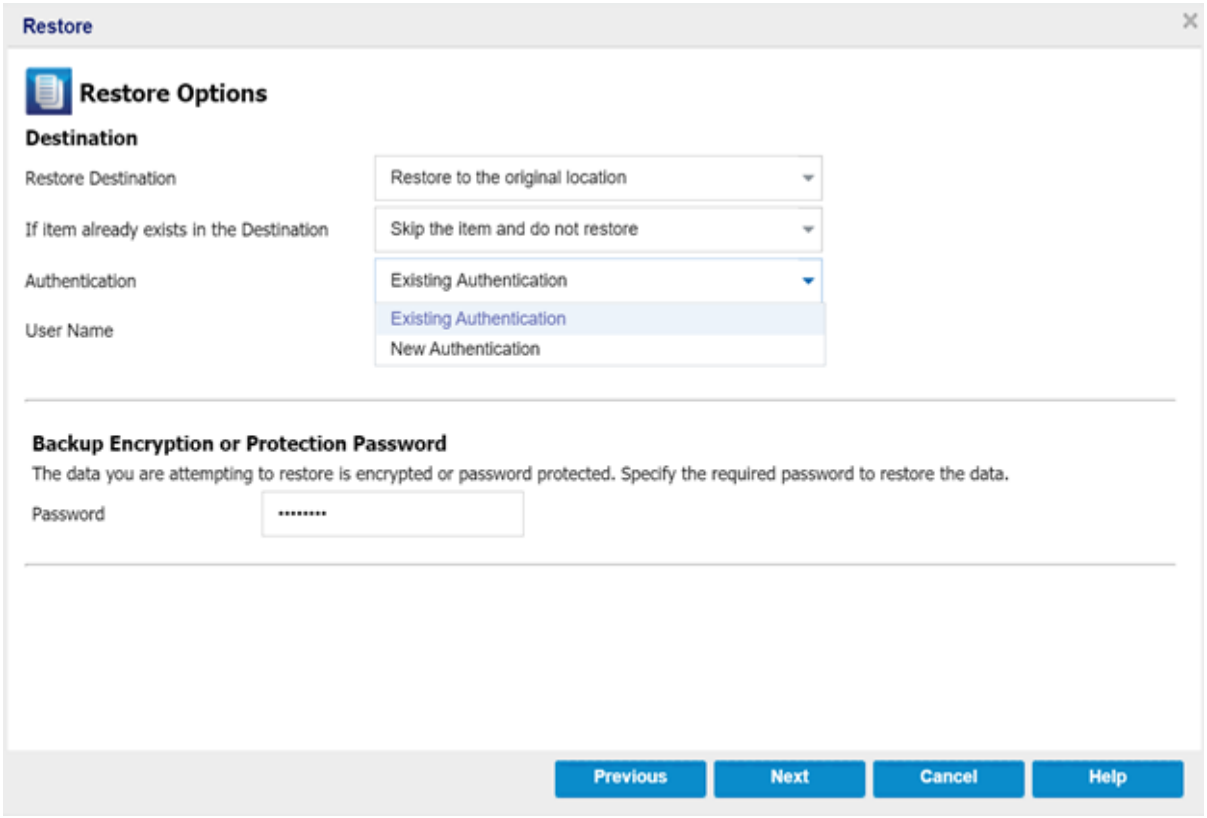
    Gli elementi di posta di Exchange Online da ripristinare sono selezionati. A questo punto, è possibile definire le opzioni di ripristino.

Definizione delle opzioni di ripristino

Dopo avere specificato le informazioni di Exchange Online da ripristinare, definire le opzioni di ripristino per il contenuto selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Opzioni di ripristino**, selezionare la destinazione di ripristino.



Le opzioni di destinazione disponibili sono:

Ripristina in posizione originale

Consente di ripristinare i dati di posta elettronica nella stessa posizione da cui è stato eseguito un backup.

Note:

- Se si ripristina un elemento di posta nella posizione originale mediante l'opzione di sovrascrittura due volte, dopo il secondo ripristino, il primo elemento di posta ripristinato non viene sovrascritto. Di conseguenza, nella posizione originale sono presenti due elementi di posta analoghi.

- Se si ripristina un elemento di posta nella posizione originale mediante l'opzione Ignora e nella cartella originale esiste già un elemento analogo a quello ripristinato, il processo di backup risulterà incompleto.

Ripristina in posizione alternativa

Consente di ripristinare i dati di posta elettronica in un'altra casella di posta o in un'altra cartella nella casella di posta originale. Quando si seleziona questa opzione, è possibile selezionare la destinazione.

2. Specificare una delle opzioni seguenti dall'elenco a discesa **Se l'elemento esiste già nella destinazione**:

Ignora elemento e non ripristinare

Consente di ignorare gli elementi senza eseguire il ripristino.

Impostazione predefinita: Ignora elemento e non ripristinare.

Sovrascrivi elemento nella destinazione

Sovrascrive l'elemento nella destinazione.

Nota: L'elenco a discesa **Se l'elemento esiste già nella destinazione** è disponibile se si seleziona l'opzione **Ripristina in posizione originale** dall'elenco a discesa **Ripristina destinazione**.

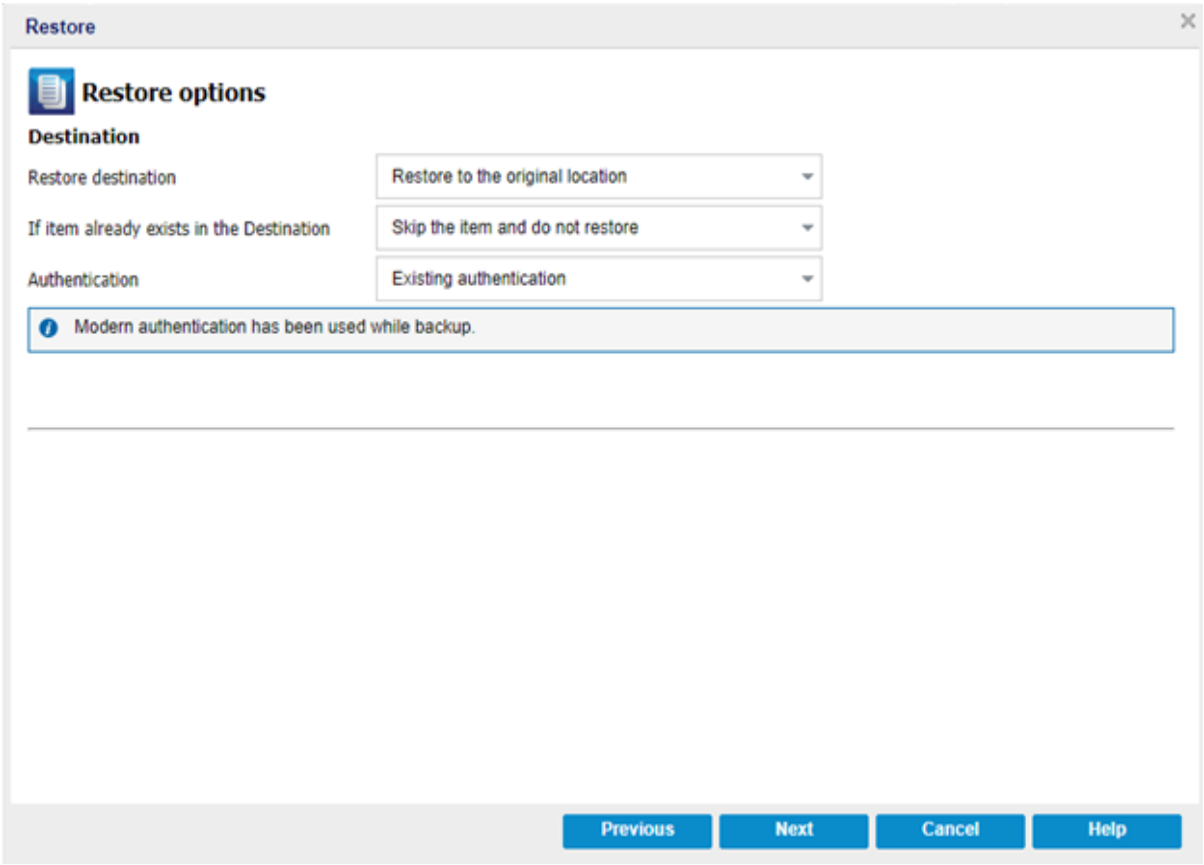
Autenticazione

Convalida e identifica l'account utente. Selezionare una delle seguenti opzioni:

- **Autenticazione esistente**

  Quando si seleziona l'autenticazione esistente, viene utilizzato il tipo di autenticazione selezionato durante la creazione del nodo.

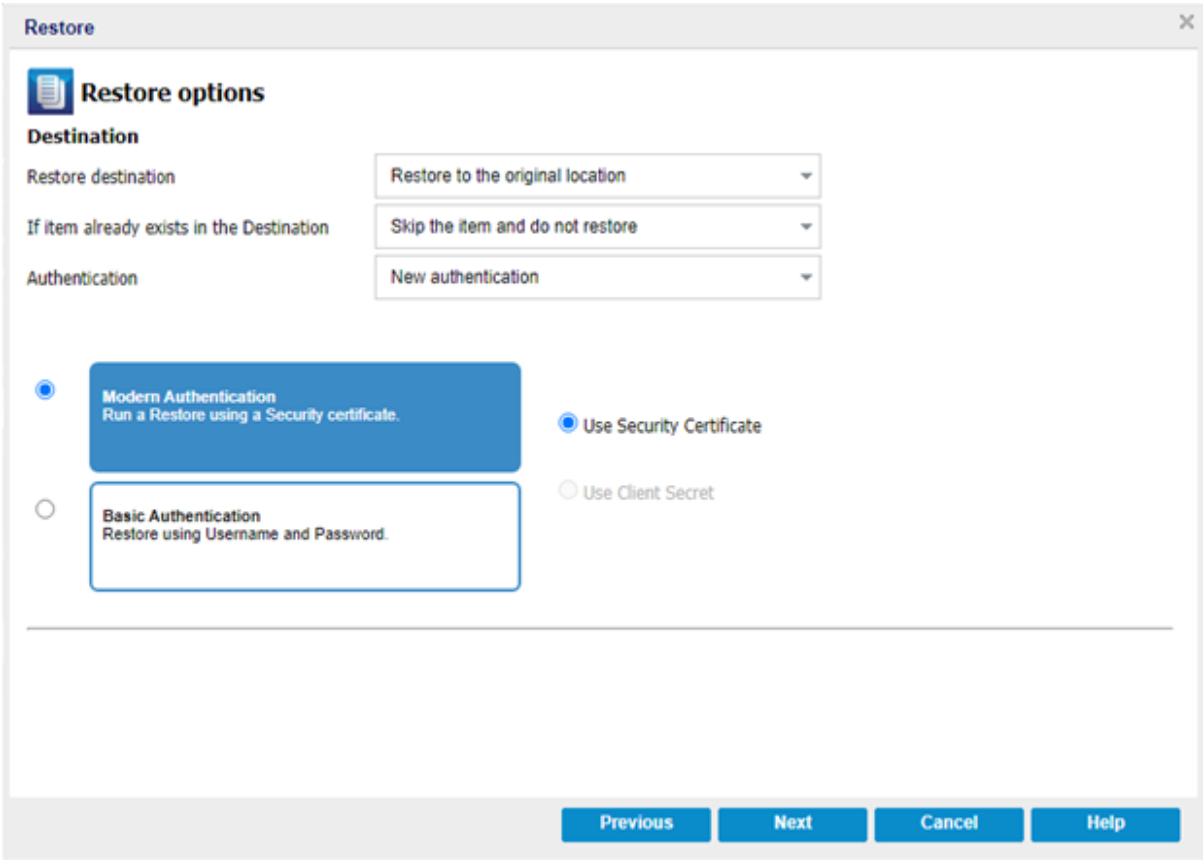
  - Se l'autenticazione del nodo è di base, i parametri quali Nome utente, Password e Crittografia di backup o Password di protezione [se crittografata] vengono caricati automaticamente per procedere con il ripristino.
  - Se l'autenticazione del nodo è moderna, vengono caricati automaticamente parametri quali Nome utente, Crittografia di backup o Password di protezione [se crittografata] per procedere con il ripristino.



- **Nuova autenticazione**

  Durante il ripristino, è possibile selezionare una delle seguenti opzioni per modificare il tipo di autenticazione:

  - Autenticazione moderna
  - Autenticazione di base



3. Per applicare l'autenticazione, eseguire una delle seguenti operazioni:

   Autenticazione moderna

   Per l'autenticazione moderna, è possibile eseguire un ripristino utilizzando un certificato di sicurezza.

   Usa certificato di sicurezza

   Nota: per impostazione predefinita, il piano di backup seleziona l'opzione **Usa certificato di sicurezza** per l'autenticazione moderna.

   Effettuare le operazioni seguenti:

   a. Per eseguire l'autenticazione utilizzando un certificato auto-firmato, consultare la sezione Download del certificato da UDP e caricamento in Azure.

   b. Immettere l'ID applicazione e il nome utente.

   c. Per applicare i ruoli e le autorizzazioni richiesti, selezionare la casella di controllo **Consentire ad Arcserve UDP di impostare i ruoli e le autorizzazioni di Azure richiesti per questa applicazione**, quindi fare clic su **Avanti**.

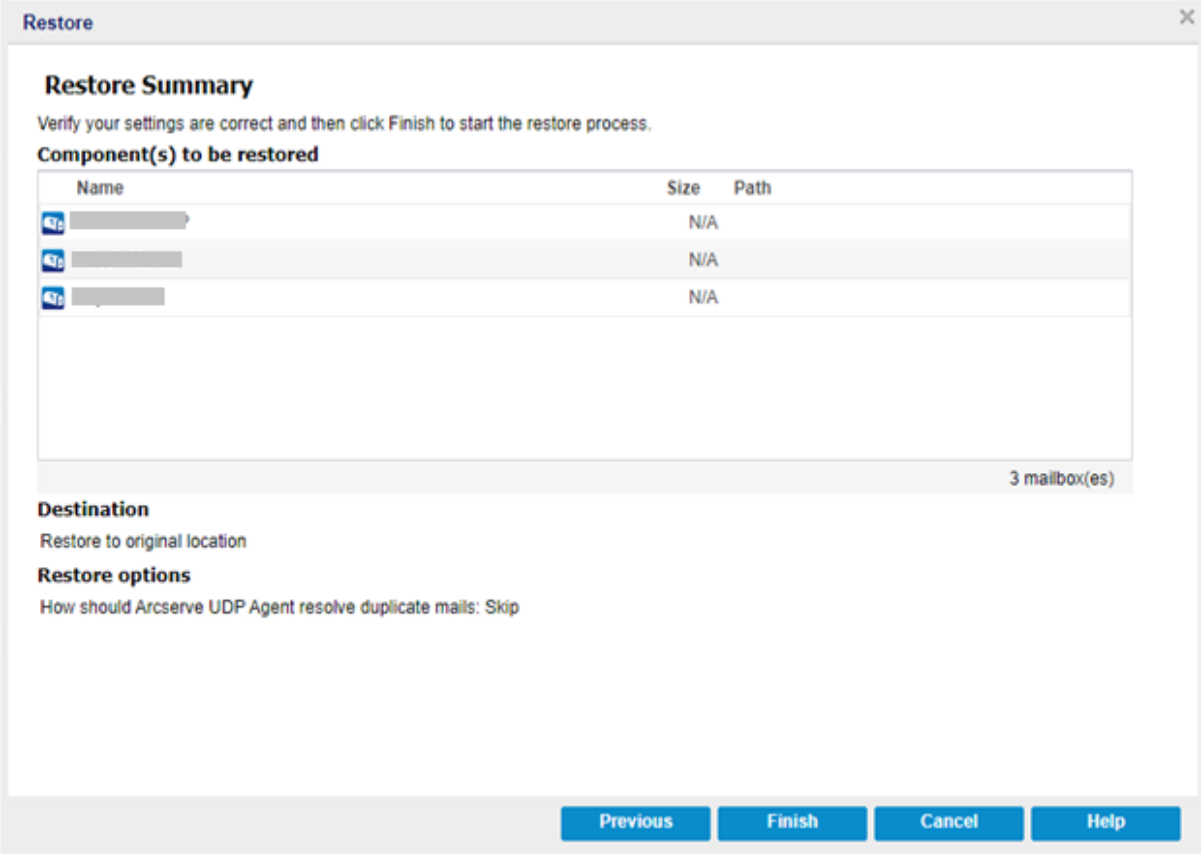
Autenticazione di base

Per l'autenticazione di base, immettere l'ID utente e la password per procedere con il ripristino.

Nota: questa opzione non riesce se l'autenticazione moderna è abilitata sul tenant o sull'account.

4. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Riepilogo ripristino**.



5. Nella finestra Riepilogo ripristino, verificare le impostazioni, quindi fare clic su **Fine**.

Le opzioni di ripristino vengono definite per ripristinare le informazioni di Exchange Online.

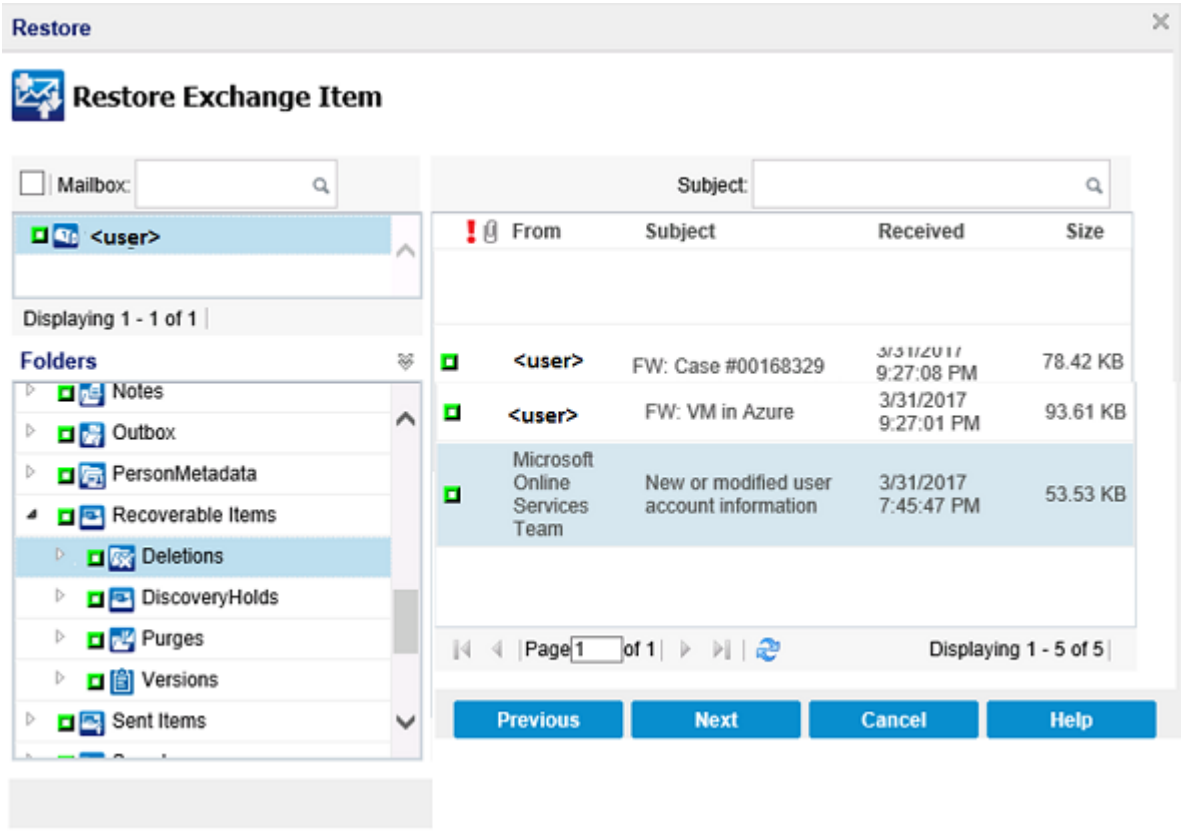
Ripristino degli elementi recuperabili

È possibile ripristinare gli elementi recuperabili dalla casella di posta che consente di utilizzare la funzionalità Blocco sul posto o Blocco per controversia legale, dall'interfaccia utente del nodo Exchange Online per individuare una sessione di backup. Per abilitare questa funzione, consultare la sezione Definizione dell'origine.

Dopo aver abilitato la funzione, mediante la procedura guidata di ripristino è possibile ripristinare gli elementi recuperabili.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Ripristina elemento Exchange**, selezionare le cartelle desiderate in **Elementi recuperabili** e fare clic su **Avanti**.



Verrà visualizzata la finestra Opzioni di ripristino.

2. Dalla schermata Opzioni di ripristino, eseguire i seguenti dettagli e fare clic su **Avanti**:
   - Selezionare Ripristina destinazione.
   - Ignorare o sovrascrivere se l'elemento esiste già nella destinazione.

     È possibile eseguire un ripristino originale o alternativo.

Ripristino originale

Gli elementi recuperabili vengono ripristinati nella cartella *UDP_RecoverableItems_yyyyMMdd_HHmmssfff* creata nella casella di posta di destinazione. Le opzioni Ignora e Sovrascrivi per il ripristino non sono applicabili a questi elementi.

Ripristino alternativo

Comein una casella di posta utente, consente di ripristinare gli elementi selezionati nel percorso di destinazione in una cartella con indicazione di data univoca, ad esempio *denominata /restore_yyyyMMdd-mmssff*.

- Fornire l'ID utente e la password della destinazione in cui si desidera eseguire il ripristino.

Gli elementi recuperabili selezionati vengono ripristinati.

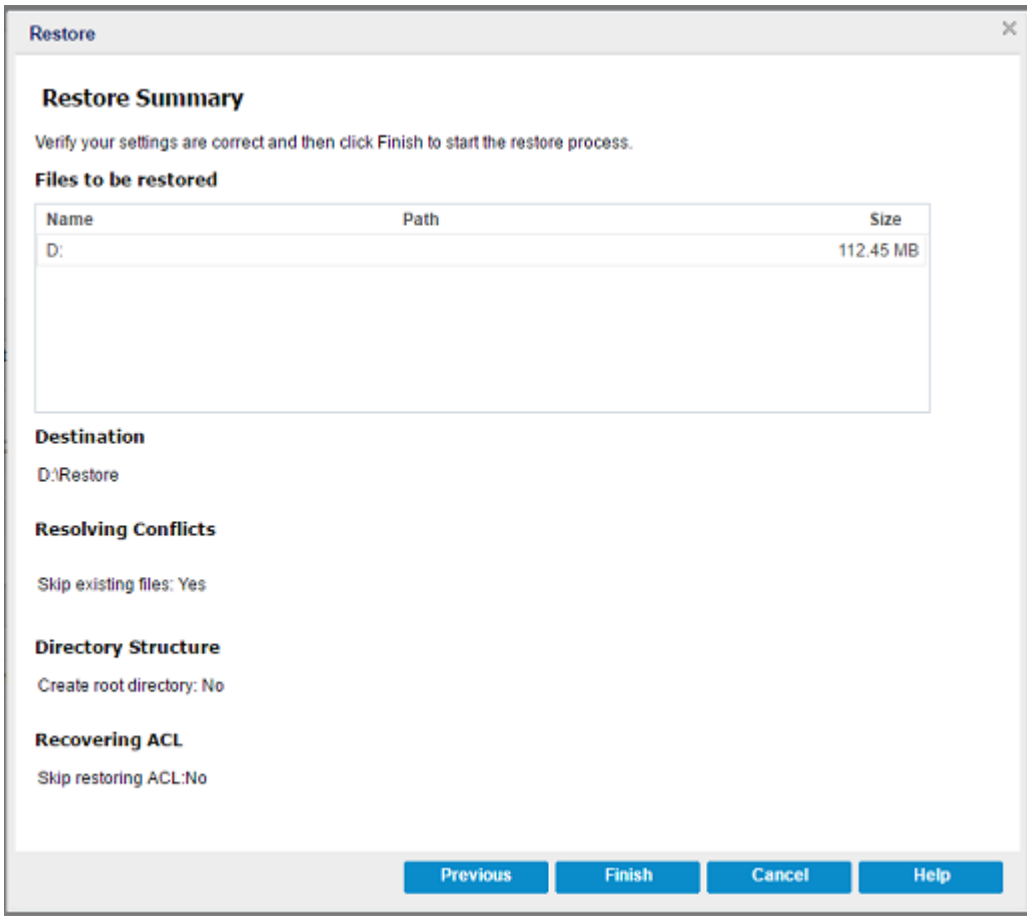
Il contenuto del punto di ripristino viene archiviato.

Ripristino del contenuto del punto di ripristino

Una volta definite le opzioni di ripristino, verificare che le impostazioni siano corrette e confermare il processo di ripristino. Il **Riepilogo di ripristino** consente di verificare tutte le opzioni di ripristino definite e, se necessario, modificarle.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Riepilogo ripristino**, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



   - Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
   - Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

Il contenuto del punto di ripristino viene archiviato.

Verifica del corretto ripristino del contenuto

Una volta completato il processo di ripristino, verificare il ripristino del contenuto nella destinazione specificata.

Effettuare le operazioni seguenti:

1. Accedere alla casella di posta di destinazione.
2. Verificare l'elemento della casella di posta ripristinato.
3. Verificare che il contenuto sia stato ripristinato.

   Il contenuto ripristinato è stato verificato correttamente.

Ripristino dei dati di una raccolta siti di SharePoint Online

È possibile ripristinare l’elenco o la libreria di SharePoint Online o l'elemento dell’elenco nel sito o nel sito padre di SharePoint Online. È possibile ripristinare i dati nel sito originale utilizzando un nuovo nome, ripristinando i dati nella posizione originale ed esportandoli su disco dai punti di ripristino.

Per ripristinare l'elemento dell'elenco di SharePoint Online, procedere come segue:

1. Selezione degli elementi nell'elenco del sito di SharePoint Online da ripristinare
2. Definizione delle opzioni di ripristino
3. Verifica del corretto ripristino del contenuto

Selezione degli elementi nell'elenco del sito di SharePoint Online da ripristinare

È possibile ripristinare i dati degli elementi nell'elenco di SharePoint Online da un punto di ripristino. Quando si seleziona una data di ripristino e poi l'ora, vengono visualizzati tutti i punti di ripristino associati per tale durata. È possibile individuare e selezionare i contenuti di backup (applicazioni incluse) da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere ad Arcserve UDP.
2. Fare clic sulla scheda **Risorse**.
3. Selezionare **Tutti i nodi** nel riquadro sinistro.

   Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   Oppure

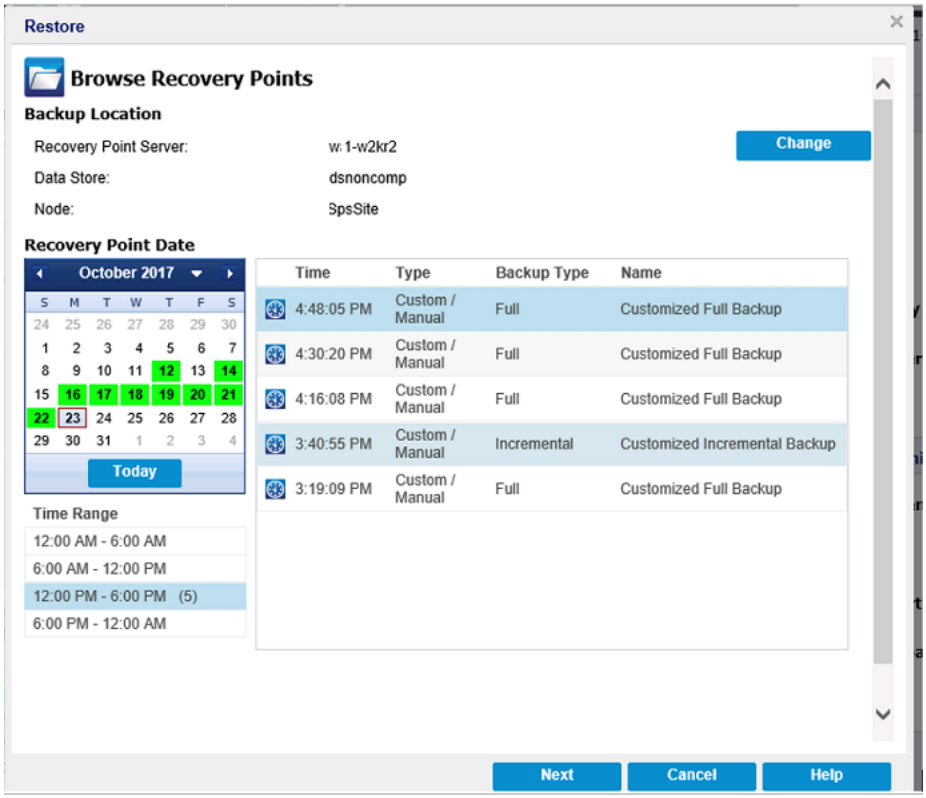
   Selezionare il gruppo **Nodi SharePoint Online**.

   Tutti i nodi SharePoint Online aggiunti vengono visualizzati nel riquadro centrale.
4. Nel riquadro centrale, selezionare il nodo SharePoint Online e fare clic su **Azioni**.
5. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

   Verrà visualizzata la finestra di dialogo di **ripristino della posta di SharePoint**.

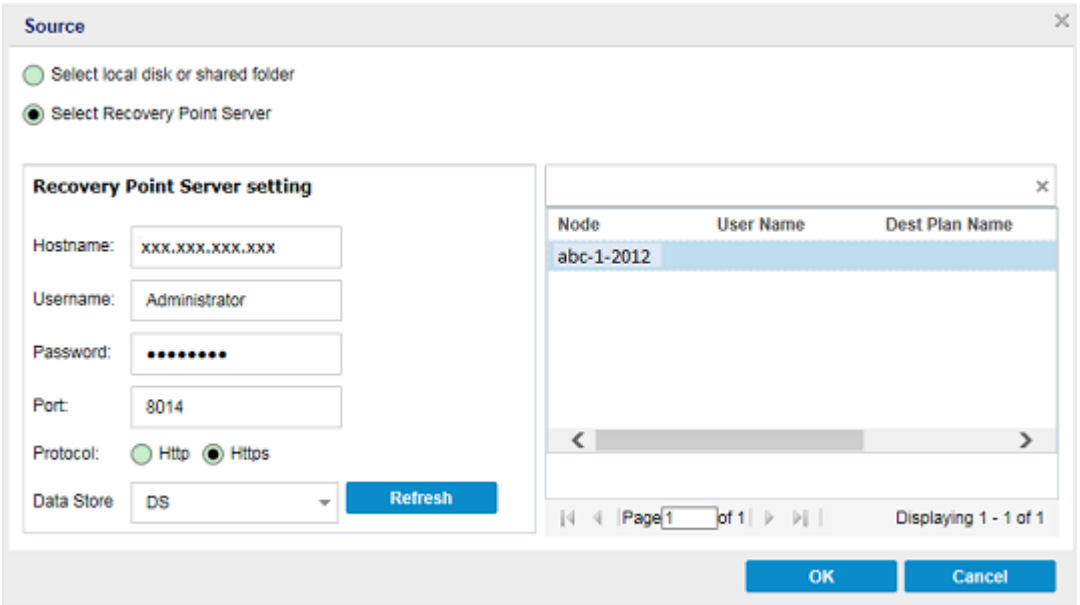
   Nota: L'utente viene connesso automaticamente al nodo dell'agente e viene aperta la finestra di dialogo **Ripristina elemento SharePoint**.

   La **posizione di backup** mostra i dettagli del **Recovery Point Server**.



6. (Facoltativo) Fare clic su **Cambia** per modificare la posizione di backup.

   Viene visualizzata la finestra di dialogo **Origine**. È possibile selezionare la posizione di backup in questa finestra di dialogo.



Nota: quando si aggiunge un'attività di copia su nastro al piano e si desidera ripristinare il punto di ripristino del backup di copia su nastro, selezionare il punto di

ripristino dal backup di copia su nastro. Per ulteriori informazioni, consultare la sezione Ricerca del punto di ripristino di copia su nastro per il ripristino.

7. Per specificare l'origine, selezionare una delle seguenti opzioni, quindi fare clic su **OK**:

   Selezione di un disco locale o una cartella condivisa

   Nota: In Arcserve UDP non si consiglia di selezionare l'opzione **Seleziona un disco locale o una cartella condivisa**.

   Selezione di un Recovery Point Server

   a. Specificare i dettagli dell'impostazione Recovery Point Server e fare clic su **Aggiorna**.

      Tutti gli agenti vengono elencati nella colonna Data Protection Agent (Agente di protezione dati) nella finestra di dialogo **Origine**.

   b. Selezionare l'agente dall'elenco/libreria visualizzato e fare clic su **OK**.

      I punti di ripristino vengono elencati nella finestra di dialogo di **ripristino dell'elemento di SharePoint**.

8. Selezionare la data per l'immagine di backup che si desidera ripristinare e fare clic su **Avanti.**

   Tutte le date contenenti punti di ripristino per l'origine di backup specificata sono evidenziate in verde.

   Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito (completo, incrementale) e al nome del backup.

9. Dalla finestra di dialogo di **ripristino degli elementi di SharePoint Online**, espandere la raccolta siti.

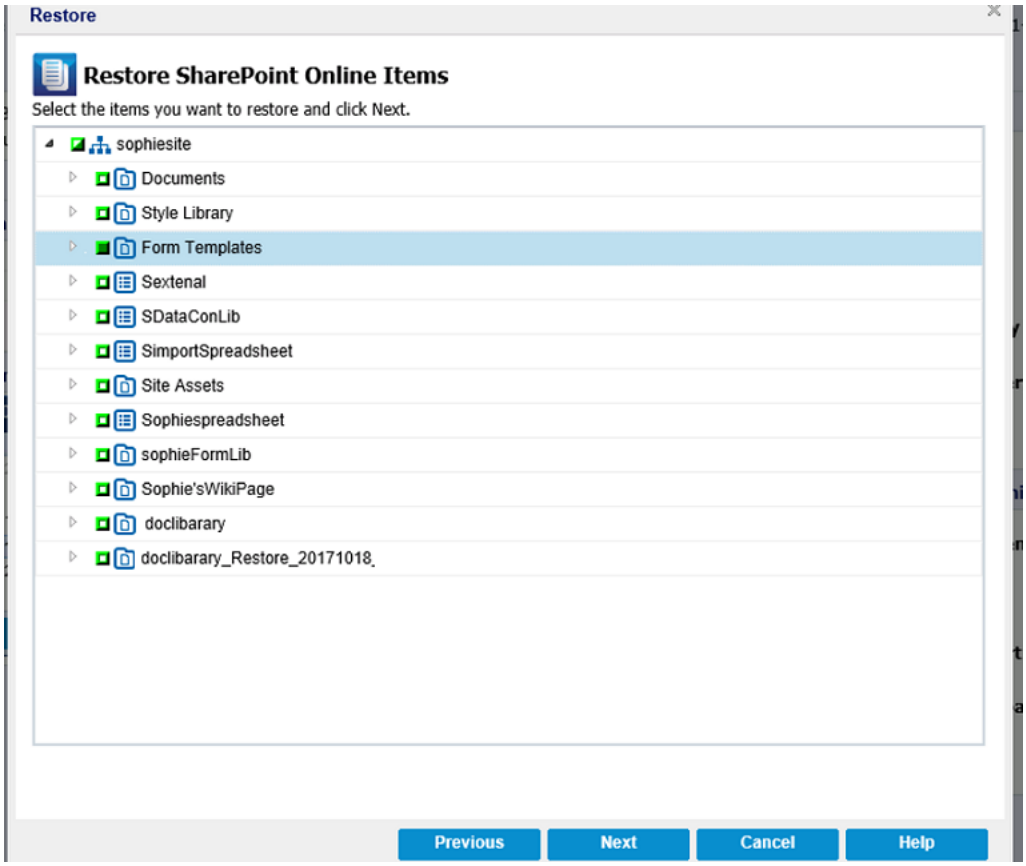
   Vengono visualizzati tutti gli elenchi/librerie e un elenco.

10. Selezionare l'elenco/libreria o l'elemento disponibile nella raccolta siti di cui si desidera eseguire il ripristino della raccolta siti SharePoint e fare clic su **Avanti**.

    Note:

    - È possibile selezionare l'intero contenuto oppure parte del contenuto dell'oggetto di SharePoint da ripristinare. Per selezionare parte del contenuto, espandere l'oggetto e fare clic sulla casella di controllo del contenuto.
    - È possibile selezionare più elenchi/librerie o l'elenco degli elementi di SharePoint da ripristinare.

Verrà visualizzata la finestra di dialogo **Opzioni di ripristino**.



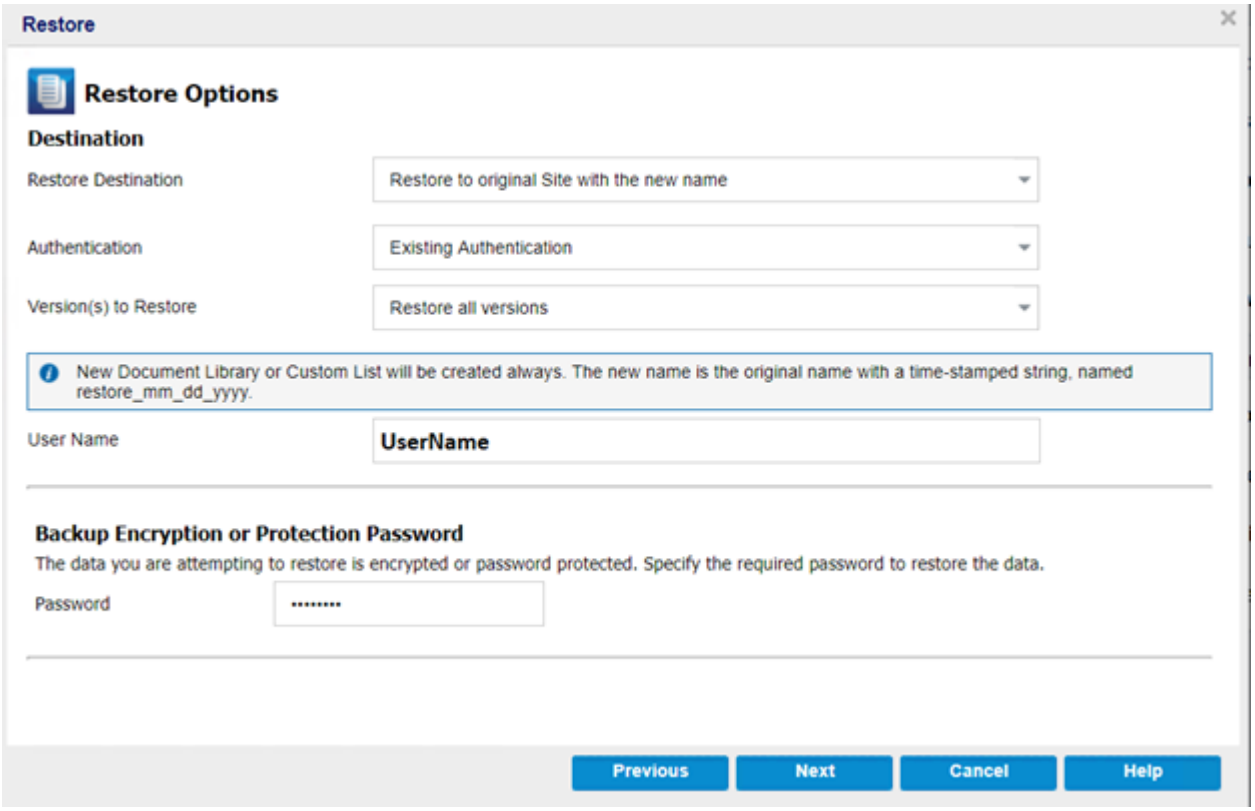
Gli elenchi/librerie o gli elementi dell'elenco di SharePoint Online da ripristinare vengono selezionati. A questo punto, è possibile definire le opzioni di ripristino.

Definizione delle opzioni di ripristino

Dopo avere specificato le informazioni di SharePoint Online da ripristinare, definire le opzioni di ripristino per il contenuto selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Opzioni di ripristino**, selezionare la destinazione di ripristino.



Le opzioni di destinazione disponibili sono:

Ripristina il sito originale con il nuovo nome

Ripristina l'elenco/libreria e i dati degli elementi nell'elenco nello stesso sito con il nome del nuovo elenco da cui è stato eseguito un backup.

Ripristino nella posizione originale

Consente di ripristinare l'elenco/libreria e i dati degli elementi nella stessa posizione da cui è stato eseguito un backup.

2. Specificare una delle opzioni seguenti dall'elenco a discesa **Se l'elemento esiste già nella destinazione**:

Se il controllo delle versioni è abilitato, aggiungere come nuova versione

Questa opzione funziona quando è abilitata l'impostazione della versione dall'impostazione libreria nel sito di SharePoint. Quando si seleziona questa opzione, se sono presenti gli elementi dell'elenco per le versioni correnti, viene aggiunta la nuova versione alle versioni correnti degli elementi dell'elenco.

Ignora elemento e non ripristinare

Consente di ignorare gli elementi senza eseguire il ripristino.

Sovrascrivi elemento nella destinazione

Sovrascrive l'elemento nella destinazione.

Esporta su disco

Consente di ripristinare gli elenchi/librerie o gli elementi nell'elenco della raccolta siti in una cartella o in una cartella condivisa nel disco.

Nota: Per il ripristino degli elenchi quando si seleziona l'opzione di ripristino dell'esportazione su disco, esportare su disco solamente gli allegati dell'elenco.

Autenticazione

Convalida e identifica l'account utente. Selezionare una delle seguenti opzioni:

- **Autenticazione esistente**

  Quando si seleziona l'autenticazione esistente, viene utilizzato il tipo di autenticazione selezionato durante la creazione del nodo.

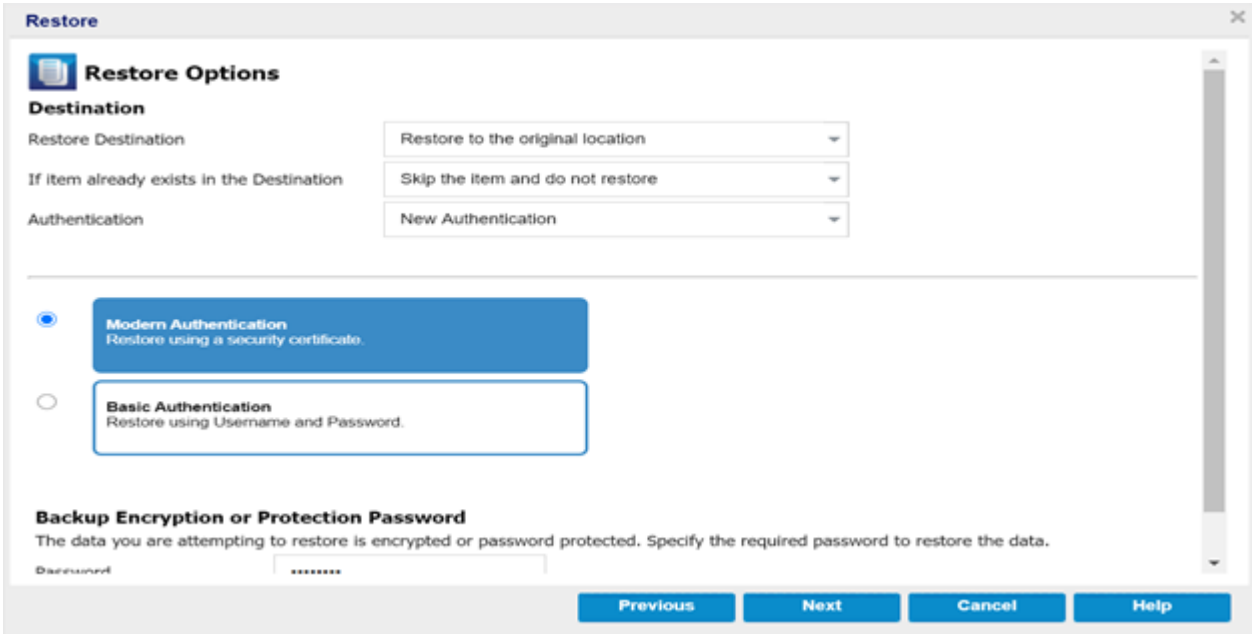
  - Se l'autenticazione del nodo è di base, i parametri quali Nome utente, Password e Crittografia di backup o Password di protezione [se crittografata] vengono caricati automaticamente per procedere con il ripristino.
  - Se l'autenticazione del nodo è moderna, vengono caricati automaticamente parametri quali Nome utente, Crittografia di backup o Password di protezione [se crittografata] per procedere con il ripristino.

- **Nuova autenticazione**

  Durante il ripristino, è possibile selezionare una delle seguenti opzioni per modificare il tipo di autenticazione:

  - Autenticazione moderna

- Autenticazione di base



3. Per applicare l'autenticazione, eseguire una delle seguenti operazioni:

Autenticazione moderna

Per l'autenticazione moderna, è possibile eseguire un ripristino utilizzando un certificato di sicurezza.

Usa certificato di sicurezza

Nota: per impostazione predefinita, il piano di backup seleziona l'opzione **Usa certificato di sicurezza** per l'autenticazione moderna.

Effettuare le operazioni seguenti:

a. Per eseguire l'autenticazione utilizzando un certificato autofirmato, consultare la sezione Download del certificato da UDP e caricamento in Azure.

b. Immettere l'ID applicazione e il nome utente.

c. Per applicare i ruoli e le autorizzazioni richiesti, selezionare la casella di controllo **Consentire ad Arcserve UDP di impostare i ruoli e le autorizzazioni di Azure richiesti per questa applicazione**, quindi fare clic su **Avanti**.

Autenticazione di base

Per l'autenticazione di base, immettere il nome utente e la password per procedere con il ripristino.

Nota: questa opzione non riesce se l'autenticazione moderna è abilitata sul tenant o sull'account.

4. Specificare le versioni dell'elemento nell'elenco che si desidera ripristinare quando è abilitata l'impostazione della versione dall'impostazione libreria nel sito di SharePoint.

   Ripristina tutte le versioni

   Consente di ripristinare tutte le versioni del backup.

   Ripristina solo la versione più recente

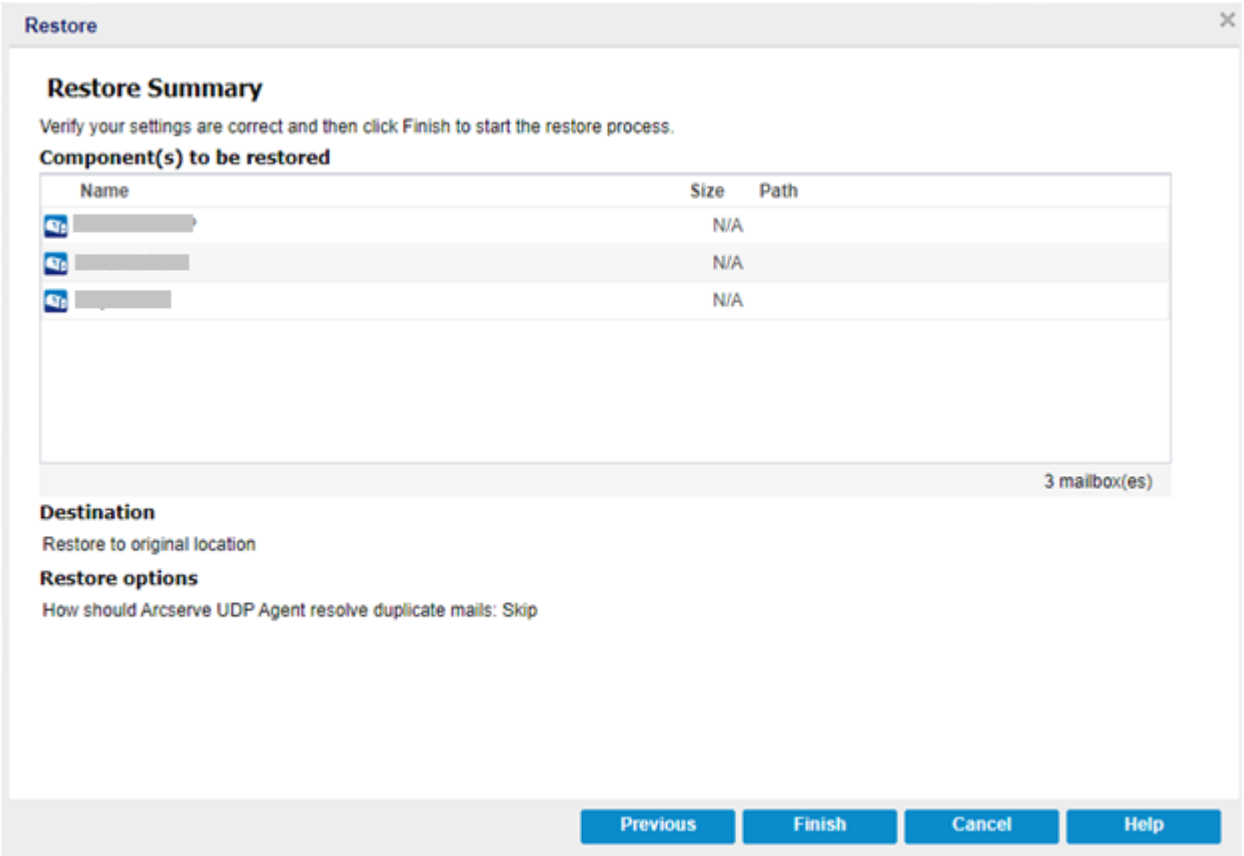
   Consente di ripristinare solo l'ultima versione del backup.

   Ripristina solo la versione principale più recente

   Consente di ripristinare solo la versione principale più recente del backup.

5. Specificare la password della sessione se necessario.
6. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Riepilogo ripristino**.



   È possibile verificare le informazioni di ripristino nella finestra di dialogo Riepilogo ripristino.

7. Fare clic su **Fine** per inviare il processo ripristinato.

Le opzioni di ripristino vengono definite per ripristinare le informazioni di SharePoint Online.

Verifica del corretto ripristino del contenuto

Una volta completato il processo di ripristino, verificare il ripristino del contenuto nella destinazione specificata.

Effettuare le operazioni seguenti:

1. Accedere alla raccolta siti di SharePoint.
2. Verificare l'elenco/libreria e gli elementi dell'elenco.
3. Verificare che il contenuto sia stato ripristinato.

   Il contenuto ripristinato è stato verificato correttamente.

Ripristino dei dati di OneDrive

È possibile ripristinare i dati OneDrive (file, cartelle e così via) utilizzando qualsiasi computer. È possibile eseguire il ripristino utilizzando l'opzione di ripristino o di montaggio del volume dall'interfaccia utente dell'agente.

Per ripristinare i dati di OneDrive utilizzando l'opzione di ripristino, procedere come segue:

1. Selezione degli elementi di OneDrive da ripristinare
2. Definizione delle opzioni di ripristino
3. Visualizzazione del riepilogo del ripristino

In alternativa

Ripristino dei dati di OneDrive mediante l'opzione di montaggio del volume.

Selezione degli elementi di OneDrive da ripristinare

È possibile ripristinare i dati di OneDrive da un punto di ripristino. Quando si seleziona una data di ripristino e poi l'ora, vengono visualizzati tutti i punti di ripristino associati per tale durata. È possibile individuare e selezionare i contenuti di backup (applicazioni incluse) da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere ad Arcserve UDP.
2. Fare clic sulla scheda **Risorse**.
3. Selezionare **Tutti i nodi** nel riquadro sinistro.

   Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.
4. Nel riquadro centrale, selezionare il nodo di OneDrive e fare clic su **Azioni**.
5. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

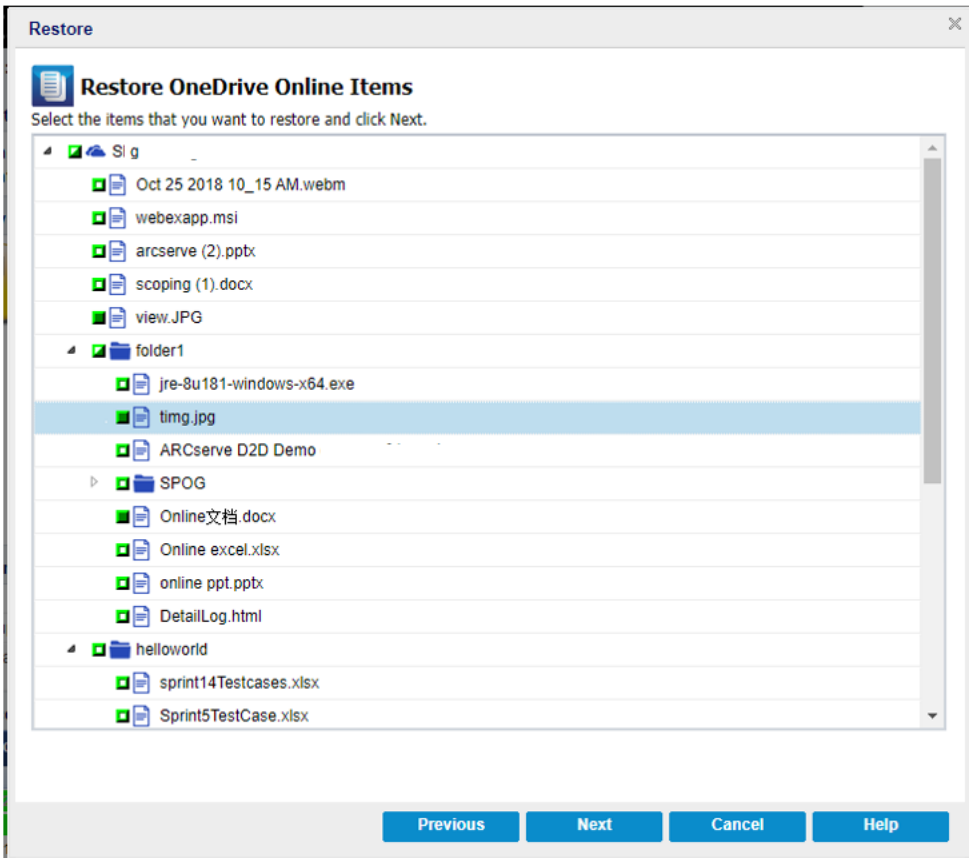
   Nota: l'utente viene connesso automaticamente al nodo dell'agente e viene aperta la finestra di dialogo **Nodo**.

   È possibile visualizzare i dettagli di **Sfoglia punti di ripristino** nella posizione di backup. Viene visualizzato il nome del *Recovery Point Server* selezionato. Se si desidera, fare clic su **Modifica** e modificare l'impostazione **Recovery Point Server** dal popup **Origine**.

   Nota: quando si aggiunge un'attività di copia su nastro al piano e si desidera ripristinare il punto di ripristino del backup di copia su nastro, selezionare il punto di ripristino dal backup di copia su nastro. Per ulteriori informazioni, consultare la sezione Ricerca del punto di ripristino di copia su nastro per il ripristino.
6. Selezionare la data per l'immagine di backup che si desidera ripristinare e fare clic su **Avanti.**

   Tutte le date contenenti punti di ripristino per l'origine di backup specificata sono evidenziate in verde.

   Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito (completo, incrementale) e al nome del backup.
7. Nel riquadro di **ripristino degli elementi del nodo di OneDrive**, selezionare le caselle di controllo per gli elementi correlati o le cartelle che si desidera ripristinare da Cartelle e fare clic su **Avanti**.



Note:

- È possibile selezionare l'intero contenuto oppure parte del contenuto dell'oggetto di OneDrive da ripristinare. Per selezionare parte del contenuto, espandere l'oggetto e fare clic sulla casella di controllo del contenuto.
- È possibile selezionare più oggetti di OneDrive da ripristinare.

Verrà visualizzata la finestra di dialogo **Opzioni di ripristino**.

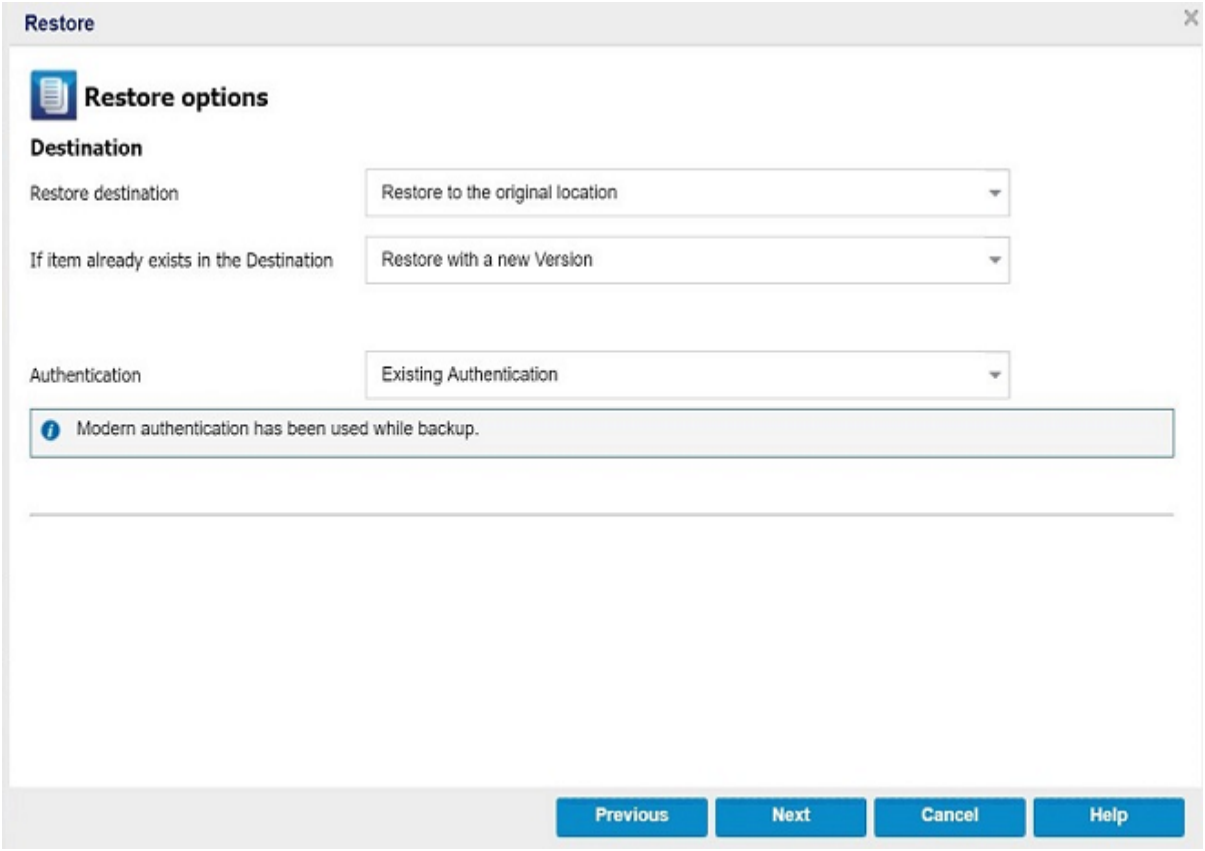
Vengono selezionati gli elementi del nodo di OneDrive da ripristinare. A questo punto, è possibile definire le opzioni di ripristino.

Definizione delle opzioni di ripristino

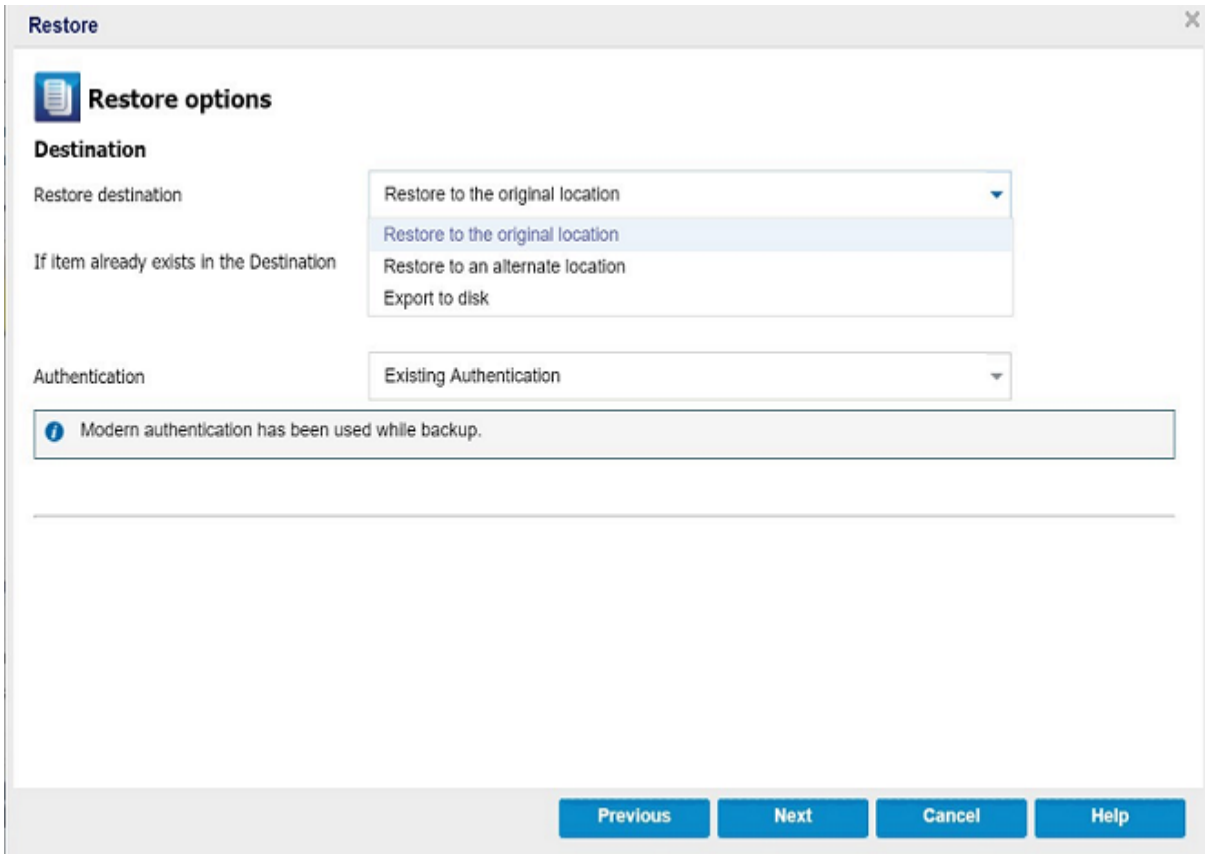
Dopo avere specificato le informazioni di OneDrive da ripristinare, definire le opzioni di ripristino per il contenuto selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Opzioni di ripristino**, selezionare la destinazione di ripristino.



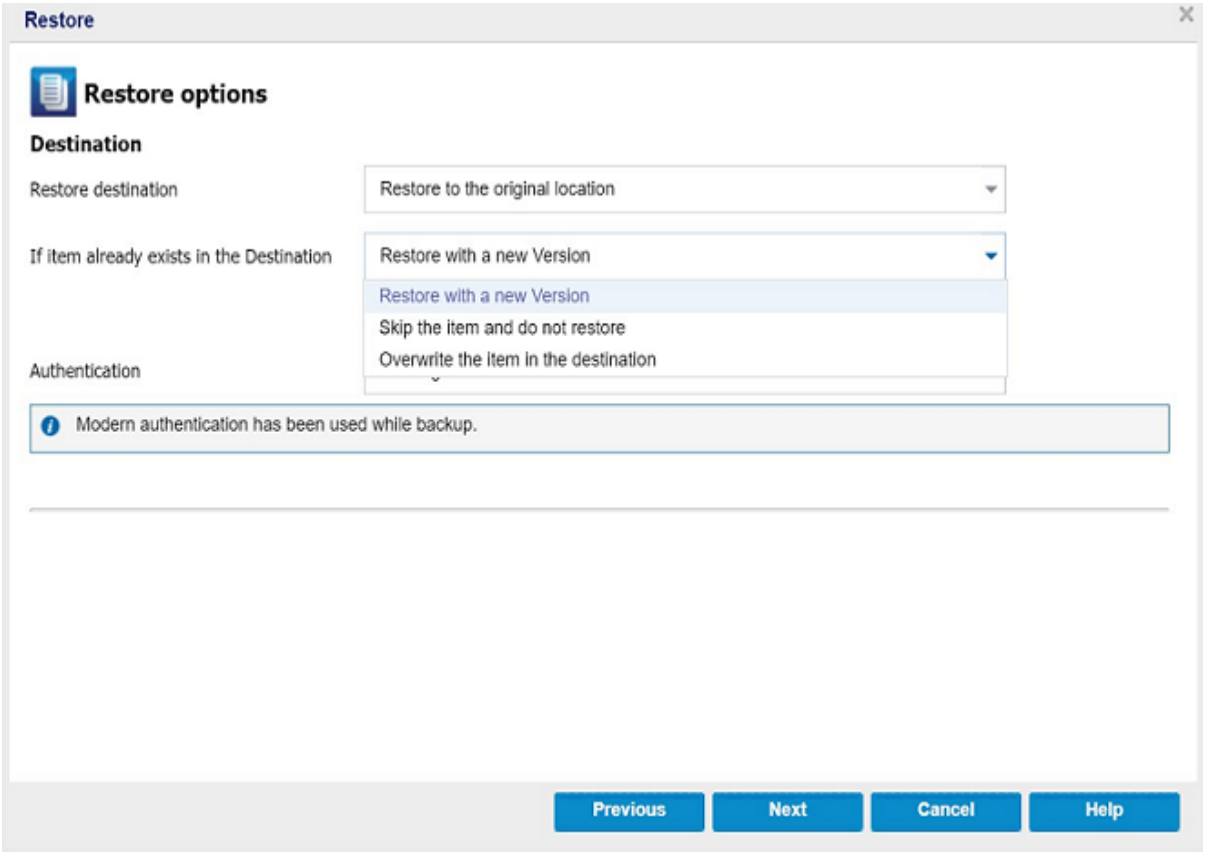
Le opzioni di destinazione disponibili sono:



Ripristino nella posizione originale

Consente di ripristinare i file o le cartelle nella stessa posizione da cui è stato eseguito un backup.

Se si seleziona l'opzione **Ripristina nella posizione originale**, dall'elenco a discesa **Se l'elemento esiste già**, selezionare una delle opzioni seguenti:



Eseguire il ripristino con una nuova versione

Aggiunge la nuova versione ai file esistenti.

Questa opzione è selezionata per impostazione predefinita.

Ignora elemento e non ripristinare

Consente di ignorare gli elementi senza eseguire il ripristino.

Sovrascrivi elemento nella destinazione

Sovrascrive l'elemento nella destinazione.

Ripristina in posizione alternativa

Ripristina i file, le cartelle o gli account su un account nella posizione alternativa. Quando si seleziona questa opzione, è possibile selezionare la destinazione.

Gerarchia dell'origine

Conserva la struttura gerarchica in base a quanto specificato nell'origine durante la creazione dei piani di backup.

Nota: questa opzione viene visualizzata solo quando è selezionata l'opzione Ripristina in posizione alternativa.

Esporta su disco

Esegue il ripristino in una cartella o in una cartella condivisa sul disco.

2. Per convalidare e identificare l'account utente, dall'elenco a discesa **Autenticazione**, selezionare una delle seguenti opzioni:

Autenticazione esistente

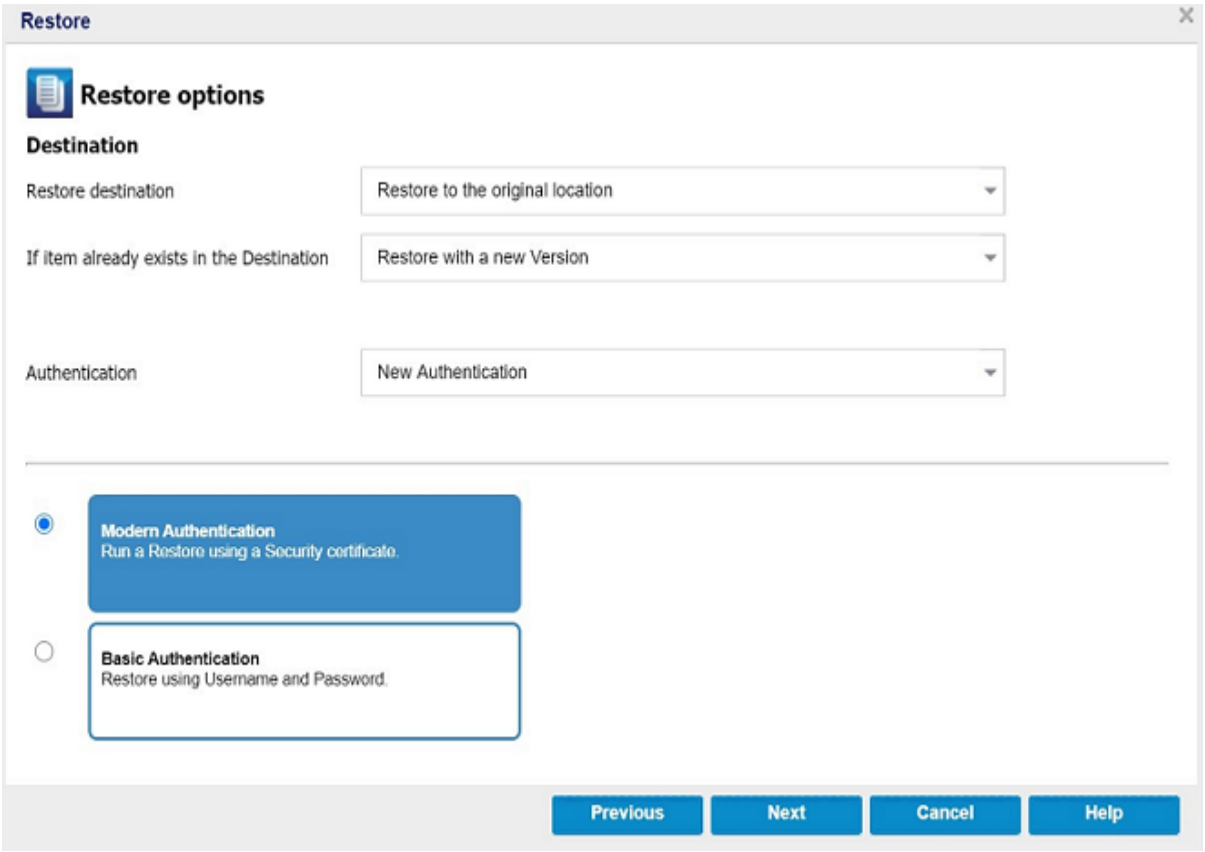
Quando si seleziona l'autenticazione esistente, viene utilizzato il tipo di autenticazione selezionato durante la creazione del nodo.

- Se l'autenticazione del nodo è di base, i parametri quali Nome utente, Password e Crittografia di backup o Password di protezione [se crittografata] vengono caricati automaticamente per procedere con il ripristino.
- Se l'autenticazione del nodo è moderna, vengono caricati automaticamente parametri quali Nome utente, Crittografia di backup o Password di protezione [se crittografata] per procedere con il ripristino.

Nuova autenticazione

Durante il ripristino, è possibile selezionare una delle seguenti opzioni per modificare il tipo di autenticazione:

- Autenticazione moderna
- Autenticazione di base



3. Per applicare la nuova autenticazione, eseguire una delle seguenti operazioni:

   Autenticazione moderna

   Per l'autenticazione moderna, è possibile eseguire un ripristino utilizzando un certificato di sicurezza.

   Effettuare le operazioni seguenti:

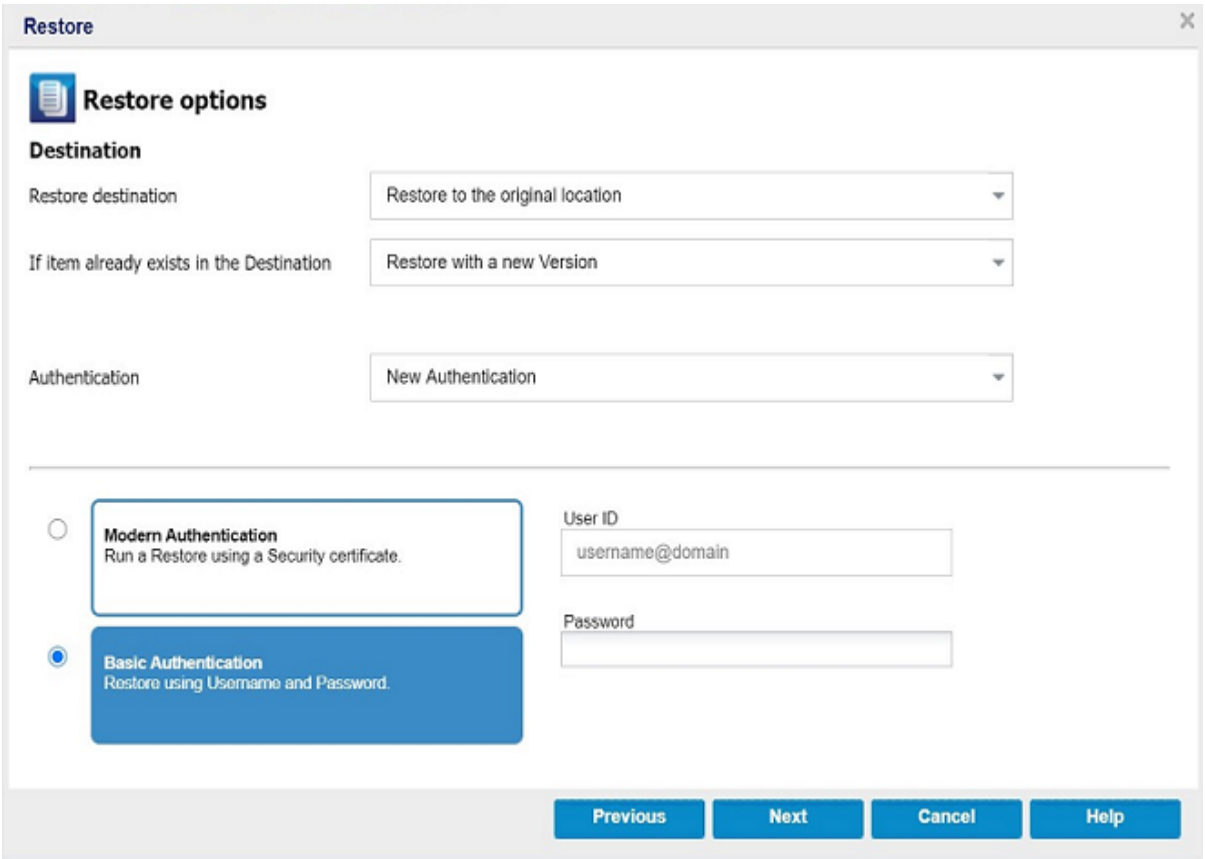
   a. Per eseguire l'autenticazione utilizzando il certificato autofirmato, consultare la sezione Download del certificato da UDP e caricamento in Azure.

   b. Immettere l'ID applicazione e il nome utente.

   c. Per applicare i ruoli e le autorizzazioni richiesti, selezionare la casella di controllo **Consentire ad Arcserve UDP di impostare i ruoli e le autorizzazioni di Azure richiesti per questa applicazione**, quindi fare clic su **Avanti**.

   Autenticazione di base

   Per l'autenticazione di base, immettere l'ID utente e la password per procedere con il ripristino.



4. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Riepilogo ripristino**.

5. Nella finestra di dialogo Riepilogo ripristino, verificare le impostazioni, quindi fare clic su **Fine**.

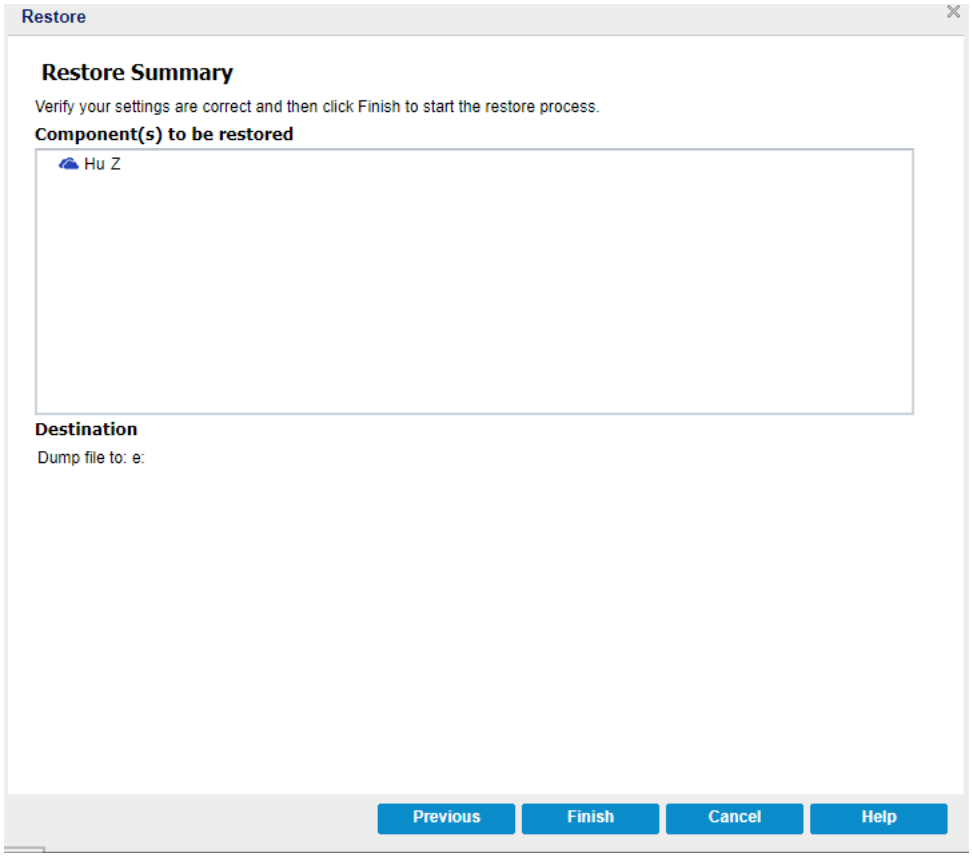
   Sono definite le opzioni di ripristino per il ripristino delle informazioni di OneDrive. A questo punto, è possibile visualizzare il riepilogo del ripristino.

Visualizzazione del riepilogo del ripristino

Una volta definite le opzioni di ripristino, verificare che le impostazioni siano corrette e confermare il processo di ripristino. **Il riepilogo del ripristino** consente di verificare tutte le opzioni di ripristino e il percorso di destinazione definito dall'utente. Se si desidera modificare le impostazioni, fare clic su **Indietro**.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Riepilogo ripristino**, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



   - Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni.
   - Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

Il contenuto del punto di ripristino viene ripristinato.

Ripristino dei dati di OneDrive mediante l'opzione di montaggio dei volumi

La protezione di OneDrive utilizza il formato della sessione di backup universale. È possibile montare la sessione di backup come lettera di unità e copiare il file o la cartella dal volume montato.

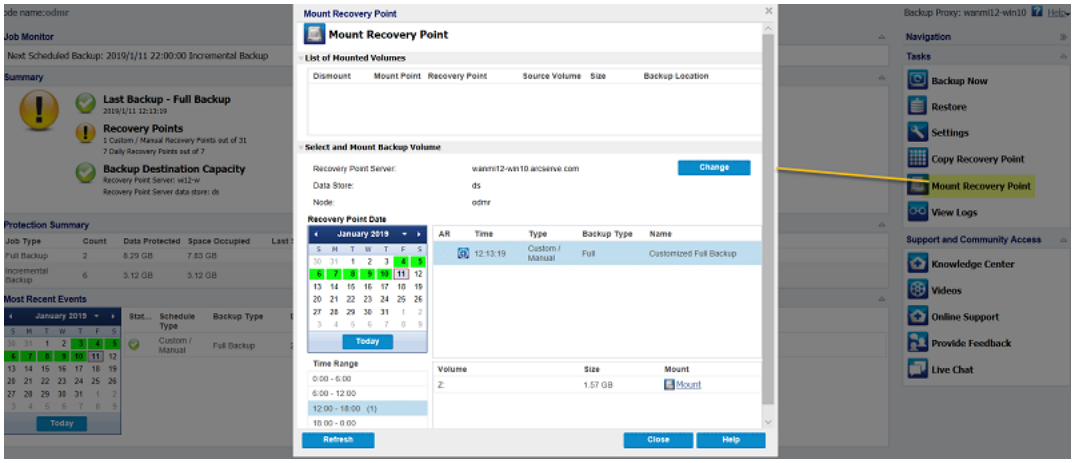
Effettuare le operazioni seguenti:

1. Accedere ad Arcserve UDP.
2. Fare clic sulla scheda **Risorse**.
3. Selezionare **Tutti i nodi** nel riquadro sinistro.

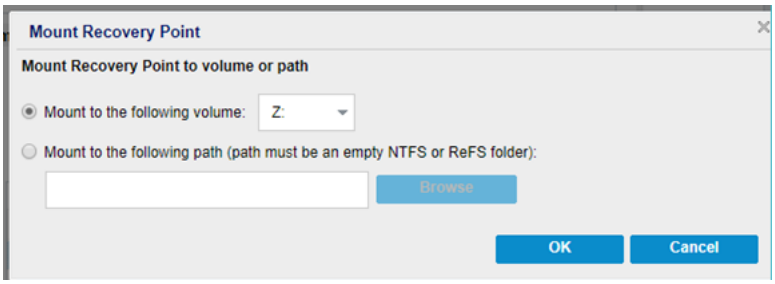
   Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.
4. Nel riquadro centrale, selezionare il nodo di OneDrive e fare clic su **Azioni**.
5. Fare clic su **Accedi all'agente** dal menu a discesa **Azioni**.

   Nota: l'accesso al nodo agente avviene automaticamente. È possibile visualizzare i dettagli completi del nodo e anche visualizzare, nel riquadro destro, l'elenco delle attività che è possibile eseguire.
6. Dal riquadro destro, in **Attività** fare clic su **Monta punto di ripristino**.

   Verrà visualizzata la finestra di dialogo **Monta punto di ripristino.** In questa finestra di dialogo è possibile selezionare la sessione di backup.



7. Selezionare la destinazione e montare la sessione come lettera di unità oppure eseguire il montaggio in una cartella NTFS vuota.



È possibile esplorare il volume. Nel volume Arcserve UDP ha salvato tutti i metadati di OneDrive. Ciascuno account disporrà di una cartella correlata sul volume principale. Il nome della cartella è basato su quello dell'account.

È possibile aprire la cartella creata in base al nome dell'account e verificare se è stato eseguito il backup dei dati di OneDrive.

Accesso al punto di ripristino della copia su nastro per il ripristino

In questa sezione vengono fornite informazioni su come selezionare un punto di ripristino dai backup di copia su nastro.

Effettuare le operazioni seguenti:

1. Scaricare i punti di ripristino utilizzando Arcserve Backup Manager e copiarli su un disco locale.
2. Dalla finestra di dialogo Ripristina, fare clic sul pulsante **Modifica**.
3. Selezionare l'opzione **Seleziona disco locale o cartella condivisa**.
4. Fare clic su **Sfoglia** per accedere alla posizione della cartella in cui vengono copiati i punti di ripristino al passaggio 1.
5. Dall'elenco dei punti di ripristino, selezionare un punto di ripristino e fare clic su **OK**.

   Il punto di ripristino selezionato viene visualizzato nella finestra di dialogo Ripristino.

Procedura di ripristino temporizzato

Il ripristino temporizzato supporta il ripristino dei database SQL in qualsiasi istante di tempo specifico tra i punti di ripristino N e N +1. Il ripristino temporizzato consente agli amministratori di ripristinare le transazioni del database SQL tra due punti di ripristino. Ad esempio, si supponga di disporre di un punto di ripristino creato il 16/03/2019 alle 12:14:04:177 e che quello successivo sia stato creato il 29/03/2019 alle 22:03:14:177. Il ripristino temporizzato consente di ripristinare le

transazioni verificatesi entro i due punti di ripristino. In tal modo, gli amministratori possono ripristinare soltanto le transazioni necessarie da dimensioni elevate di dati di backup.

Come procedere?

1. Verifica dei prerequisiti
2. Revisione delle considerazioni
3. Esecuzione del ripristino temporizzato

Prerequisiti

Verificare i prerequisiti seguenti prima di eseguire il ripristino temporizzato:

- MS SQL Database Server deve essere installato sul computer dell'agente Windows.
- È necessario disporre di almeno due punti di ripristino per eseguire il ripristino temporizzato.
- È necessario abilitare manualmente il ripristino temporizzato ogni volta.

Considerazioni

Rivedere le considerazioni seguenti prima di eseguire il ripristino temporizzato:

- È possibile eseguire il ripristino temporizzato utilizzando soltanto l'utilità della riga di comando PIT.EXE.
- È necessario disporre di due punti di ripristino collegati tra loro per eseguire il ripristino temporizzato.
- Il ripristino temporizzato supporta soltanto il backup basato sull'agente. Il backup basato sull'agente non è supportato.
- Il ripristino temporizzato supporta soltanto il ripristino sulla posizione originale. Il ripristino in una posizione alternativa e il dumping su disco non sono supportati.
- Il backup del registro della transazioni del database SQL verrà salvato nella stessa directory del file di registro SQL prima di acquisire la snapshot.
- Il primo punto di ripristino consente il ripristino a livello di database SQL. Al termine del ripristino temporizzato, il database SQL è impostato sullo stato di ripristino. È possibile eseguire il backup del punto di ripristino in modalità temporizzata disattivata.

- Per eseguire il ripristino temporizzato, è necessario selezionare un intervallo di tempo compreso tra N e N+1 punti di ripristino. Qualsiasi intervallo non incluso tra N e N+1 punti di ripristino non sarà consentito. Se l'intervallo impostato non è compreso tra N e N+1 punti di ripristino, il processo di ripristino non riesce e il database risulta danneggiato.
- L'opzione Tronca registro è disabilitata per impostazione predefinita nel backup temporizzato e nei piani di ripristino. Se tale opzione è abilitata, i registri della transazione di backup verranno troncati e nel backup temporizzato successivo mancheranno alcune transazioni.

Esecuzione del ripristino temporizzato

1. Eseguire il file **PIT.EXE**.

   L'utilità della riga di comando temporizzata apre e visualizza il prompt dei comandi PIT$.

   Per ulteriori informazioni, consultare la sezione Informazioni sull'utilità della riga di comando temporizzata.

2. Dal prompt dei comandi, eseguire **set pitbackup=1**.

   Il backup temporizzato è abilitato.

3. Dalla **Arcserve UDP**Console , eseguire un backup del database SQL.

   Viene creato il punto di ripristino N.

4. Verificare che i seguenti file vengano generati nella cartella **Catalogo**:
   - Se il nome dell'istanza di SQL Server è MSSQLSERVER (nome di istanza predefinito):
     - ***_<DatabaseName>.idx.pit***

       Contiene le dimensioni fisse di riepilogo del ripristino temporizzato.

     - ***_<DatabaseName>.cat.pit***

       Contiene una dimensione variabile dei dettagli relativi al ripristino temporizzato.

     - ***_<DatabaseName>.map.pit***

       Contiene la mappatura tra la stringa interna e l'identità della stringa interna.
   - Se il nome dell'istanza di SQL Server è diverso da MSSQLSERVER (nome di istanza diverso da quello predefinito):

- ***<SQLInstanceName>_<DatabaseName>.idx.pit***

  Contiene le dimensioni fisse di riepilogo del ripristino temporizzato.

- ***<SQLInstanceName>_<DatabaseName>.cat.pit***

  Contiene una dimensione variabile dei dettagli relativi al ripristino temporizzato.

- ***<SQLInstanceName>_<DatabaseName>.map.pit***

  Contiene la mappatura tra la stringa interna e l'identità della stringa interna.

5. Dalla **Console Arcserve UDP** , eseguire un ulteriore backup del database SQL.

   Viene creato il punto di ripristino N+1.

6. Dal prompt dei comandi, eseguire ***set pitrestore=1***.

   Il ripristino temporizzato è abilitato.

7. Dal prompt dei comandi, eseguire le query SQL sottostanti per visualizzare le informazioni sul ripristino temporizzato della sessione di backup N+1:

   - *Query <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<N+1 backup session folder name>*

     Mostra il riepilogo di tutti i ripristini temporizzati nel backup

8. Dal prompt dei comandi, eseguire ***set pittime="<MM/DD/YYYY HH:MM:SS:ss>"***

9. Dalla **Arcserve UDP**Console , eseguire il ripristino a livello di database nella posizione originale tramite il punto di ripristino N.

   Il processo di ripristino temporizzato viene completato correttamente. Verificare i dati previsti siano stati ripristinati sul database.

Informazioni sull'utilità della riga di comando temporizzata

L'utilità della riga di comando temporizzata è disponibile al percorso *<Arcserve UDP Installed path>\BIN* ed è denominata *PIT.exe*.

Il prompt dei comandi nell'utilità della riga di comando viene visualizzato come **PIT$**.

Di seguito sono riportate le opzioni disponibili che è possibile eseguire nell'utilità della riga di comando:

HELP

Visualizza tutte le opzioni disponibili in PIT.exe.

COMMAND /?

Visualizza l'utilizzo del comando.

CONFIG

Utilizza l'impostazione nel Registro di sistema.

OPTION

Specifica l'opzione globale. Il valore corrisponde sempre a un numero esadecimale.

SEQ

Specifica il numero di sequenza nel backup del database/TLog.

TIMEOUT

Specifica il timeout della connessione, in secondi.

DEVICE

Specifica il tipo di dispositivo di backup, ovvero un disco.

DATABASE

Specifica il nome del database. Immettere il valore in formato *[server]*\ *[instance]*\<*Database*>.

LOGBACKUP

Specifica il percorso di backup di TLog.

LOGRESTORE

Specifica il percorso del ripristino TLog.

DBBACKUP

Specifica il percorso di backup di TLog.

DBRESTORE

Specifica il percorso del ripristino TLog.

CATALOG

Specifica il percorso del catalogo.

STOPAT

Specifica il punto temporizzato da ripristinare.

NORECOVERY

Specifica se disabilitare (1) o abilitare (0) il ripristino automatico in seguito al ripristino del database UDP.

PITBACKUP

Specifica se disabilitare (1) o abilitare (0) il backup temporizzato per UDP.

Esempio: set pitbackup=1

PITRESTORE

Specifica se disabilitare (1) o abilitare (0) il ripristino temporizzato per UDP.

Esempio: *set pitrestore=1*

PITTEMP

Cartella temporanea per il ripristino temporizzato

PITTIME

Specifica il punto di ripristino temporizzato da ripristinare.

Esempio: set pittime="<MM/DD/YYYY HH:MM:SS:ss>

PITNOSTAGE

Specifica l'utilizzo del registro nel volume montato invece del ripristino della cartella temporanea.

BACKUPOPT

Specifica l'opzione di backup per il controllo di VSS.

RESTOREOPT

Specifica l'opzione di ripristino per il controllo di VSS.

Di seguito sono riportate le query SQL che è possibile eseguire nell'utilità della riga di comando:

- *Query <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<N+1 backup session folder name>*

  Visualizza il riepilogo di tutti i ripristini temporizzati nel backup.

- *Query /d <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<N+1 backup session folder name>*

  Visualizza tutti i dettagli di ripristino temporizzato nel backup.

- *Query /i N <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<N+1 backup session folder name>*

  Visualizza il riepilogo del punto di ripristino temporizzato di N in backup.

- *Query /d /i N <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<N+1 backup session folder name>*

  Visualizza i dettagli di ripristino temporizzato di N nel backup.

Ripristino del volume cluster condiviso

Ogni volta che Arcserve UDP esegue correttamente un backup, viene creata un'immagine di snapshot temporizzata del backup (punto di ripristino). L'insieme dei punti di ripristino consente di individuare e specificare esattamente le immagini di backup da ripristinare. Se in un momento successivo si ritiene che le informazioni di backup siano mancanti, corrotte o non affidabili, è possibile individuare ed eseguire il ripristino da una versione precedente attendibile.

Come procedere?

1. Verifica dei prerequisiti e delle considerazioni
2. Definizione delle informazioni CSV per il ripristino
   a. Definizione di CSV e del contenuto da ripristinare
   b. Definizione delle opzioni di ripristino
3. Ripristino del contenuto CSV

Verifica dei prerequisiti e delle considerazioni

Verificare i seguenti prerequisiti prima di procedere al ripristino:

- È necessario disporre di almeno un punto di ripristino per il ripristino.
- È necessario disporre di una destinazione valida e accessibile da cui eseguire il ripristino del contenuto del punto di ripristino.
- È necessario disporre di una posizione di destinazione valida e accessibile dove eseguire il ripristino del punto di ripristino.
- Riesaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Verificare le seguenti considerazioni sul ripristino:

- Se il ripristino viene eseguito su una destinazione remota e tutte le unità (A - Z) sono occupate, non sarà possibile eseguire il ripristino su posizione remota. Arcserve UDPL'agente (Windows) deve utilizzare una lettera di unità per eseguire il montaggio del percorso di destinazione remoto.
- (Facoltativo) Comprendere il funzionamento del processo di ripristino. Per ulteriori informazioni, consultare la sezione Funzionamento del ripristino a livello di file.
- (Facoltativo) Rivedere i file ignorati durante il ripristino. Per ulteriori informazioni, consultare la sezione File ignorati durante il ripristino.

- Quando si esegue il ripristino di una sessione di backup ottimizzata su un volume non vuoto (ripristino non ottimizzato), il processo di ripristino potrebbe richiedere più tempo del tempo previsto visualizzato nel monitoraggio dei processi. La quantità di dati elaborata e il tempo trascorso potrebbero aumentare in base ai dati ottimizzati sul volume.

Esempio:

La dimensione del volume di backup è 100 GB. In seguito all'ottimizzazione, la dimensione del volume viene ridotta a 50 GB.

Quando si esegue un ripristino non ottimizzato del volume, il monitoraggio del processo di ripristino mostra 100% dopo aver ripristinato 50 GB. Sarà tuttavia necessario più tempo per eseguire il ripristino dei 50 GB restanti.

- Il messaggio seguente del Registro attività viene visualizzato quando si ripristinano i file di sistema:

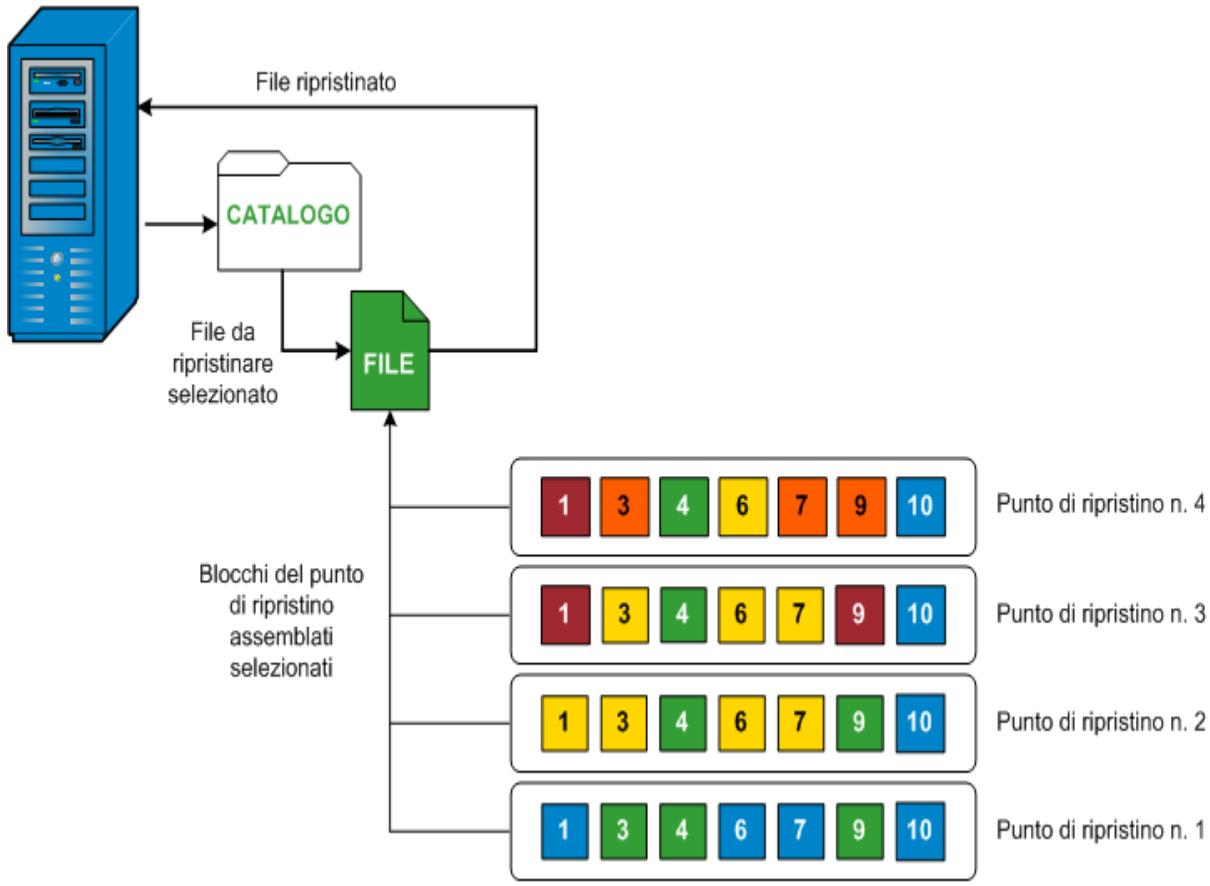
  I file di sistema sono stati ignorati. Se necessario, è possibile utilizzare l'opzione di ripristino bare metal per eseguire il ripristino.

Funzionamento del ripristino a livello di file

Durante il processo di backup a livello di blocco, ciascun file di backup include un insieme di blocchi che definiscono tale file. Il file di catalogo creato contiene un elenco dei file di backup, i singoli blocchi utilizzati per ciascun file e i punti di ripristino disponibili per tali file. Nel caso in cui sia necessario ripristinare un file specifico, è possibile individuare il file che si desidera ripristinare e il punto di ripristino che si desidera utilizzare. Arcserve UDP esegue la raccolta della versione dei blocchi utilizzati per il punto di ripristino del file specificato, li riassembla ed esegue il ripristino del file.

Nota: è inoltre possibile eseguire un ripristino senza un file di catalogo da un punto di ripristino di backup senza catalogo.

Nel seguente diagramma di flusso è possibile visualizzare il processo di ripristino di un file specifico di Arcserve UDP:



File ignorati durante il ripristino

Durante un ripristino con l'agente Arcserve UDP (Windows), è possibile che alcuni file vengano ignorati intenzionalmente.

I file e le cartelle nella tabella seguente vengono ignorati durante il ripristino se si verificano le due condizioni seguenti:

- I file vengono ignorati se esistono prima del ripristino e l'opzione di conflitto è Ignora file esistenti.
- I file e le cartelle elencati nella tabella seguente vengono ignorati poiché non costituiscono un componente importante di Windows o dell'agente Arcserve UDP (Windows).

Sistema operativo	Cartella o posizione	Nome di file o cartella	Note

Tutto	Cartella root di ciascun volume	CAVolTrc.dat	Utilizzato dal driver di rilevamento di Arcserve UDP.
		cavoltrcsnapshot.dat	
		System Volume Information*	Utilizzato per salvare file/cartelle con un sistema Windows, ad esempio file di copia shadow del volume.
		RECYCLER*	Utilizzato solamente su partizioni NTFS. Contiene un cestino per ogni utente che accede al computer, ordinato in base al rispettivo ID di sicurezza (SID).
		$Recycle.Bin*	Quando si elimina un file da Gestione risorse o da Risorse del computer, il file viene archiviato nel cestino finché non si svuota il cestino o si ripristina il file.
	Qualsiasi cartella con file di immagini	Thumbs.db	Archivia le immagini di anteprima per la visualizzazione Anteprima di Esplora risorse.
	Cartella root del volume	PageFile.Sys	File di scambio per la memoria virtuale di Windows.
		Hiberfil.sys	File per l'ibernazione usato per salvare i dati di sistema quando si attiva la modalità di ibernazione.

I file e le cartelle seguenti vengono ignorati soltanto quando si esegue il ripristino nella posizione originale o in una posizione alternativa:

Sistema operativo	Cartella o posizione	Nome di file o cartella	Nota
Tutto	Cartella specificata nel record di valore in: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Tutti i file/cartelle (in modo ricorsivo)	La cartella contiene un file .dll memorizzato nella cache che viene utilizzato per il controllo dei file di sistema (SFC). I contenuti della

			directory di cache dll di sistema vengono ricostruiti mediante SFC.
	%SystemRoot%\SYSTEM32\dllCache		
	Cartella principale di quorum_device	MSCS*	Utilizzato per Microsoft Cluster Server.
	%SystemRoot%\SYSTEM32\	perf?00?.dat	Dati relativi alle prestazioni utilizzati dal contatore delle prestazioni di Windows.
		perf?00?.bak	Utilizzato per le firme digitali dei record Protezione file Windows (WFP) installati nel sistema operativo (ad esempio DLL, EXE, SYS, OCX e così via) per evitare che siano eliminati o sostituiti con versioni precedenti.
		CATROOT*	

	%SystemRoot%\inetsrv\	metabase.bin	File binario metabase delle versioni di IIS precedenti alla 6.0.
	File o cartella specificato nel valore eccetto l'Archivio comune SIS in HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup	Tutti i file/cartelle (in modo ricorsivo)	I file e le cartelle non devono essere sottoposti a backup e ripristino. Per ulteriori informazioni, fare clic sul seguente collegamento.
XP W2003	Volume di sistema	NTLDR	Caricatore di avvio principale.
		BOOT.INI	Contiene la configurazione di avvio (se assente, il valore predefinito NTLDR sarà impostato su \Windows nella prima par-

			tizione del primo disco rigido).
		NTDETECT.COM	Richiesto per l'avvio del sistema operativo basato su NT. Rileva le informazioni hardware di base necessarie per il corretto avvio.
Vista e sistemi successivi	Cartella root del volume di sistema	boot*	Cartella di avvio per Windows.
		bootmgr	File di Windows Boot Manager.
		EFI\Microsoft\Boot*	Usata per l'avvio EFI.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Archivia i file di traccia ETW (estensione .etl) per le sessioni di traccia degli eventi in tempo reale.
		config\RegBack*	Backup della tabella

			del registro di sistema attuale.
Win8 e sistemi successivi	Volume di sistema	swapfile.sys	File del controller di sistema, in genere di circa 256 MB. Viene utilizzato da applicazioni come Metro che non si adattano alle caratteristiche di paging tradizionali (schema di utilizzo, crescita, spazio riservato) di pagefile.sys.
		BOOTNXT	Utilizzato per l'avvio da un sistema operativo diverso da Windows 8. Creato durante l'abilitazione delle opzioni di

			avvio e aggior-nato da Windows.

Il Registro attività fornisce le seguenti informazioni:

- Informazioni di data e ora: File system jobxxxx ignorati. È possibile utilizzare l'opzione Ripristino bare metal (BMR) per ripristinarli.
- Informazioni di data e ora: File o directory jobxxxx ignorati. L'elenco dei file o delle directory ignorati è disponibile in: C:\Programmi\Arcserve\Unified Data Protection\Engine\Logs\Restore-<YYYYMMDD>-<hhmmss>-<Process ID>-<Job ID>.log.

Definizione delle informazioni CSV per il ripristino

Arcserve UDP include un'opzione per il ripristino dei dati da un punto di ripristino. L'obiettivo di un processo di ripristino è quello di identificare rapidamente i dati necessari e di recuperarli dalla posizione di backup appropriata. Per ciascun processo di ripristino è richiesta un'origine e una destinazione.

Come procedere?

1. Definizione di CSV e del contenuto da ripristinare
2. Definizione delle opzioni di ripristino

Definizione di CSV e del contenuto da ripristinare

Utilizzare l'opzione **Sfoglia punti di ripristino** per eseguire il ripristino da un punto di ripristino. Quando si seleziona una data di ripristino e poi l'ora, vengono visualizzati tutti i punti di ripristino associati per tale durata. È possibile individuare e selezionare i contenuti di backup (applicazioni incluse) da ripristinare.

Effettuare le operazioni seguenti:

1. Accedere alla finestra di dialogo per la selezione del metodo di ripristino in uno dei modi seguenti:

   Dalla console Arcserve UDP:

   a. Accedere ad **Arcserve UDP**.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

Nota: Viene effettuato automaticamente l'accesso al nodo agente e la finestra di dialogo per la selezione del metodo di ripristino viene visualizzata dal nodo agente.

Dall'agente Arcserve UDP (Windows):

a. Accedere all'agente Arcserve UDP (Windows).

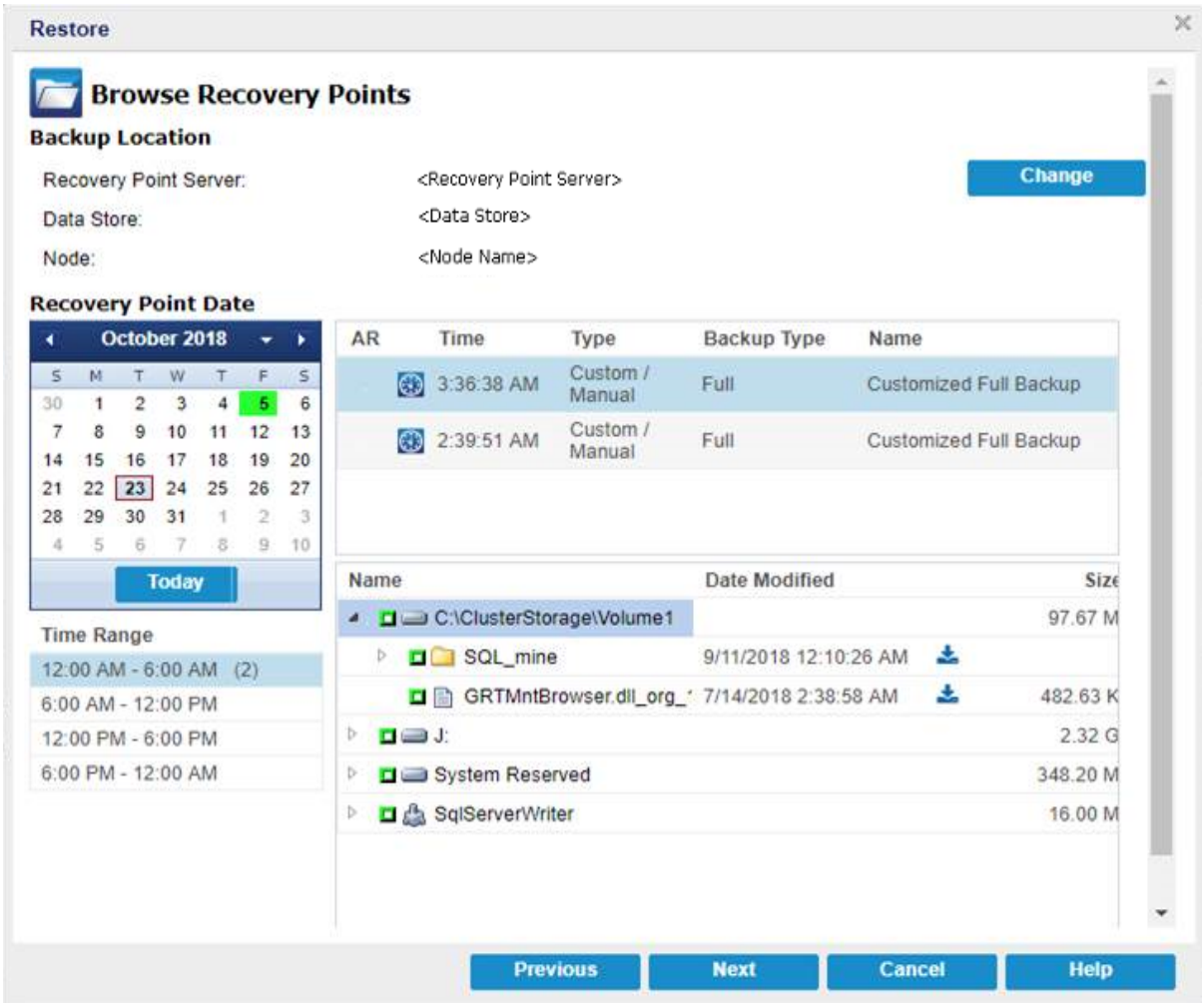
b. Dalla pagina principale selezionare **Ripristino**.

Viene visualizzata la finestra di dialogo per la selezione del metodo di ripristino.

2. Fare clic sull'opzione **Sfoglia punti di ripristino**.

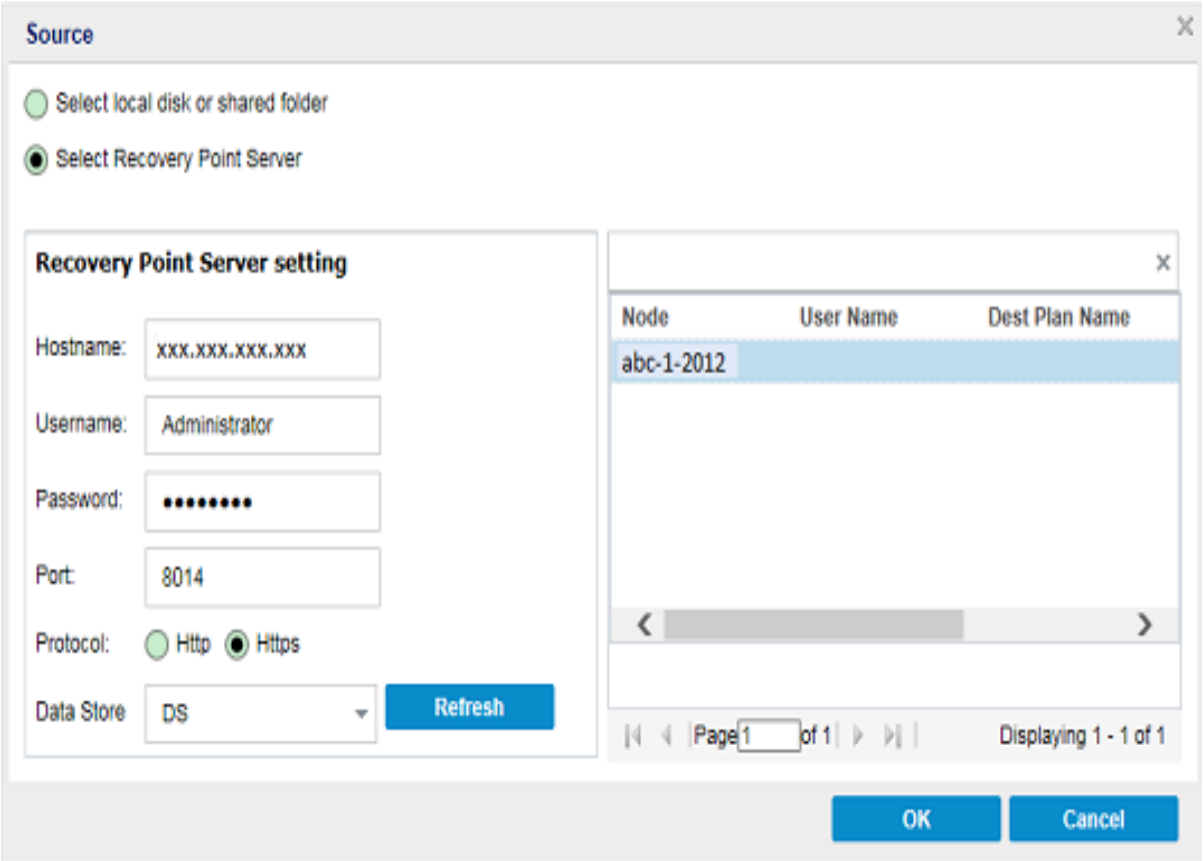
Verrà visualizzata la finestra di dialogo **Sfoglia punti di ripristino**. È possibile visualizzare i dettagli del **Recovery Point Server** in **Posizione di backup**.

AR indica il risultato dell'esecuzione se è stato eseguito Assured Recovery per la sessione.



3. Fare clic su **Modifica** per aggiornare la posizione di backup.

   Viene visualizzata la finestra di dialogo **Origine** in cui è possibile selezionare la posizione di backup.



4. Selezionare una delle origini seguenti:

   Selezione di un disco locale o una cartella condivisa

   a. Specificare o accedere al percorso di archiviazione delle immagini di backup e selezionare l'origine di backup appropriata.

      Per verificare la connessione al percorso specificato, fare clic sulla freccia verde. Se necessario, immettere le credenziali **Nome utente** e **Password** per poter accedere alla posizione di origine.

      Viene visualizzata la finestra di dialogo **Selezionare la posizione di backup**.

   b. Selezionare la cartella di archiviazione dei punti di ripristino e fare clic su **OK**.

      La finestra di dialogo **Selezionare la posizione di backup viene chiusa** e la posizione di backup viene visualizzata nella finestra di dialogo **Origine**.

   c. Fare clic su **OK**.

      I punti di ripristino vengono elencati nella finestra di dialogo **Sfoglia punti di ripristino**.

      Selezione di un Recovery Point Server

d. Specificare i dettagli dell'impostazione Recovery Point Server e fare clic su **Aggiorna**.

   Tutti gli agenti vengono elencati nella colonna Data Protection Agent (Agente di protezione dati) nella finestra di dialogo Origine.

e. Selezionare l'agente dall'elenco visualizzato e fare clic su **OK**.

   I punti di ripristino vengono elencati nella finestra di dialogo **Sfoglia punti di ripristino**.

5. Selezionare la data dell'immagine di backup che si desidera ripristinare.

   Tutte le date contenenti punti di ripristino per l'origine di backup specificata sono evidenziate in verde.

   Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito (completo, incrementale o di verifica) e al nome del backup.

6. Selezionare un punto di ripristino da ripristinare.

   Viene visualizzato il contenuto di backup (incluse tutte le applicazioni) per i punti di ripristino selezionati.

   Nota: l'icona di un orologio con lucchetto indica che il punto di ripristino contiene informazioni crittografate e potrebbe richiedere una password per il ripristino.

7. Selezionare il volume CSV da ripristinare.

   - Per un ripristino a livello di volume, è possibile scegliere di ripristinare l'intero volume oppure alcuni file/cartelle specifici.
   - Per un ripristino a livello di applicazione, è possibile scegliere di ripristinare l'intera applicazione o solo determinati componenti, database, istanze, ecc. dell'applicazione.

8. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Opzioni di ripristino**.

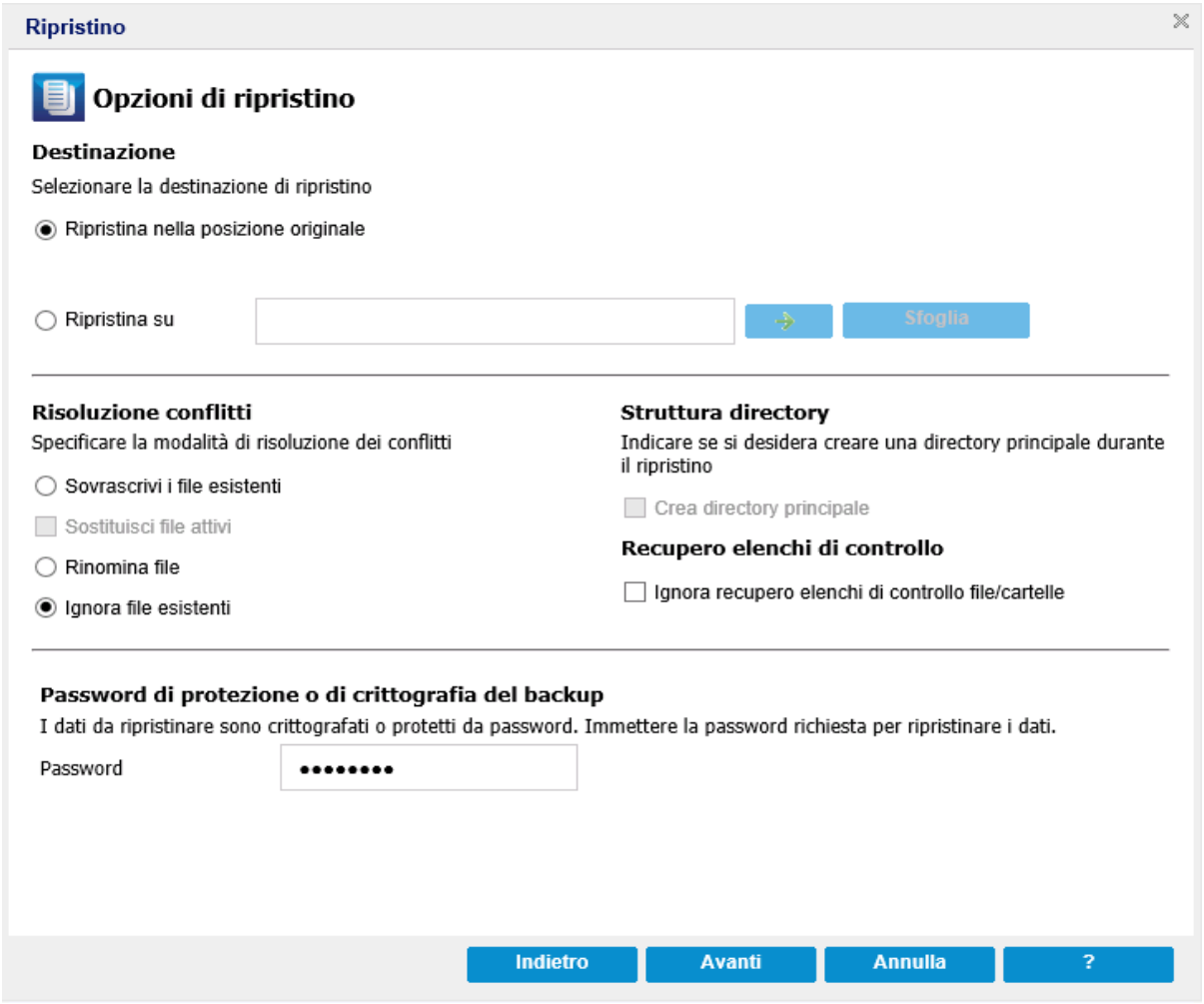
   Il punto di ripristino e il contenuto da ripristinare sono specificati.

Definizione delle opzioni di ripristino

Dopo avere specificato un punto di ripristino e il contenuto da ripristinare, definire le opzioni di copia per il punto di ripristino selezionato.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Opzioni di ripristino**, selezionare la destinazione di ripristino.



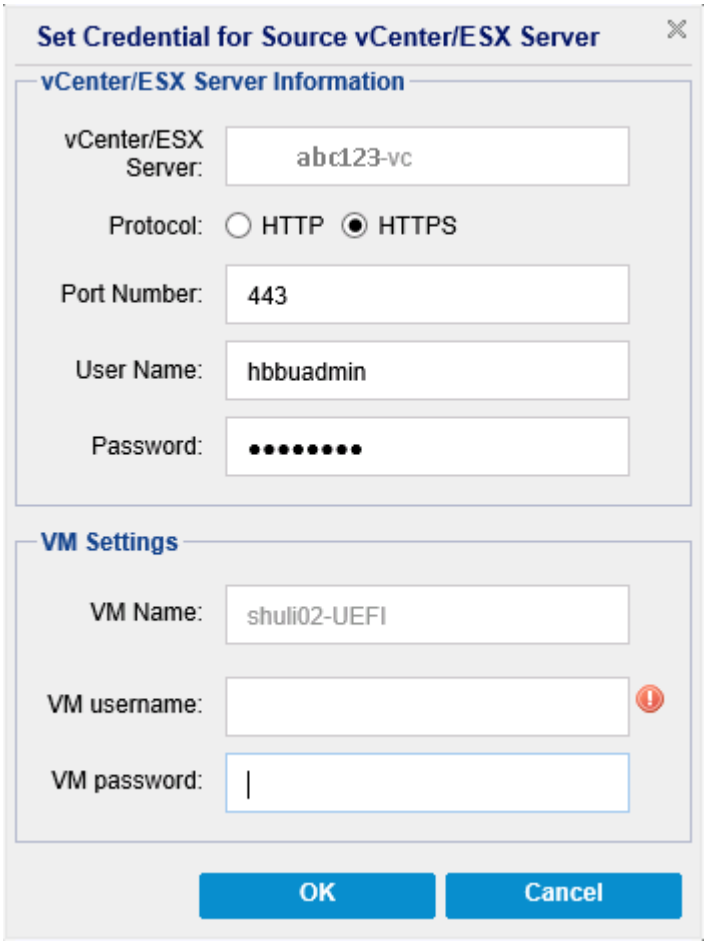
Le opzioni di destinazione disponibili sono:

Ripristina in posizione originale

Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

Nota: se è stato eseguito il backup del punto di ripristino tramite il backup senza agente basato su host, per eseguire il ripristino sulla posizione originale sarà necessario eseguire nuovamente il ripristino sul computer virtuale. In questo caso, viene visualizzata una finestra di dialogo. È possibile immettere le credenziali dell'hypervisor e il sistema operativo del computer virtuale.

Valido per il computer virtuale VMware:



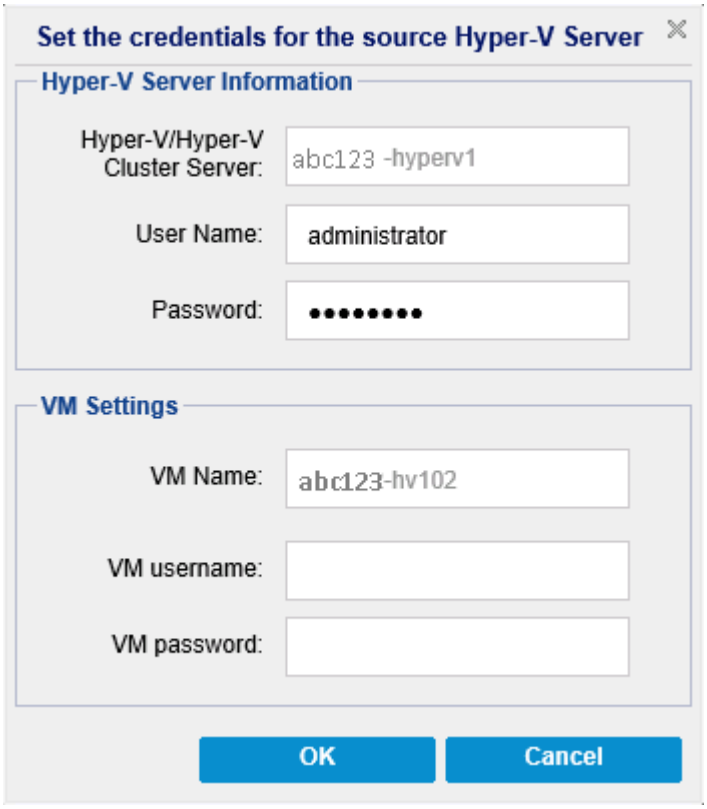
Nota: per poter creare o scrivere i file all'interno del computer virtuale, prendere in considerazione i seguenti requisiti per le impostazioni e l'autorizzazione di account del computer virtuale:

- Gli strumenti VMware vengono installati e sono in esecuzione.
- Il firewall deve consentire la condivisione di file e stampanti.
- L'account può appartenere all'amministratore locale integrato, all'amministratore di dominio integrato o al dominio appartenente al gruppo degli amministratori locali. Se vengono utilizzati altri account:
  - Disabilitare l'accesso remoto a UAC. Per disabilitare l'accesso UAC remoto, consultare la sezione Importazione di computer virtuali con un account amministrativo aggiuntivo.
  - Disabilitare l'UAC nel Local Security Policy disattivando l'impostazione di esecuzione di tutti gli amministratori nella modalità di approvazione dell'amministratore in secpol.msc -

> Criteri locali -> Opzioni di protezione. (Secpol.msc è l'editor delle policy di protezione di Microsoft).

Importante: non disabilitare l'UAC nella finestra di dialogo Impostazioni di Controllo account utente accessibile dal pannello di controllo.

Per il computer virtuale Hyper-V:



Nota: per poter creare o scrivere i file all'interno del computer virtuale, prendere in considerazione i seguenti requisiti per le impostazioni e l'autorizzazione di account del computer virtuale:

- I servizi di integrazione Hyper-V devono essere installati e in esecuzione.
- Il firewall deve consentire la condivisione di file e stampanti.
- L'account può appartenere all'amministratore locale integrato, all'amministratore di dominio integrato o al dominio appartenente al gruppo degli amministratori locali. Se vengono utilizzati altri account:

Disabilitare l'accesso remoto a UAC. Per disabilitare l'accesso UAC remoto, consultare la sezione Importazione di computer virtuali con un account amministrativo aggiuntivo.

- Se il sistema operativo guest del computer virtuale è Windows versione Client (ad esempio, Windows 10), è necessario configurare manualmente il firewall per consentire Windows Management Instrumentation (WMI).

Ripristina su

Esegue il ripristino alla posizione specificata. Per verificare la connessione al percorso specificato, fare clic sulla freccia verde. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso.

2. Specificare l'opzione **Risoluzione conflitti** che verrà eseguita da Arcserve UDP in caso di conflitti durante il processo di ripristino.

   Le opzioni disponibili sono:

   Sovrascrivi i file esistenti

   Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dai file di backup, indipendentemente dalla loro presenza sul computer.

   Sostituisci file attivi

   Consente di sostituire i file attivi dopo il riavvio. Se durante il tentativo di ripristino l'agente Arcserve UDP (Windows) rileva che il file esistente è attualmente in uso, tale file non verrà immediatamente sostituito, ma, per evitare l'insorgere di problemi, la sostituzione dei file attivi avverrà con il riavvio successivo del computer. Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita al riavvio successivo.

   Questa opzione è disponibile solo se l'opzione **Sovrascrivi i file esistenti** è stata selezionata.

   Nota: se l'opzione non è selezionata, tutti i file attivi verranno ignorati durante il processo di ripristino.

   Rinomina file

   Se il nome file esiste già, consente di creare un nuovo file. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno quindi ripristinati nel nuovo file.

   Ignora file esistenti

Ignora e non sovrascrive (sostituisce) i file esistenti contenuti nella destinazione di ripristino. Solo gli oggetti inesistenti sul computer verranno ripristinati dai file di backup.

Impostazione predefinita: Ignora file esistenti.

3. Specificare la **struttura di directory** per creare una directory principale durante il ripristino.

Crea directory principale

Se l'immagine di backup acquisita contiene una struttura delle directory principali, Arcserve UDP ricrea la stessa struttura della directory principale nel percorso di destinazione di ripristino.

Se questa opzione non viene selezionata, il file o cartella verrà ripristinato direttamente nella cartella di destinazione.

Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt e C:\Folder1\SubFolder2\B.txt e durante il ripristino è stata specificata la destinazione D:\Restore.

- Se si sceglie di ripristinare i file A.txt e B.txt individualmente, la destinazione dei file ripristinati corrisponderà a D:\Restore\A.txt e D:\Restore\B.txt. La directory principale sopra il livello di file specificato non verrà ricreata.
- Se si sceglie di eseguire il ripristino a partire dal livello SubFolder2, la destinazione dei file ripristinati corrisponderà a D:\Restore\SubFolder2\A.txt e D:\Restore\SubFolder2\B.txt. La directory principale al di sopra del livello di cartella specificato non verrà ricreata.

Se questa opzione è selezionata, verrà ricreato l'intero percorso della directory principale per i file o le cartelle (compreso il nome del volume) nella cartella di destinazione. Se i file o le cartelle da ripristinare appartengono allo stesso nome del volume, il percorso della directory principale di destinazione non includerà tale nome del volume. Tuttavia, se i file o le cartelle da ripristinare appartengono a diversi nomi di volume, il percorso della directory principale di destinazione includerà il nome del volume.

Ad esempio, se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt, C:\Folder1\SubFolder2\B.txt e E:\Folder3\SubFolder4\C.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

- Se si desidera ripristinare soltanto il file A.txt, la destinazione del file ripristinato corrisponderà a D:\Restore\ Folder1\SubFolder2\A.txt (verrà ricreata l'intera directory principale, eccetto il nome del volume).

- Se si esegue il ripristino di entrambi i file A.txt e B.txt, la destinazione dei file ripristinati corrisponderà a D:\Restore\C\Folder1\SubFolder2\A.txt e D:\Restore\E\Folder3\SubFolder4\C.txt (verrà ricreata l'intera directory principale, compreso il nome del volume).

4. Da **Recupero elenchi di controllo**, selezionare l'opzione **Ignora recupero elenchi di controllo file/cartelle** per ignorare l'autorizzazione originale per i file o le cartelle ripristinati. Selezionando questa opzione vengono ereditate le autorizzazioni della cartella di destinazione. In caso contrario, vengono conservate le autorizzazioni originali.
5. Se necessario, specificare la **Password di crittografia di backup** nel caso in cui i dati che si desidera ripristinare siano crittografati.

   Se il ripristino viene eseguito dallo stesso computer dell'agente Arcserve UDP (Windows) da cui è stato eseguito il backup crittografato, non è necessario specificare una password. Tuttavia, la password verrà richiesta quando il ripristino viene eseguito da un computer dell'agente Arcserve UDP (Windows) diverso.

   Nota: l'icona di un orologio con lucchetto indica che il punto di ripristino contiene informazioni crittografate e potrebbe richiedere una password per il ripristino.
6. Fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Riepilogo ripristino**.

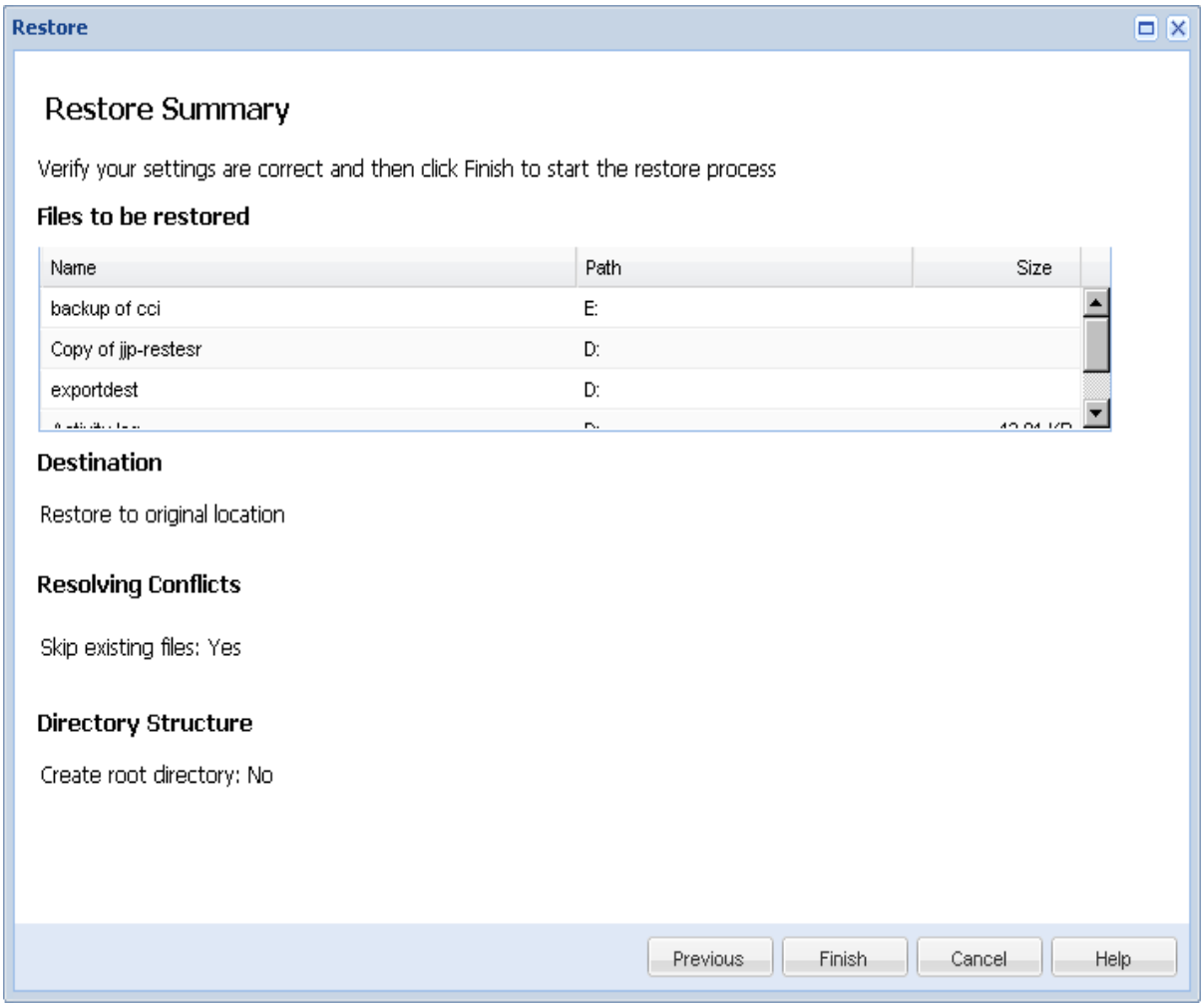
   Le opzioni di ripristino vengono definite per il ripristino da un punto di ripristino.

Ripristino del contenuto CSV

Una volta definite le opzioni di ripristino, verificare che le impostazioni siano corrette e confermare il processo di ripristino. Il **riepilogo di ripristino** consente di verificare tutte le opzioni di ripristino definite e, se necessario, modificarle.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo **Riepilogo ripristino**, controllare le informazioni visualizzate per verificare che tutte le opzioni e le impostazioni di ripristino siano corrette.



- Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
- Se le informazioni di riepilogo sono corrette, fare clic su **Fine** per avviare il processo di ripristino.

Il contenuto del punto di ripristino viene ripristinato.

Chapter 2: Gestione del backup e del ripristino su nastro

Arcserve UDP consente di eseguire il backup dei dati su un nastro e il ripristino dei dati sottoposti a backup dal nastro a un nodo.

La presente sezione descrive i seguenti argomenti:

Backup di un archivio dati di deduplicazione su un nastro

Per eseguire il backup di un archivio dati di deduplicazione su un nastro, utilizzare i metodi seguenti:

- Eseguire il backup dei nodi UDP su nastro. Per ulteriori informazioni, consultare la sezione Metodo 1: Backup della sessione di backup UDP più recente su nastro nella Guida all'amministrazione di Arcserve Backup.
- Backup dei dati Arcserve UDP dagli archivi dati. Per ulteriori informazioni, consultare la sezione Metodo 2: Backup dei dati Arcserve UDP dagli archivi dati nella Guida all'amministrazione di Arcserve Backup.

Ripristino di un archivio dati di deduplicazione da un nastro

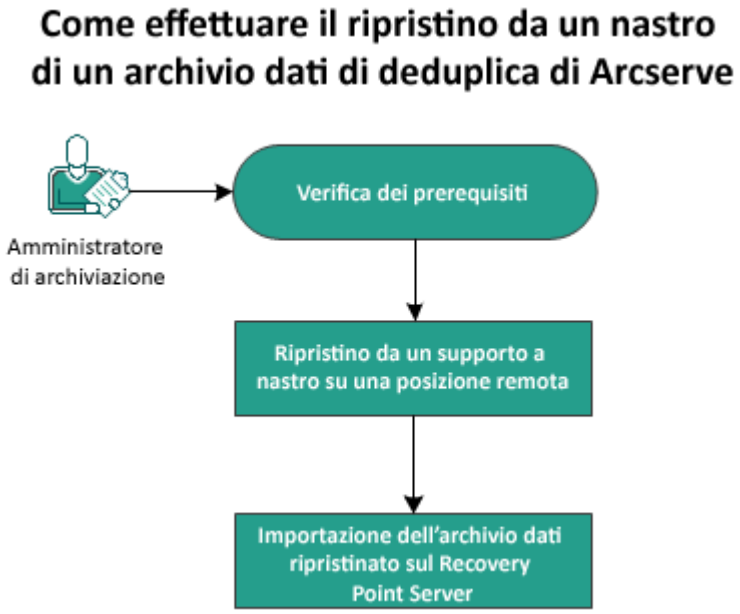
Se in precedenza è stato eseguito il backup di un archivio dati di deduplicazione da un Recovery Point Server (RPS) su una periferica nastro, è possibile ripristinare l'archivio dati. Per questa procedura, Arcserve Backup e Arcserve UDP vengono utilizzati contemporaneamente per ripristinare un archivio dati di deduplicazione da un nastro. Arcserve Backup consente il ripristino dal nastro su una destinazione specifica, mentre Arcserve UDP permette l'importazione in un server RPS.

Nella procedura di ripristino sono coinvolti i due processi seguenti:

1. Nel primo processo viene utilizzato Arcserve Backup per ripristinare le sessioni dal supporto nastro su un volume. Si consiglia di ripristinare le sessioni in una posizione alternativa.
2. Nel secondo processo viene utilizzato Arcserve UDP per importare l'archivio dati ripristinato sul server RPS.

   Nota: per la ricerca del percorso durante l'importazione, sarà necessario specificare il percorso della **cartella di destinazione del backup** dell'archivio dati di deduplicazione.

   Il diagramma seguente illustra la procedura di ripristino di un archivio dati di deduplicazione Arcserve da un nastro:



Come procedere?

1. Verifica dei prerequisiti
2. Ripristino da un supporto nastro su una posizione alternativa
3. Importazione dell'archivio dati ripristinato sul server RPS

Verifica dei prerequisiti

Verificare i prerequisiti seguenti prima di avviare il ripristino:

- Deve essere stato eseguito il backup di un archivio dati RPS sul nastro.
- Se necessario, immettere la password di sessione.
- Sarà necessario inserire il nome utente e la password della destinazione di ripristino.

Ripristino da un supporto nastro su una posizione alternativa

Per ripristinare la sessione dal supporto nastro su una posizione alternativa, sarà necessario utilizzare la gestione di Arcserve Backup.

Al completamento del ripristino, sarà possibile importare l'archivio dati ripristinato sul server RPS mediante Arcserve UDP.

Effettuare le operazioni seguenti:

1. Da Arcserve Backup, accedere alla Gestione di Arcserve Backup.
2. Dal riquadro di navigazione **Avvio rapido**, fare clic su **Ripristino** e dal riquadro centrale, selezionare la scheda **Origine**.
3. Dal menu a discesa, selezionare **Ripristino per sessione** e selezionare la sessione che si desidera ripristinare.
4. Fare clic sulla scheda **Destinazione**.
5. Cancellare (deselezionare) la casella di controllo **Ripristina i file nella posizione di origine**.
6. Espandere **Sistemi Windows** e andare alla posizione su cui si desidera effettuare il ripristino.
7. Fare clic sulla scheda **Pianificazione** e selezionare **Once** (Una volta) per l'opzione **Metodo ripetizione**.
8. Fare clic su **Invia**.

   Viene aperta la finestra di dialogo **Supporto di ripristino**.
9. Verificare il supporto di ripristino e fare clic su **OK**.

   Viene aperta la finestra di dialogo **Nome utente e password sessione.**
10. Se necessario, inserire il nome utente e la password della posizione di ripristino e la password di sessione dei punti di ripristino.
11. Fare clic su **OK**.

    Viene visualizzata la finestra di dialogo **Inoltra processo**.
12. Inserire le informazioni richieste nella finestra di dialogo **Inoltra processo** e fare clic su **OK**.

    Il processo di ripristino viene inoltrato.

    Al completamento del processo di ripristino, i file dell'archivio dati di Arcserve UDP verranno visualizzati nella posizione specificata.

Importazione dell'archivio dati ripristinato sul server RPS

Per importare l'archivio dati ripristinato sul server RPS, è necessario utilizzare la Console Arcserve UDP. La funzionalità **Importa archivio dati** consente di aggiungere un archivio dati al Recovery Point Server. È possibile importare in un Recovery Point Server qualsiasi archivio dati esistente.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Viene visualizzata la pagina **Destinazioni: Recovery Point Server**.
3. Eseguire una delle seguenti operazioni:
   - Fare clic su un Recovery Point Server.
   - Selezionare un Recovery Point Server e dal menu centrale fare clic sul menu a discesa **Azioni**.
4. Fare clic su **Importa archivio dati**.

   Viene visualizzata la pagina **Importa archivio dati**.
5. Selezionare le opzioni seguenti e fare clic su **Avanti**:
   a. Fare clic su **Sfoglia** e selezionare la **Cartella di destinazione del backup** da cui si desidera importare l'archivio dati.
   b. Se necessario, immettere la **password di crittografia**.

      Note: se l'archivio dati non è crittografato, è possibile lasciare vuoto questo campo.

   Dopo avere autenticato la **Cartella di destinazione del backup**, la pagina **Importa archivio dati** mostra i dettagli dell'archivio dati.

   Nota: l'importazione dell'archivio dati ripristinato non è supportata se l'archivio dati originale è presente nello stesso server RPS. È necessario eliminare l'archivio dati originale prima di importare l'archivio dati ripristinato, oppure è necessario importare l'archivio dati in un altro server RPS.
6. Se necessario, modificare i dettagli dell'archivio dati e fare clic su **Salva**.

   Al termine dell'importazione dell'archivio dati ripristinato, Arcserve UDP continuerà a leggere le destinazioni di indice, hash e dati dalle impostazioni di configurazione dell'archivio dati e mostrerà i percorsi effettivi in cui si trovava

originariamente l'archivio dati. Al completamento dell'importazione, queste destinazioni di percorso devono essere sostituite con i nuovi percorsi ripristinati.

Nota: Non è possibile abilitare o disabilitare l'opzione di crittografia per un archivio dati esistente.

L'archivio dati viene aggiunto al Recovery Point Server e visualizzato nella finestra di dialogo **Destinazioni: Recovery Point Server**.

Al termine dell'importazione, accanto al nome dell'archivio dati corrispondente viene visualizzato un segno di spunta verde.

L'archivio dati di deduplicazione è stato ripristinato correttamente da un nastro.

Chapter 3: Utilizzo dell'interfaccia PowerShell

La presente sezione descrive i seguenti argomenti:

Utilizzo dell'interfaccia PowerShell

Arcserve UDP offre le funzionalità di PowerShell che consentono di inoltrare un processo di backup, eseguire un ripristino e ripristinare il computer virtuale dalla riga di comando. L'interfaccia PowerShell è denominata UDPPowerCLI.ps1.

Revisione del prerequisito

Prima di utilizzare l'interfaccia PowerShell, rivedere i seguenti prerequisiti:

- È necessario disporre di Windows 2008 R2 Server o versioni successive.
- È necessario avere installato PowerShell 3 o versioni successive sul server.

Utilizzo dell'interfaccia PowerShell per Arcserve UDP

L'utilità PowerShell è fornita in bundle con il file di installazione di Arcserve UDP.

Quando si installa Arcserve UDP, in genere il file viene installato nella posizione seguente:

C:\Programmi\Arcserve\Unified Data Protection

In tali casi, nella Console viene installato UDPPowerCLI.ps1 nella posizione seguente:

C:\Programmi\Arcserve\Unified Data Protection\Management\PowerCLI

Sul server RPS o sull'agente, UDPPowerCLI.ps1 viene installato nella posizione seguente:

C:\Programmi\Arcserve\Unified Data Protection\Engine\PowerCLI

Consultare le opzioni seguenti per utilizzare l'interfaccia PowerShell:

- Aggiornare il criterio di esecuzione di PowerShell per consentire l'esecuzione degli script. Ad esempio, aggiornare il criterio di esecuzione a **Set-ExecutionPolicy RemoteSigned**.

  Nota: Per ulteriori informazioni sulla modifica del criterio di esecuzione, consultare il sito Web di Microsoft.

- Eseguire il seguente comando PowerShell per ottenere messaggi ed esempi dettagliati per gli script:

  ```
  Sulla Console:
  ```

  Get-Help 'C:\Programmi\Arcserve\Unified Data Protection\Management\PowerCLI\UDPPowerCLI.ps1' -full

  Sul server RPS o sull'agente:

  Get-Help 'C:\Programmi\Arcserve\Unified Data Protection\Engine\PowerCLI\UDPPowerCLI.ps1' -full

Sintassi e parametri di PowerShell

SINTASSI 1

```
UDPPowerCLI.ps1 -Command <CreatePswFile> -Password
<System.Security.SecureString> -PasswordFile
<string> [<CommonParameters>]
```

SINTASSI 2

```
UDPPowerCLI.ps1 -Command <Backup> [-UDPCon-
soleServerName <String>] [-UDPConsoleProtocol <{htt-
p|https}>] [-UDPConsolePort <int>] [-
UDPConsoleUserName [<String>]] [-UDPConsolePassword
<System.Security.SecureString>] [-UDPCon-
solePasswordFile <String>] [-UDPConsoleDomainName
<String>] -planName <String> -nodeName <String> [-
backupJobType <String>] [-jobDescription <String>]
[-waitJobFinish <String String>] [-timeOut <int>] [-
jobType <{ agentbase|agentless|uncpath} String>] [-
backupScheduleType <String>] [<CommonParameters>]
```

SINTASSI 3

```
UDPPowerCLI.ps1 -Command <Restore> [-UDPCon-
soleServerName <String>] [-UDPConsoleProtocol
<String>] [-UDPConsolePort <int>] [-UDPCon-
soleUserName <String>] [-UDPConsolePassword
<System.Security.SecureString>] [-UDPCon-
solePasswordFile <String>] [-UDPConsoleDomainName
<String>] [-UDPAgentServerName <String>] [-UDPA-
gentProtocol <String>] [-UDPAgentPort <int>] [-UDPA-
gentUserName <String>] [-UDPAgentPassword
<System.Security.SecureString>] [-UDPA-
gentPasswordFile <String>] [-UDPAgentDomainName
<String>] [-RestoreDirectoryPath <String>] [-Resto-
reFilePath <String>] [-BackupSessionNumber <int>] [-
VmName <String>] -RestoreDestination <String> [-
RestoreDestinationUserName <String>] [-Resto-
reDestinationPassword <System.Se-
curity.SecureString>] [-CreateRootFolder <String>]
[-ChangeFileName <String>] [-ReplaceActiveFilesFlag
<String>] [-OverwriteExistFiles <String>] [<Com-
monParameters>]
```

SINTASSI 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>] [-Bac-
kupSessionNumber <int>] -RecoverVmName <String> [-
OverwriteExistingVM <String>] [-PoweronVM <String>]
[<CommonParameters>]
```

DESCRIZIONE

Utilità per connettere il servizio della console Arcserve UDP e inoltrare i processi di backup e ripristino.

PARAMETRI

-Command <String>

Specifica il comando utilizzato. Attualmente sono supportate le stringhe seguenti:

- CreatePswFile
- Backup
- Ripristino
- RecoverVM

Obbligatorio? **true**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-Password <System.Security.SecureString>

Specificare la password da utilizzare per la creazione del file di password.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPConsoleServerName <String>

Specifica il nome DNS del server UDP (dove è installata la console) a cui stabilire la connessione. Se non si specifica un valore, il comando cmdlet utilizza quello predefinito, ossia il nome DNS del computer locale.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **$env:COMPUTERNAME**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPConsolePort <int>

Specifica il numero di porta da utilizzare per la connessione. Se non si specifica un valore, il comando cmdlet utilizza quello predefinito, ossia 8015.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **8015**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPConsoleProtocol <String>

Specifica il protocollo su server da utilizzare per la connessione. Può trattarsi del protocollo http o https. Se non si specifica un valore, il comando cmdlet utilizza quello predefinito, ossia http.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **http**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPConsoleUserName <String>

Specifica il nome utente da utilizzare per la connessione al server UDP. Se non si specifica il nome utente, il comando cmdlet utilizza quello attualmente in uso per accedere al sistema.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **$env:UserName**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPConsolePassword <System.Security.SecureString>

Specifica la password da utilizzare per la connessione al server UDP.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-PasswordFile <String>

Specifica di creare il file di password.

Obbligatorio? **true**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPConsolePasswordFile <String>

Specifica il file di password UDP da utilizzare per la connessione al server UDP.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPAgentServerName <String>

Specifica il nome DNS del server dell'agente UDP a cui stabilire la connessione per il ripristino.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **$env:COMPUTERNAME**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPAgentProtocol <String>

Specifica il protocollo Internet da utilizzare per la connessione al server dell'agente UDP. Può trattarsi del protocollo http o https. Se non si specifica un valore, il comando cmdlet utilizza quello predefinito, ossia http.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **http**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPAgentPort <int>

Specifica il numero di porta da utilizzare per la connessione al server dell'agente UDP. Se non si specifica un valore, il comando cmdlet utilizza quello predefinito, ossia 8014.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **8014**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPAgentUserName <String>

Specifica il nome utente da utilizzare per la connessione al server dell'agente UDP. Se non si specifica il nome utente, il comando cmdlet utilizza quello attualmente in uso per accedere al sistema.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **$env:UserName**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPAgentPassword <System.Security.SecureString>

Specifica la password da utilizzare per la connessione al server dell'agente UDP.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPAgentPasswordFile <String>

Specifica il file di password da utilizzare per la connessione al server dell'agente UDP.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPAgentDomainName <String>

Specifica il nome del dominio in cui si trova l'utente dell'agente UDP specificato.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-NodeName <String>

Specifica il nome del nodo da sottoporre a backup.

Obbligatorio? **true**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-RestoreFilePath <String>

Specifica il file da ripristinare.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-RestoreDirectoryPath <String>

Specifica la directory da ripristinare.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-BackupSessionNumber <int>

Specifica il numero di sessione da utilizzare per il processo di ripristino.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-VmName <String>

Specifica il nome host del computer virtuale per il ripristino del file o della directory dalla sessione di backup.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-RestoreDestination <String>

Specifica il percorso della directory in cui verranno ripristinati i file.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-RestoreDestinationUserName <String>

Specifica il nome utente del computer di destinazione in cui ripristinare i dati. Il nome utente è quello dell'utente in grado di accedere al computer di destinazione.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-RestoreDestinationPassword <System.Security.SecureString>

Specifica la password da utilizzare per accedere al computer di destinazione.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-CreateRootFolder <String>

Se l'immagine di backup acquisita contiene una struttura delle directory principali, Arcserve UDP ricrea la stessa struttura della directory principale nel percorso di destinazione di ripristino. Se questa opzione non è selezionata, il file o cartella verrà ripristinato direttamente nella cartella di destinazione. È possibile utilizzare una delle seguenti stringhe:

- True
- False

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **False**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-ChangeFileName <String>

Se il nome file esiste già, consente di creare un nuovo file. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno quindi ripristinati nel nuovo file. È possibile utilizzare una delle seguenti stringhe:

- True
- False

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **False**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-ReplaceActiveFilesFlag <String>

Sostituisce i file attivi dopo il riavvio. Se, durante il ripristino, l'Agente Arcserve Unified Data Protection per Windows rileva che è in corso l'accesso al file esistente o che quest'ultimo è momentaneamente in uso, tale file non viene sostituito immediatamente. Per evitare l'insorgere di problemi, i file attivi vengono sostituiti al riavvio successivo del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita con il riavvio successivo). Questa opzione è disponibile solo quando il parametro **OverwriteExistingFiles** è impostato su True. È possibile utilizzare una delle seguenti stringhe:

- True
- False

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **False**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-OverwriteExistingFiles <String>

Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dai file di backup, indipendentemente dalla loro presenza sul computer. È possibile utilizzare una delle seguenti stringhe:

- True
- False

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **False**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-UDPConsoleDomainName <String>

Specifica il nome del dominio in cui si trova l'utente indicato. Se non si specifica un valore, il comando cmdlet utilizza il nome di dominio del computer locale o il nome DNS del computer locale, se non è incluso in un dominio.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-PlanName <String>

Specifica il nome del piano in cui sono definite le impostazioni del processo di backup.

Obbligatorio? **true**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-BackupJobType <String>

Specifica il tipo di processo di backup. Può essere utilizzato uno dei seguenti valori: Full (backup completo), Incr (backup incrementale) o Rsyn (backup di risincronizzazione). Sono supportate le stringhe seguenti:

- Completo
- Incr
- Rsyn

Obbligatorio? **true**

Posizione? **denominata**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-JobDescription <String>

Specifica la descrizione del processo di backup.

Obbligatorio? **true**

Posizione? **denominata**

Valore predefinito: **PowerCLIJo**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-RecoverVmName <String>

Specifica il nome host del computer virtuale da recuperare.

Obbligatorio? **true**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-OverwriteExistingVM <String>

Se il valore è true, il processo di ripristino andrà a sovrascrivere il computer virtuale esistente. Il valore predefinito è false. È possibile utilizzare una delle seguenti stringhe:

- True
- False

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **False**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-PoweronVM <String>

Se il valore è true, il computer virtuale viene attivato una volta recuperato. Il valore predefinito è false. È possibile utilizzare una delle seguenti stringhe:

- True
- False

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **False**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-waitJobFinish <{true|false} String>

Se il valore è true, il comando attende ulteriori istruzioni fino al completamento del processo di backup. Il valore predefinito è false. È possibile utilizzare una delle seguenti stringhe:

- True
- False

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **False**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-timeOut <int>

Specifica il tempo di attesa massimo (in secondi) per completare il processo di backup.

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito: **600**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-jobType <String>

Specifica il tipo di processo di backup per il tipo di nodo differente. Il valore predefinito è agentabse. Utilizzare una delle seguenti stringhe:

- agentbase
- agentless
- uncpath

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito **agentbase**

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

-backupScheduleType <String>

Consente di indicare una pianificazione per il processo di backup, inoltrare immediatamente il processo di backup alla pianificazione specificata ed eseguirlo una sola volta. Sono supportate le stringhe seguenti:

- Ogni giorno
- Ogni settimana
- Ogni mese

Obbligatorio? **false**

Posizione? **denominata**

Valore predefinito

Accettare input da pipeline? **false**

Accettare caratteri jolly? **false**

<CommonParameters>

Questo comando cmdlet supporta parametri comuni quali **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer** e **OutVariable**. Per ulteriori informazioni, consultare la sezione about_CommonParameters.

INPUT

OUTPUT

- 0 o 1

Se il processo viene inoltrato correttamente, il comando restituisce 0, altrimenti 1.

Esempi di PowerShell

Creare una password di tipo System.Security.SecureString

Nota: se si dispone di uno script PowerShell configurato in Arcserve UDP 6.5 che utilizza una password di testo normale, modificare la stessa operazione per utilizzare $SecurePassword o utilizzare il file di password.

Descrizione

Il comando viene utilizzato per creare la password con il tipo System.Security.Security.SecureString e viene utilizzato anche da tutti gli altri comandi. Il tipo System.Security.SecureString è un tipo di sistema predefinito. Esistono diversi modi per generarlo. I due tipi seguenti sono comunemente usati per scopi diversi:

- Questo comando richiede l'inserimento della password sulla console PowerShell. Richiede l'interazione con gli utenti finali. In genere dopo l'esecuzione di questo comando, è possibile eseguire il comando *CreatePswFile* per scrivere la password di un file di password. Quindi utilizzare il file di password per l'esecuzione degli script PowerShell automaticamente.

  ```
  $SecurePassword = Read-Host -AsSecureString
  ```

- Questo comando richiede la password con testo in chiaro. Può essere utilizzato direttamente per eseguire automaticamente gli script PowerShell.

  ```
  $SecurePassword = ConvertTo-SecureString
  "<PlainPassword>" - AsPlainText - Force
  ```

- (Facoltativo) Dopo aver eseguito uno dei comandi precedenti per assegnare una password, eseguire il comando CreatePswFile per scrivere la password in un file di password. Quindi utilizzare il file di password per l'esecuzione degli script PowerShell automaticamente.

  Il comando cripta la password sicura e la salva nel file della password.

  ```
  C:\PS>UDPPowerCLI.ps1 -Command CreatePswFile
  -Password $SecurePassword -PasswordFile
  myUDPPasswordFile
  ```

Esempio 1

Descrizione

Il comando cripta la password sicura e la salva nel file della password.

```
C:\PS>UDPPowerCLI.ps1 -Command CreatePswFile -Pas-
sword $SecurePassword -PasswordFile myUDPPas-
swordFile
```

Esempio 2

Descrizione

Sul server locale, il comando consente la connessione al servizio della console UDP con il protocollo HTTP tramite la porta 8015 e l'inoltro di un processo di backup incrementale per il piano denominato *myplan*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleUserName myUsr -UDPConsolePassword $Se-
curePassword -PlanName myPlan -BackupJobType Incr
```

Esempio 3

Descrizione

Sul server locale, il comando consente la connessione al servizio della console UDP con il protocollo HTTP tramite la porta 8015 e l'inoltro di un processo di backup incrementale per il nodo denominato *myNodeName*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleUserName myUsr -UDPConsolePasswordFile myUDPPas-
swordFile -NodeName myNodeName -BackupJobType Incr
```

Esempio 4

Descrizione

Il comando consente la connessione al servizio della console UDP sul server denominato *myServer* con il protocollo HTTPS tramite la porta 8018 e l'inoltro di un processo di backup completo per il piano denominato *myPlan*, impostando la descrizione del processo come *myJob*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleServerName myServer -UDPConsoleProtocol https -
UDPConsolePort 8018 -UDPConsoleUserName myUsr -
UDPConsolePassword $SecurePassword -UDPCon-
soleDomainName myDomain -PlanName myPlan -Bac-
kupJobType Full -JobDescription myJob
```

Esempio 5

Descrizione

Il comando consente la connessione al servizio dell'agente UDP sul server denominato *yourUDPAgentServer* con il protocollo HTTP tramite la porta 8014 e l'inoltro di un processo di backup incrementale per *yourUDPAgentServer*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPA-
gentServerName yourUDPAgentServer -
```

```
UDPAgentPasswordFile myUDPAgentPasswordFile -Bac-
kupJobType Incr
```

Esempio 6

Descrizione

Il comando consente di abbreviare il nome del parametro.

```
C:\PS>UDPPowerCLI.ps1 -Cmd Backup -Svr myServer -Ptc
https -Prt 8018 -Usr myUsr -Psw $SecurePassword -Dmn
myDomain -Pln myPlan -Jbt Full -Jbd myJob
```

Esempio 7

Descrizione

Il comando consente la connessione al server denominato *yourUDPAgentServer* utilizzando il nome utente dell'ambiente, il protocollo HTTP predefinito e la porta 8014. Verifica se il numero della sessione di backup è 1 dalla configurazione di backup di *yourUDPAgentServer*, quindi esegue il ripristino della directory nel percorso originale, con l'opzione di ripristino Sovrascrivi i file esistenti selezionata.

```
C:\PS>UDPPowerCLI.ps1 -Command restore -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
RestoreDirectoryPath 'c:\Test' -BackupSessionNumber
1
```

Esempio 8

Descrizione

Il comando consente la connessione al server denominato *yourUDPAgentServer* utilizzando il protocollo HTTPS e la porta 8018. Verifica se il numero della sessione di backup è 1 dalla configurazione di backup di *yourUDPAgentServer*, quindi esegue il ripristino del file 1.txt in un altro percorso, con l'opzione di ripristino Sovrascrivi file esistente e crea directory radice selezionata.

```
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' -
RestoreDestination 'C:\restore' -Resto-
reDestinationUserName remoteAccessUser -Resto-
reDestinationPassword remoteAccessPsw -
CreateBaseFolder 'true'
```

Esempio 9

Descrizione

Il comando consente la connessione al server denominato *yourUDPAgentServer* utilizzando il nome utente dell'ambiente, il protocollo HTTP predefinito e la porta 8014. Quindi stabilisce la connessione al server UDP utilizzando la porta 8015 e il protocollo HTTP predefiniti per verificare se il numero della sessione di backup è 1. Infine, esegue il ripristino della directory in un altro percorso, con l'opzione di ripristino Sovrascrivi file esistente e crea directory radice selezionata.

```
C:\PS>UDPPowerCLI.ps1 -Command restore -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
RestoreDirectoryPath 'c:\Test' -BackupSessionNumber
1 -RestoreDestination 'C:\restore' -Resto-
reDestinationUserName remoteAccessUser -Resto-
reDestinationPassword remoteAccessPsw -
UDPConsoleServerName yourUDPServer -vmname sour-
ceVMName -UDPConsolePasswordFile myUDPPasswordFile -
domainname yourUDPDomainName -OverwriteExistFiles
'true' -CreateRootFolder 'true'
```

Esempio 10

Descrizione

Il comando consente la connessione al server denominato *yourUDPAgentServer* utilizzando il nome utente dell'ambiente, il protocollo HTTP predefinito e la porta 8014. Quindi stabilisce la connessione al server UDP utilizzando la porta 8015 e il protocollo HTTP predefiniti per verificare se il numero della sessione di backup è 1. Infine, esegue il ripristino del computer virtuale nel percorso originale con l'opzione Sovrascrivi computer virtuale esistente e attiva computer virtuale dopo il ripristino selezionata.

```
C:\PS>UDPPowerCLI.ps1 -Command RecoverVM -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
BackupSessionNumber 1 -UDPConsoleServerName you-
rUDPServer -recovervmname sourceVMName -UDPCon-
solePasswordFile myUDPPasswordFile -
UDPConsoleDomainName yourUDPDomainName -Over-
writeExistingVM 'true' -PoweronVM 'true'
```

Esempio 11

Descrizione

Il comando consente di inoltrare un processo di backup settimanale sull'agente UDP immediatamente e di eseguirlo solo una volta.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPA-
gentServerName myServer -UDPAgentPassword $Se-
curePassword -UDPAgentDomainName myDomainName -
UDPAgentUserName UDPAgentUsername -BackupJobType
Incr -backupScheduleType 'weekly' -jobDescription
'PowerCLIJob'
```

Esempio 12

Descrizione

Il comando consente di inoltrare il processo di backup e impostare il timeout di attesa in secondi per il completamento del processo.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleServerName myServer -UDPConsolePasswordFile
myUDPPasswordFile -UDPConsoleDomainName myDomainName
-nodeName myNodeName -UDPConsoleUserName myAdmin -
BackupJobType Incr -jobDescription 'PowerCLIJob' wai-
tJobFinish 'true' -timeout 600 -jobType 'agentbase'
```

File di configurazione e proprietà di PowerCLI

È possibile personalizzare il file di configurazione e le proprietà di UDP PowerCLI seguenti:

Nome file di configurazione: *PowerCLIConfiguration.properties*

Posizione di installazione del file di configurazione:

- *C:\Programmi\Arcserve\Unified Data Protection\Management\Configuration*
- *C:\Programmi\Arcserve\Unified Data Protection\Engine\Configuration*

Formato del file di configurazione:

Enable24HoursSetting=yes

LogPath=D:\PowerCLILogPath

RotationSizeInMB=2

RetentionPeriodInDays=5

RetainNoOfFiles=6

Proprietà di configurazione:

Nome proprietà	Descrizione	Valore predefinito	Valore accettato
Enable24HoursSetting	▪ Se il valore è impostato su Sì, il	Sì	Sì o No

	timestamp del file di registro viene scritto in formato 24 ore. ▪ Se il valore è impostato su No, il timestamp del file di registro viene scritto in formato 12 ore.		
LogPath	▪ La posizione della cartella dei file di registro di PowerCLI. ▪ Se la posizione non viene fornita, il file di registro viene scritto nella posizione predefinita. ▪ LogPath accetta percorsi relativi e assoluti. ▪ Simboli eccetto \ / : * ? < > | sono accettabili per il nome del file o della cartella.	-	-
RotationSizeInMB	▪ Se viene raggiunto il limite specificato in RotationSizeInMB, il file di registro PowerCLI viene rinominato (Ruotato) con un'indicazione di data/ora.	0	Minimo = 1 Massimo = 1024
RetentionPeriodInDays	▪ Se i file ruotati sono precedenti rispetto valore fornito in RetentinPeriodInDays, i file di registro precedenti vengono eliminati.	0	Minimo = 5 Massimo = 365
RetainNoOfFiles	▪ Se sono presenti più file di registro ruotati rispetto al valore fornito in RetainNoOfFiles, i file aggiuntivi vengono eliminati.	0	Minimo = 5 Massimo = 1000

Note:

- Se si forniscono valori per le proprietà di configurazione diversi da quelli consentiti, PowerCLI visualizza un errore e l'esecuzione viene interrotta.
- Se si forniscono valori predefiniti per le proprietà di configurazione, l'esecuzione di PowerCLI continua e viene eseguita con il comportamento predefinito.

Chapter 4: Protezione del sistema Oracle mediante Recovery Manager (RMAN)

Recovery Manager (RMAN) è un'utilità Oracle che consente di eseguire processi di backup, ripristinare e recuperare attività sui database e automatizzare l'amministrazione delle strategie di backup. Utilizzando questa funzionalità, è possibile eseguire facilmente il backup, il ripristino e il recupero dei file di database.

La presente sezione descrive i seguenti argomenti:

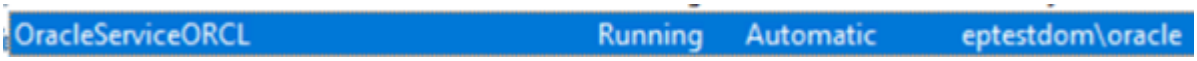
Verifica dei prerequisiti per i database Oracle con RMAN (Windows e Linux)

Prerequisiti per la configurazione quando Oracle è installato su Windows

Aggiunta di un piano

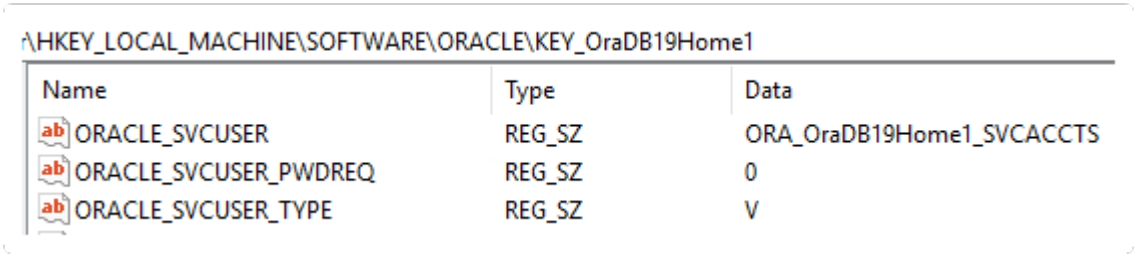
- I nodi Oracle di Windows, la console UDP e il server RPS devono trovarsi nello stesso dominio.
- La console UDP e i sistemi RPS devono essere installati e utilizzati con un account amministratore di dominio ("<domain>\administrator") o un account equivalente.
- Quando si accede alla console UDP, procedere come segue:
  1. L'utente "<dominio>\Amministratore" viene aggiunto al gruppo "ORA_DBA" locale nei nodi Oracle di Windows.
  2. Aggiungere il nodo Oracle alla console UDP utilizzando l'ID utente "<domain>\DomainUser".

  Nota: è possibile utilizzare qualsiasi utente in UDP diverso dall'amministratore, ma è necessario fornire le autorizzazioni appropriate.
- Supporta gli account Oracle seguenti utilizzati durante le installazioni Oracle (impostazione valida sia per RAC che per stand-alone).
  - Utente del dominio: prendere nota dell'utente del dominio proprietario del servizio Oracle (account di servizio). Ad esempio, eptest-dom\oracle.

  - Account virtuale: quando Oracle viene installato utilizzando un account virtuale, verificare i parametri nel registro di sistema del server Oracle prima di aggiungere il database al piano UDP.

    Nota: per impostazione predefinita, gli account virtuali sono abilitati in Windows.

- Assicurarsi di configurare correttamente il listener, il quale consente di proteggere il database Oracle e di connettersi a sqlplus e RMAN per tale database.

  Esempio: "rman target /" deve tenere conto del database corretto.

Backup

- Quando si esegue il backup dei database Oracle, assicurarsi che siano in stato APERTO con la modalità ARCHIVELOG attivata. Per ulteriori informazioni, consultare la sezione Attivazione della modalità ARCHIVELOG.
- Per eseguire correttamente i backup Oracle RMAN con Arcserve UDP, è necessario abilitare l'autenticazione nativa di Windows. Per confermare se l'autenticazione di Windows è abilitata, assicurarsi che la riga seguente sia stata aggiunta al file sqlnet.ora nel percorso ORACLE_HOME/-network/admin.

  SQLNET.AUTHENTICATION_SERVICES= (NTS)
- La condivisione delle cartelle pubbliche è disattivata per consentire l'accesso protetto ai database.

  Per disattivare l'utilizzo della cartella pubblica per la condivisione di rete, procedere come segue:

  1. Accedere a Centro connessioni di rete e condivisione, quindi fare clic su **Modifica impostazioni di condivisione avanzate**.
  2. Nel riquadro sinistro, cercare l'impostazione di condivisione della cartella pubblica per il percorso di rete attivo, quindi fare clic su **Disattiva condivisione cartelle pubbliche (le persone che hanno eseguito l'accesso a questo computer potranno comunque accedere a queste cartelle)**.
  3. Fare clic su **Salvare le modifiche**.

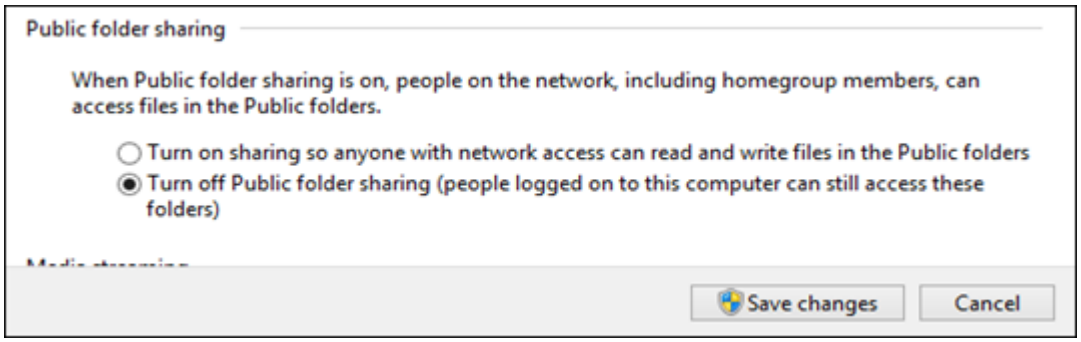


Tabelle di ripristino

I ripristini a livello di tabella e di spazio tabella utilizzano il database ausiliario, il

quale richiede le seguenti autorizzazioni:

- **Utente di dominio per l'installazione Oracle:** l'account di servizio dell'utente Oracle al gruppo “Amministratori” nei nodi Oracle. Ad esempio, eptestdom\oracle viene aggiunto al gruppo di amministratori locali.
- **Account virtuale per l'installazione Oracle**: aprire la chiave di registro: HKLM\SYSTEM\CurrentControlSet\services\eventlog\Application, quindi fare clic con il pulsante destro del mouse e aggiungere le autorizzazioni al gruppo, ad esempio 'ORA_OraDB18Home1_SVCACCTS'.

Ripristina sul nodo alternativo

- La stessa versione di Oracle con la stessa configurazione è installata sul sistema di destinazione.
- Il database viene installato con lo stesso SID del computer di origine (originale).
- Il database Oracle sul nodo di destinazione deve essere in stato di arresto.

Impostazioni del firewall per consentire l'accesso ai nodi Oracle di 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="ora_1521" dir=in action=allow protocol=TCP localport=**1521**	

netsh advfirewall firewall add rule name="ora_1521" dir=out action=allow protocol=TCP localport=**1521**	Il numero di porta può cambiare in base alla porta configurata.

Prerequisiti per la configurazione quando Oracle è installato su Linux

Aggiunta di un piano

- Il nodo Oracle /etc/hosts deve disporre di una voce per FQDN e "resolv.conf" con la voce DNS appropriata.
- Ciascun database da proteggere deve disporre di una voce nel file /etc/oratab.

  Nota: in un ambiente RAC, assicurarsi che il contenuto sia aggiornato per entrambi i nodi.

  La sintassi nel file /etc/oratab è la seguente:

  <DB_UNIQUE_NAME>:<ORACLE_HOME>:<ACTIVE/INACTIVE>

  Esempio: ORCL:/u01/app/oracle/ORCL/:Y

Backup

- Quando si esegue il backup dei database Oracle, assicurarsi che siano in stato APERTO con la modalità ARCHIVELOG attivata. Per ulteriori informazioni, consultare la sezione Attivazione della modalità ARCHIVELOG.
- Installare smbclient utilizzando il seguente comando:

  #yum install smbclient
- Assicurarsi di configurare correttamente il listener, il quale consente di proteggere il database Oracle e connettersi a sqlplus e RMAN per tale database.

  Esempio: verificare “lsnrctl status” per i database disponibili per un particolare listener.

  Il comando "rman target /" deve essere connesso al database corretto specificato per il backup.

Processi Assured Recovery

- Assicurarsi che i database Oracle per il backup siano nello stato MONTAGGIO o APERTO.

Autenticazione basata su chiave pubblica e privata

Nota: l'autenticazione basata su chiave pubblica e privata è stata implementata per l'esecuzione degli script RMAN di Linux. In tal modo si evita l'utilizzo di password di testo normale durante l'esecuzione di script remoti su server Oracle di

Linux da Recovery Point Server (RPS).

1. Sul nodo RPS, procedere come segue:
   a. Verificare che il programma di installazione abbia creato la directory *PrivateKey* nel seguente percorso:

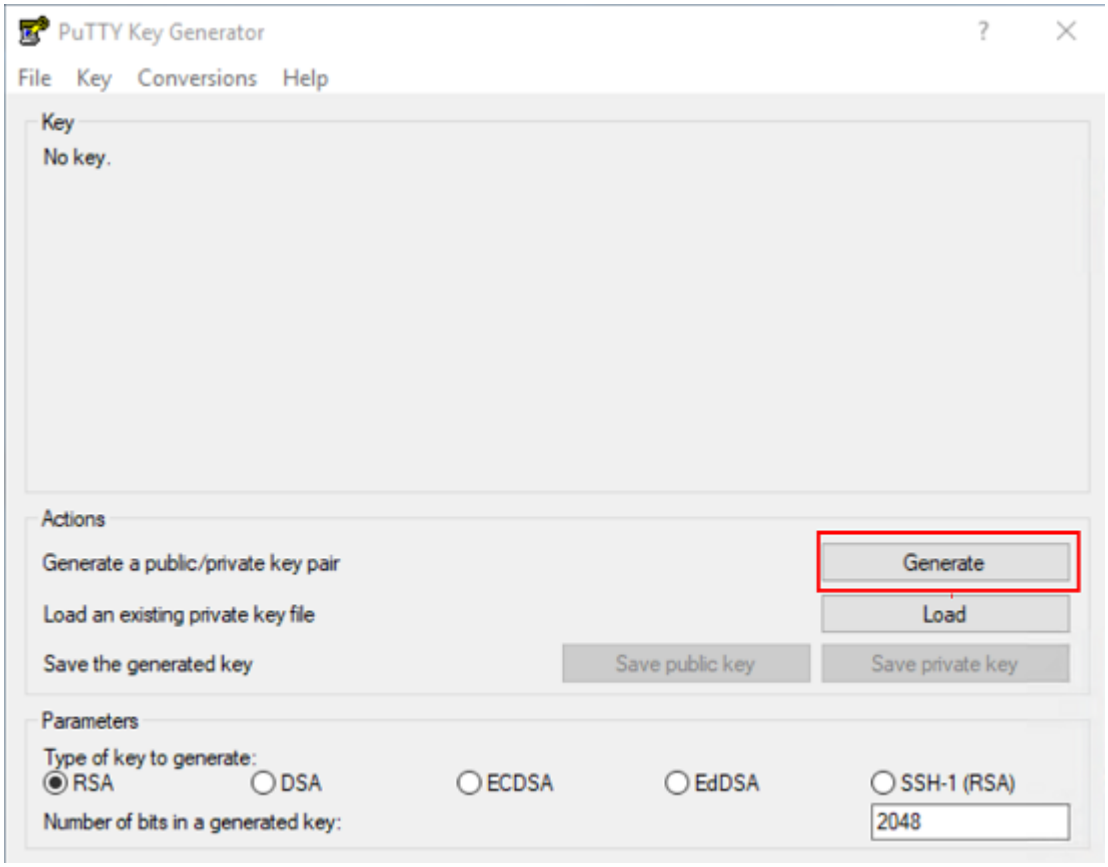
      Install Path\Arcserve\Unified Data Protection\Engine\BIN\OracleRMAN\PrivateKey

   b. Installare PuTTY (versione 0.73 o successiva), quindi eseguire una delle seguenti operazioni per aprire il Generatore di chiavi PuTTY.
      - In cmd.exe, eseguire il comando *puttygen*.
      - Accedere a **Tutti i programmi** > **PuTTY** > **PuTTYgen**.

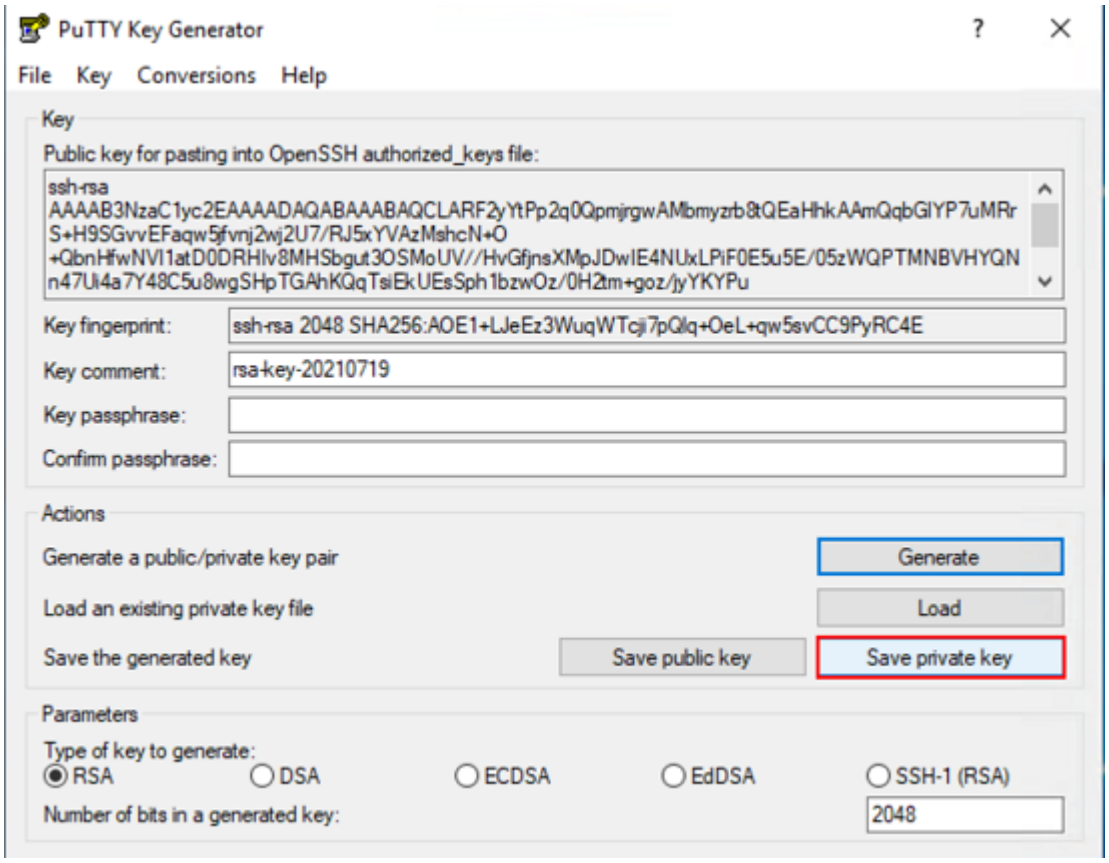
      Verrà visualizzata la finestra di dialogo Generatore di chiavi PuTTY.

   c. Nella finestra di dialogo PuTTY Key Generator y, fare clic su **Genera**.

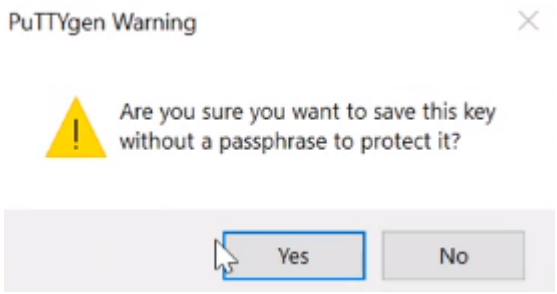
      Vengono generate le chiavi pubbliche e private.



   d. Fare clic su **Salva chiave privata**.



e. Nella finestra di dialogo PuTTYgen Warning, fare clic su **Yes** per salvare la chiave senza una passphrase.



f. Durante il salvataggio della chiave privata, accedere al percorso seguente, digitare il nome del file e fare clic su **Salva**:

Install Path\Arcserve\Unified Data Protection\Engine\BIN\OracleRMAN\PrivateKey

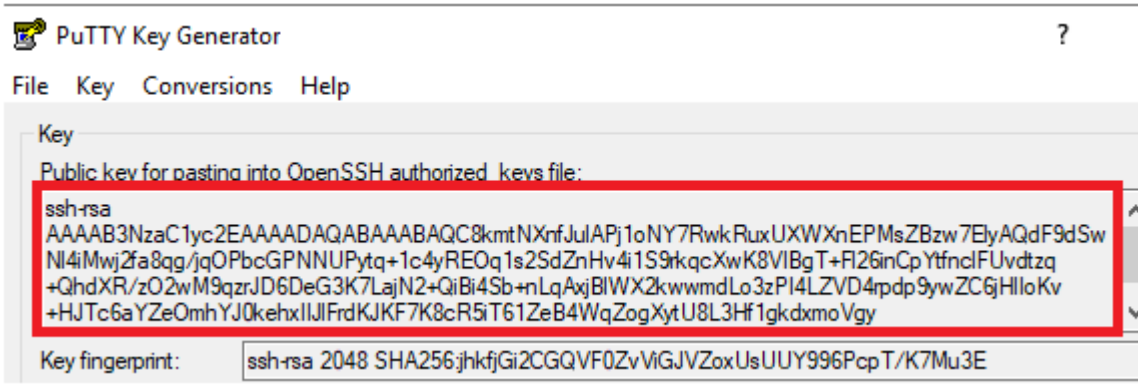
Note:

- Il nome del file deve essere nel formato PrivateKeyFile.ppk. È possibile specificare qualsiasi nome.
- Salvare la chiave privata con estensione .ppk nel seguente percorso:

Engine\Bin\OracleRMAN\PrivateKey

- Copiare manualmente la chiave pubblica dalla finestra di dialogo PuTTY Key Generator e salvarla in formato di testo nella cartella seguente per riferimenti futuri nel caso in cui sia necessario aggiungerla ad altri server Oracle di Linux:

  Engine\Bin\OracleRMAN\PrivateKey



g. Aprire il percorso *Engine\Bin directory* su cmd.exe.

h. Eseguire il comando seguente per crittografare la chiave privata utilizzando l'utilità della riga di comando RMANCryptUtil.exe:

   RMANCryptUtil.exe "C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN\<Nome della chiave privata generata>.ppk"

   Il file della chiave privata crittografata viene generato con estensione **.enc** nel percorso seguente:

   Engine\Bin\OracleRMAN\PrivateKey

   Un esempio del nome file: PrivateKey.ppk.enc

   La chiave privata crittografata (.enc), generata mediante RMANCryptutil, viene salvata nella cartella Chiave privata.

i. Copiare la chiave **.enc** su altri nodi RPS e altre console UDP.

j. Sul nodo della console UDP, creare la cartella PrivateKey come segue, quindi copiare la chiave .enc nella cartella PrivateKey:

   UDP\Engine\Bin\OracleRMAN\PrivateKey

k. Copiare la chiave pubblica dall'interfaccia utente di PuTTYgen e fare riferimento al passaggio 2 per aggiungere la chiave pubblica nel nodo Oracle di Linux.

2. Sul nodo Linux in cui è installato Oracle, eseguire le seguenti operazioni:

a. Assicurarsi che la cartella *.ssh* sia disponibile nella directory principale (~). Se la directory *.ssh* non è disponibile, creare la directory utilizzando il seguente comando e le autorizzazioni predefinite:

   mkdir ~.ssh

b. Verificare che il servizio *sshd* sia in esecuzione sul server Linux utilizzando il seguente comando:

   service sshd status

   Nota: se *sshd* non è installato, installare *sshd* in base alla versione del sistema operativo Linux.

c. Aprire o modificare il file *authorized_keys* utilizzando il seguente comando:

   vim authorized_keys

d. Creare o modificare il file *.ssh/authorized_keys*.

e. Aggiungere la chiave pubblica generata sul server RPS al file *.ssh/authorized_keys* utilizzando PuTTY Key Generator.

f. Impostare le autorizzazioni minime richieste per il file *.ssh/authorized_keys* utilizzando il seguente comando:

   chmod 400 .ssh/authorized_keys

Note:

- Per aggiungere una chiave pubblica in qualsiasi altro nodo Oracle di Linux ma facendo in modo che il server RPS rimanga invariato, eseguire solo il passaggio 2 indicato sopra.
- Durante la modifica del nodo RPS, seguire i passaggi 1 e 2 sopra indicati.

Creazione di un piano di backup per il database Oracle (Windows e Linux)

Per proteggere i nodi semplici o i nodi del cluster di Windows e Linux, è necessario creare un piano. Il piano consiste in un'attività di backup. Questa attività di backup consente di specificare i nodi che si desidera proteggere, la destinazione di backup e la pianificazione dei backup. La destinazione di backup è un Recovery Point Server su cui archiviare i dati sottoposti a backup. La destinazione può essere una destinazione locale o una cartella di condivisione remota.

La presente sezione descrive i seguenti argomenti:

Creazione di un piano con un'attività di backup

Un piano di backup include un'attività di backup che esegue un backup del nodo e archivia i dati nella destinazione specificata. Ciascuna attività consiste di parametri che definiscono l'origine, la destinazione, la pianificazione, e altri dettagli di backup. In questa sezione vengono fornite informazioni sulla creazione di un piano di backup per il database Oracle.

Effettuare le operazioni seguenti:

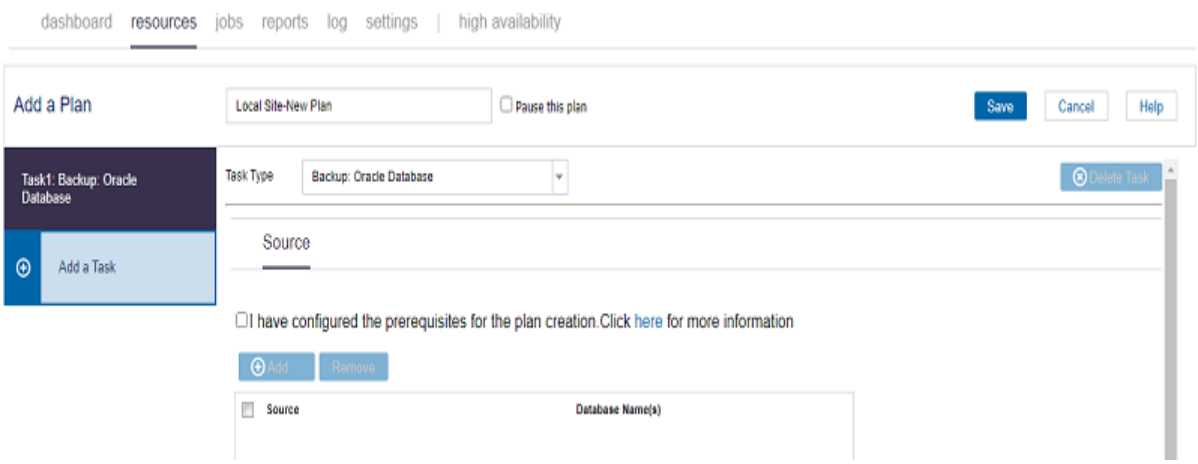
1. Accedere alla console Arcserve UDP.
2. Accedere a **Risorse** > **Piano** > **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

   Viene visualizzata la pagina Aggiungi un piano.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.
6. Dall'elenco a discesa Tipo di attività, selezionare **Backup: Oracle Database**.



Specificare i dettagli Origine, Destinazione, Pianificazione e Avanzate.

Note:

- Per verificare il danneggiamento dei blocchi fisici e logici nei file di dati esistenti sul computer di origine Oracle, viene utilizzato il comando Backup Validate RMAN.
- Per aggiungere la convalida al processo di backup, utilizzare la seguente chiave di registro:

  \HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\SourceDBValidation

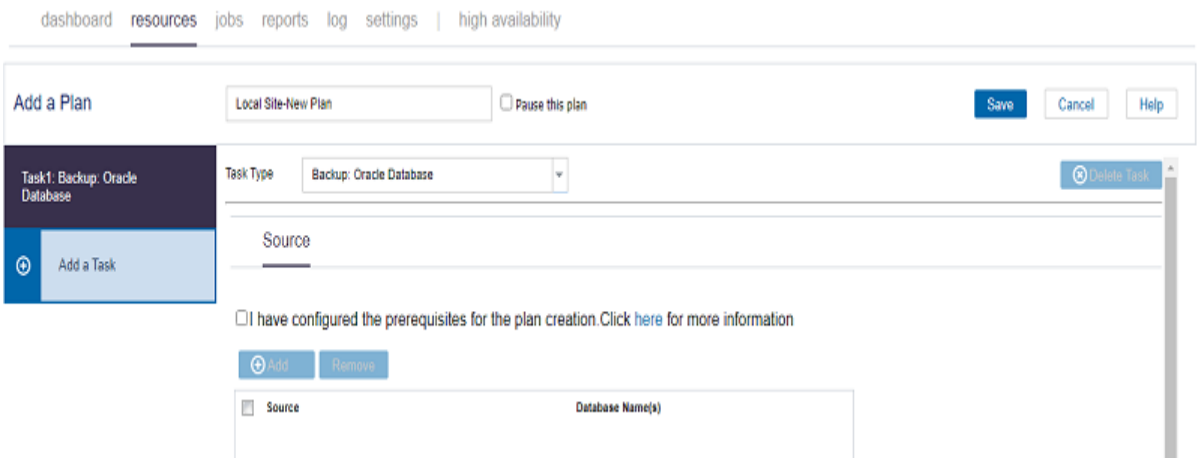
  - Se la chiave non viene aggiunta (impostazione predefinita), la convalida del backup non è abilitata
  - Se la chiave viene aggiunta come 1, la convalida del backup è abilitata
  - Se la chiave viene aggiunta con qualsiasi altro valore, la convalida del backup non è abilitata
- La convalida del backup è un'attività che richiede molto tempo. L'attivazione di questa impostazione aumenta il tempo di backup in base alla dimensione dei file di dati. La convalida viene eseguita sull'intero file di dati di origine anche per un backup incrementale.

Definizione dell'origine

La pagina Origine consente di specificare i nodi di origine che si desidera proteggere. È possibile selezionare più di un nodo per un piano. Se non sono stati aggiunti nodi alla console, è possibile aggiungerli in fase di creazione o modifica di un piano dalla pagina Origine. È inoltre possibile salvare un piano senza aggiungere nessun nodo di origine. Il piano viene distribuito soltanto dopo l'aggiunta dei nodi di origine.

Effettuare le operazioni seguenti:

1. Nella scheda Origine, per confermare le configurazioni dei prerequisiti, selezionare la casella di controllo **I prerequisiti per la creazione del piano sono stati configurati**. Per ulteriori informazioni, consultare la sezione Verifica dei prerequisiti per il database Oracle per RMAN (Windows e Linux).



2. Fare clic su **+ Aggiungi**.
3. Selezionare una delle seguenti opzioni:

Selezionare le origini da proteggere in Arcserve UDP

Viene visualizzata la finestra di dialogo Selezionare i nodi da proteggere. Selezionare i nodi dall'elenco visualizzato. Selezionare questa opzione se sono stati già aggiunti nodi alla Console.

Aggiungi nodo Windows

Viene visualizzata la finestra di dialogo Aggiungi nodo Oracle di Windows. Selezionare questa opzione se non sono stati aggiunti nodi e si desidera aggiungere manualmente i nodi da proteggere.

Aggiungi nodo Linux

Viene visualizzata la finestra di dialogo Aggiungi nodo Oracle di Linux. Selezionare questa opzione se non sono stati aggiunti nodi e si desidera aggiungere manualmente i nodi da proteggere.

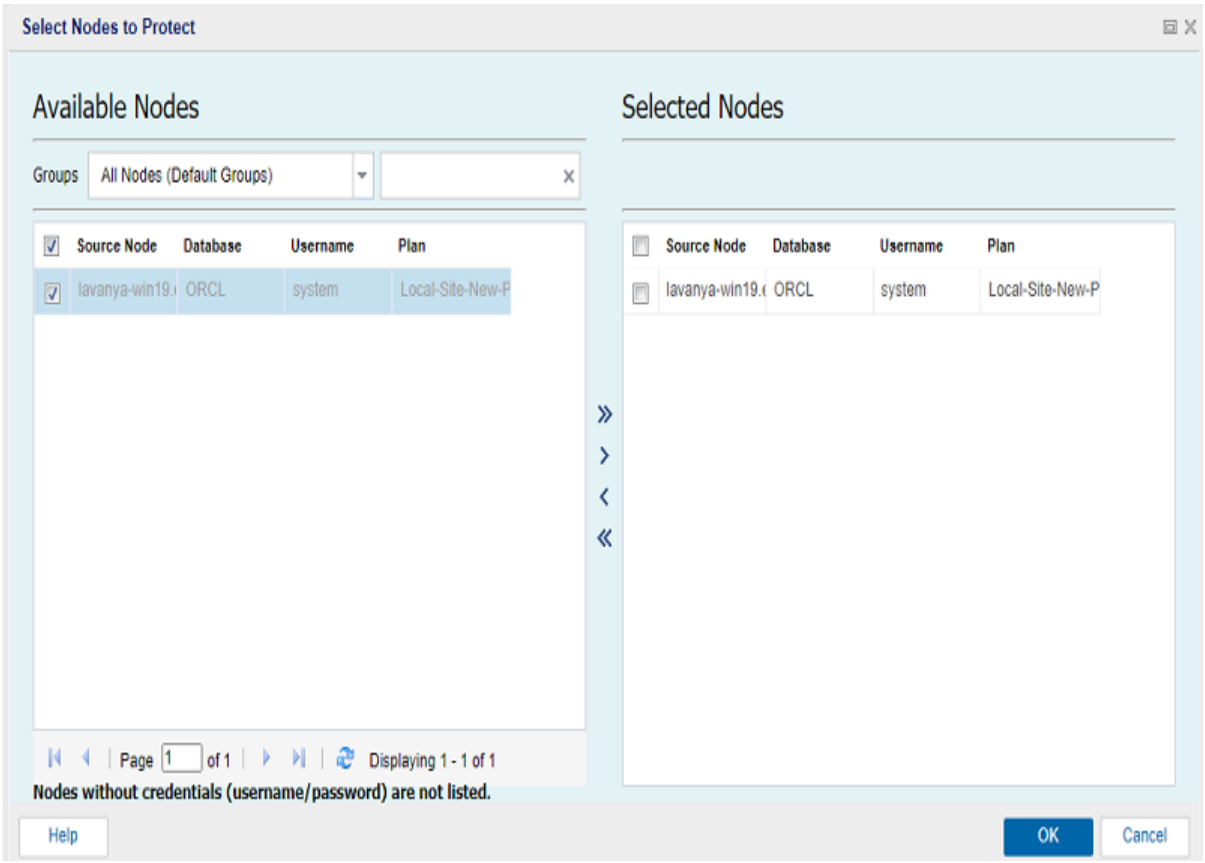
4. Se si seleziona l'opzione **Seleziona origini da proteggere in Arcserve UDP**, nella finestra di dialogo Seleziona nodi da proteggere, procedere come segue:
   a. (Facoltativo) Selezionare un filtro dall'elenco a discesa Gruppi per filtrare i nodi. Immettere parole chiave per applicare ulteriori filtri ai nodi.

      I nodi vengono visualizzati nella colonna Nodi disponibili.

   b. Selezionare i nodi dalla colonna Nodi disponibili, quindi fare clic sulla freccia destra singola (>) o sulla freccia destra doppia (>>) per spostare rispettivamente i nodi selezionati o tutti i nodi nella colonna Nodi selezionati.

      I nodi vengono visualizzati nella colonna Nodi selezionati.

   c. Fare clic su **OK** per chiudere la finestra di dialogo.



5. Se si seleziona l'opzione **Aggiungi nodo Windows**, nella finestra di dialogo Aggiungi nodo Oracle di Windows eseguire le seguenti operazioni:
   a. Immettere il nome del nodo o l'indirizzo IP del nodo Oracle che si desidera aggiungere.

b. Immettere una descrizione per il nodo.

c. Immettere le credenziali di amministratore.

d. Fare clic su **Aggiungi**.

   Attendere il completamento della convalida del nome utente e della password.

   Il nodo viene aggiunto al riquadro centrale.

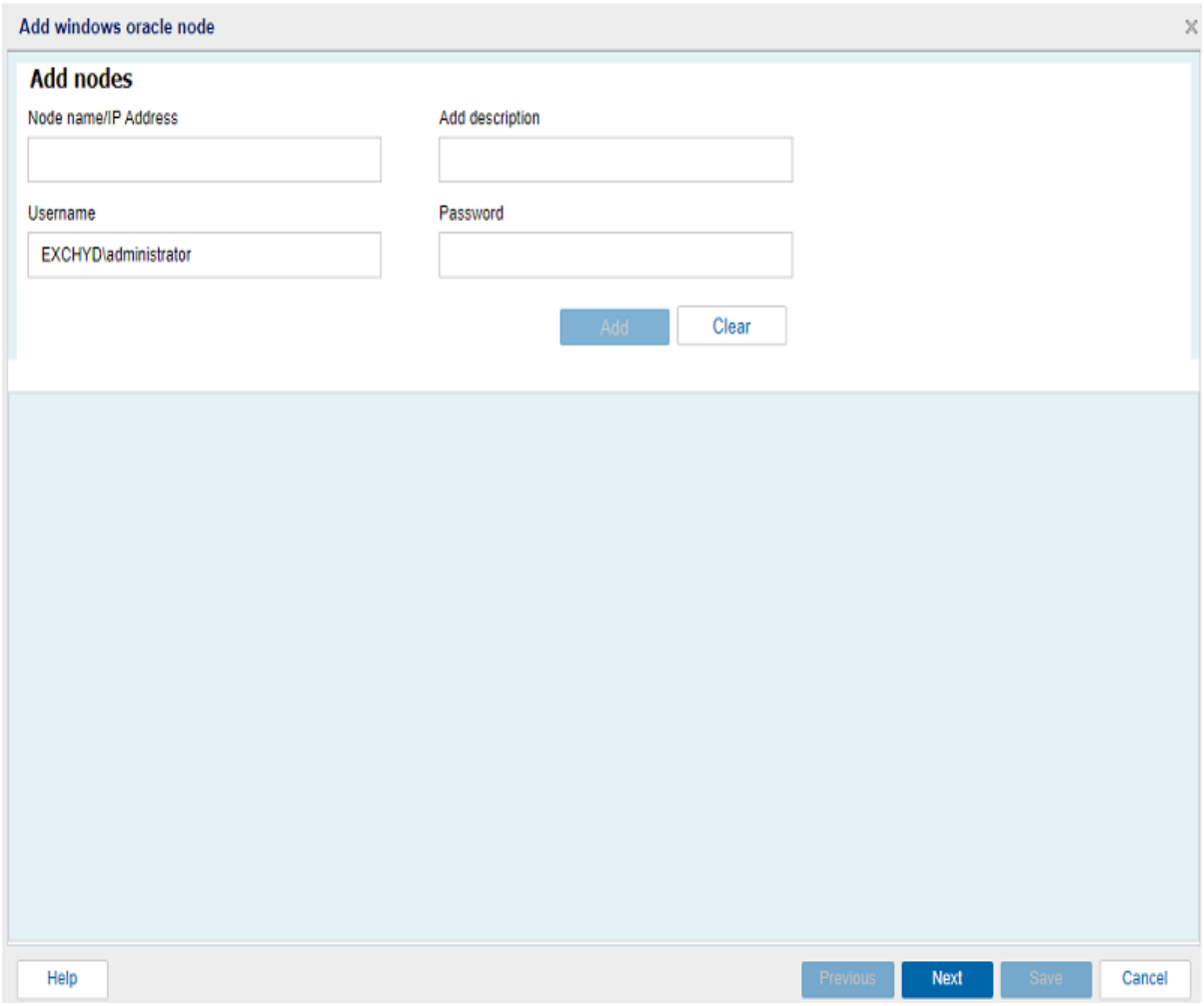
e. Per aggiungere più nodi, seguire nuovamente la procedura. Tutti i nodi aggiunti vengono elencati nel riquadro centrale.

f. Fare clic sul simbolo di espansione accanto all'indirizzo IP, quindi verificare i dettagli aggiunti.

   Note:

   - Per modificare i nodi aggiunti dall'elenco, selezionare il nodo che si desidera modificare, quindi fare clic su **Modifica**.
   - Per rimuovere i nodi aggiunti dall'elenco, selezionare i nodi che si desidera rimuovere, quindi fare clic su **Rimuovi**.
   - Per rimuovere tutti i nodi aggiunti, fare clic su Rimuovi **tutto**.

g. Fare clic su **Avanti**.



6. Se si seleziona l'opzione **Aggiungi nodo Linux**, nella finestra di dialogo Aggiungi nodo Oracle di Linux eseguire le seguenti operazioni:
   a. Immettere il nome del nodo o l'indirizzo IP del nodo Oracle che si desidera aggiungere.
   b. Immettere una descrizione per il nodo.
   c. Immettere il nome utente.
   d. Per il titolare di Oracle, immettere il nome utente utilizzato per l'installazione di Oracle.
   e. Per la porta SSH, specificare il valore della porta. Il valore predefinito della porta è 22.
   f. Fare clic su **Aggiungi**.

      Attendere il completamento della convalida del nome utente e della password.

      Il nodo viene aggiunto al riquadro centrale.

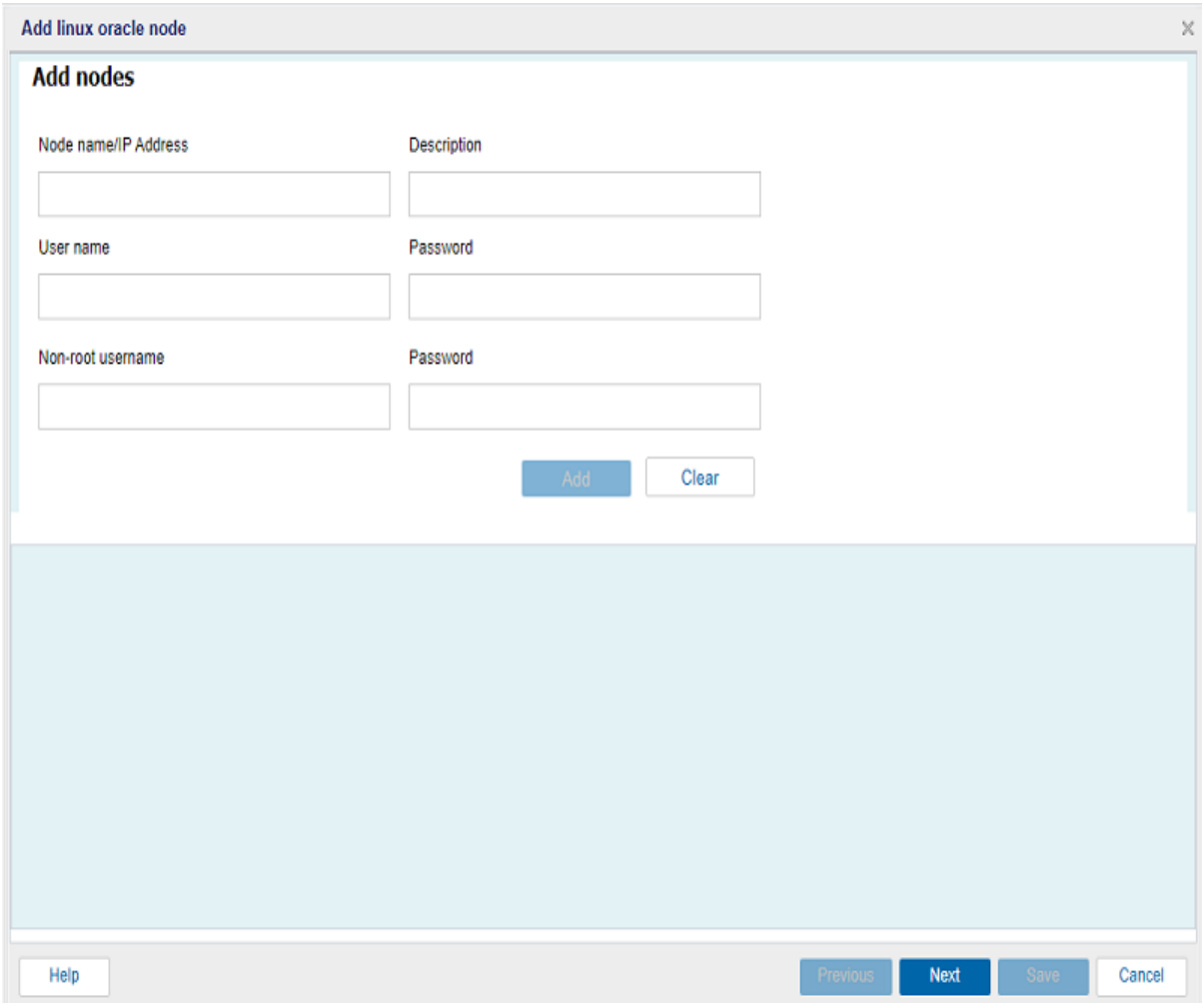
g. Per aggiungere più nodi, seguire nuovamente la procedura. Tutti i nodi aggiunti vengono elencati nel riquadro centrale.

h. Fare clic sul simbolo di espansione accanto all'indirizzo IP, quindi verificare i dettagli aggiunti.

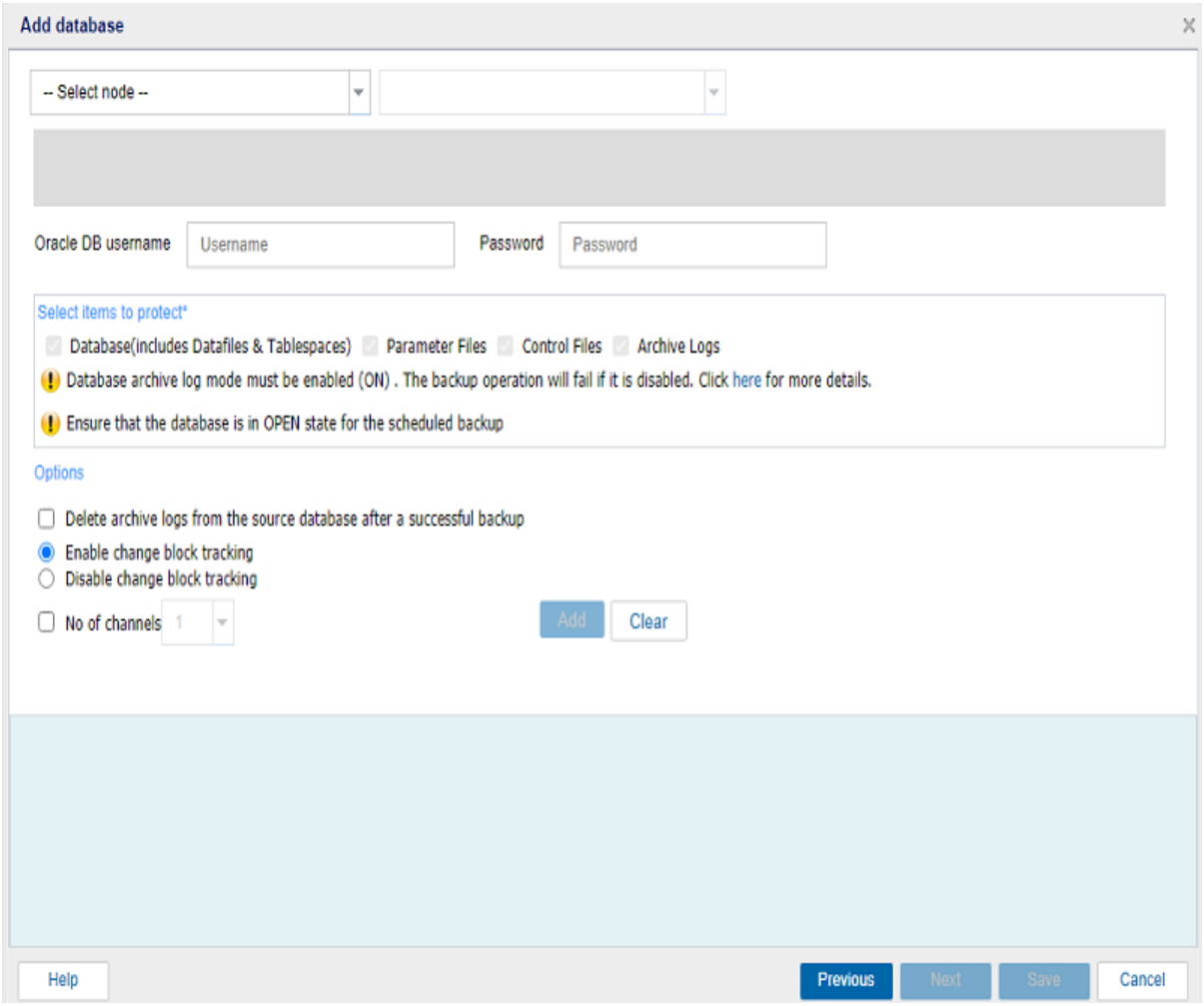
Note:

- Per modificare i nodi aggiunti dall'elenco, selezionare il nodo che si desidera modificare, quindi fare clic su **Modifica**.
- Per rimuovere i nodi aggiunti dall'elenco, selezionare i nodi che si desidera rimuovere, quindi fare clic su **Rimuovi**.
- Per rimuovere tutti i nodi aggiunti, fare clic su Rimuovi **tutto**.

i. Fare clic su **Avanti**.



7. Nella finestra di dialogo Aggiungi database, eseguire la seguenti operazioni:



a. Selezionare il nodo dall'elenco a discesa.

   Attendere fino alla visualizzazione dell'elenco dei database disponibili sull'host selezionato e l'attivazione dell'elenco a discesa.

b. Dall'elenco a discesa, selezionare una delle seguenti opzioni:

   Aggiungi nuovo database

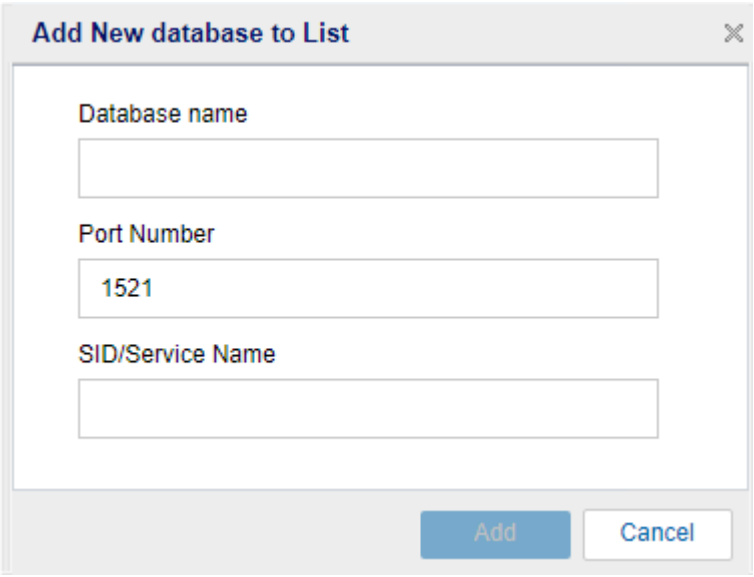
   Per aggiungere un nuovo database, procedere come segue:

   1. Selezionare l'opzione **Aggiungi nuovo database**.
   2. Nella finestra di dialogo Aggiungi nuovo database all'elenco, eseguire le operazioni seguenti, quindi fare clic su **Aggiungi**:

      - **Nome database/SID**: immettere il nome del database o il nome SID.
      - **Numero di porta:** immettere il numero di porta. Il valore pre-

definito della porta è 1521.

- **Nome servizio**: immettere il nome del servizio.



Il nuovo database viene aggiunto all'elenco a discesa.

Selezione del database esistente

Selezionare il database richiesto dall'elenco a discesa. Una volta selezionato, il database viene spostato al di fuori dell'elenco e visualizzato nel riquadro centrale.

Note:

- per evitare input multipli per ciascun database, raggruppare i database configurati con lo stesso nome utente e la stessa password.
- Per aggiungere diversi tipi di file ai database con credenziali diverse, selezionare i singoli database, quindi aggiungerli.
- Per rimuovere il database dal gruppo (nel riquadro centrale), procedere come segue:

  a. Fare clic sul nome del database.

     Verrà visualizzato un messaggio di conferma.

  b. Fare clic su **Sì** per confermare.

  Una volta rimosso, il database viene nuovamente aggiunto all'elenco a discesa.

c. Immettere le credenziali utente del sistema per il database Oracle.

Note:

- Tutti gli elementi da proteggere, quali database (inclusi file di dati e spazi tabella), file di controllo, file di parametri e registri archivio sono abilitati per impostazione predefinita.
- Assicurarsi di attivare il database ARCHIVELOG prima di attivare l'operazione di backup. Per verificare se la modalità di registro ARCHIVELOG è abilitata, consultare la sezione Verifica dei prerequisiti per il database Oracle. Se ARCHIVELOG non è abilitato, il processo di backup non riesce.

d. Per Opzioni, specificare quanto segue:

Eliminare i registri di archiviazione dal database di origine in seguito alla corretta esecuzione del backup

Consente di eliminare i registri di archiviazione dal database di origine in seguito al completamento di un backup.

Numero di canali

Consente di selezionare il numero di canali o di thread che si desidera creare per il processo di backup.

Nota: il numero massimo di canali supportati è 10.

Abilita traccia dei blocchi modificati

Consente di attivare la funzionalità di rilevamento dei blocchi di modifica. Utilizzare questa opzione per migliorare le prestazioni di RMAN. Consente all'utilità RMAN o al file binario di individuare più rapidamente i dati differenziali e di eseguire il processo di backup.

Disattiva rilevamento dei blocchi di modifica

Consente di disattivare la funzionalità di rilevamento dei blocchi di modifica.

Nota: Oracle supporta la funzionalità di disattivazione del rilevamento dei blocchi di modifica solo per Enterprise Edition (EE).

e. Fare clic su **Aggiungi**.

Tutti i database aggiunti vengono elencati.

Nota: dopo aver fatto clic sul pulsante Aggiungi, vengono verificate tutte le credenziali del database e i parametri del firewall.

f. Per aggiungere più database, seguire nuovamente la procedura. Tutti i database aggiunti vengono elencati.

g. Fare clic sul simbolo di espansione accanto all'indirizzo IP, quindi verificare i dettagli aggiunti.

Note:

- Per modificare i database aggiunti dall'elenco, selezionare il database che si desidera modificare, quindi fare clic su **Modifica**.
- Per rimuovere i database aggiunti dall'elenco, selezionare i database che si desidera rimuovere, quindi fare clic su **Rimuovi**.

8. Fare clic su **Salva**.

   Note:

   - È possibile aggiungere più nodi e più database.
   - Per rimuovere l'origine, selezionare la casella di controllo accanto all'origine aggiunta, quindi fare clic su **Rimuovi**.

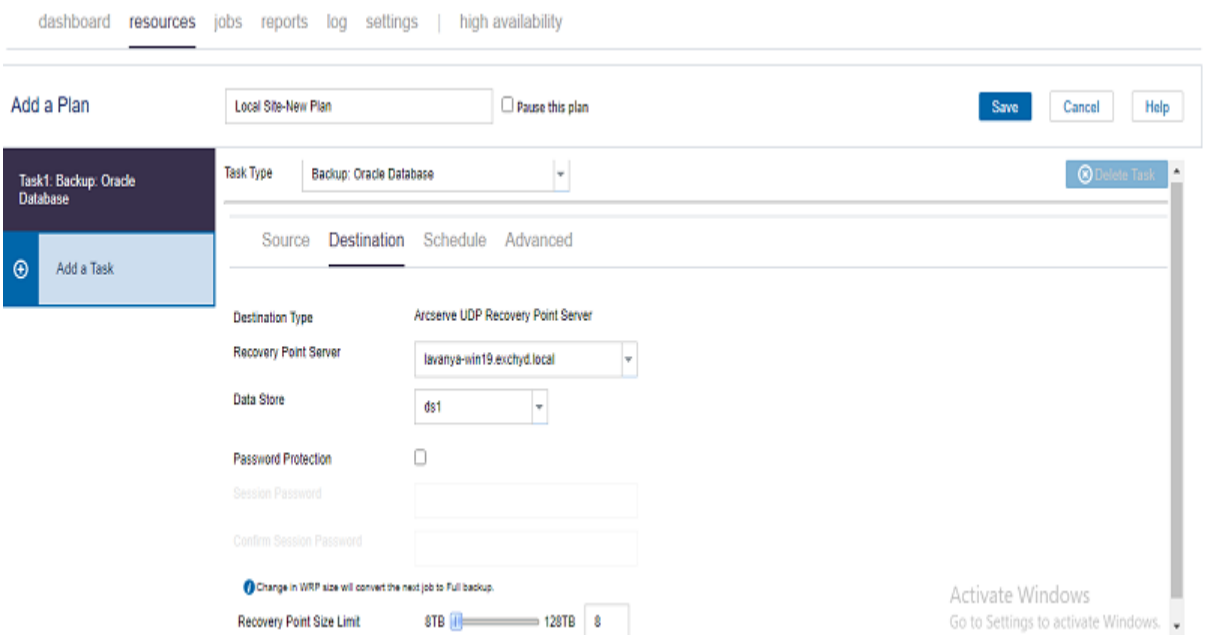
   L'origine viene specificata.

Definizione della destinazione

La destinazione è una posizione di archiviazione dei dati di backup. Per salvare il piano è necessario specificare almeno la destinazione.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Destinazione**.



2. Procedere come segue:
   - **Recovery Point Server**: dall'elenco a discesa, selezionare il Recovery Point Server (RPS) di destinazione.
   - **Archivio dati**: dall'elenco a discesa, selezionare l'archivio dati di destinazione.
   - **Protezione password**: selezionare la casella di controllo **Protezione password**, fornire la password di sessione, quindi digitare nuovamente la password di sessione per confermare.

     Nota: la password di sessione è facoltativa se la destinazione di backup è un archivio di dati RPS non crittografato.
   - **Limite dimensione punto di ripristino**: specifica la dimensione del Recovery Point Server per il backup. Impostare la dimensione del Recovery Point Server sulla scala.

     Intervallo: da 8 TB a 128 TB

   La destinazione viene specificata.

Definizione della pianificazione

La pagina Pianificazione consente di definire una pianificazione per le funzioni di backup, unione e limitazione della velocità ripetuta a intervalli specifici. Dopo aver definito una pianificazione, i processi verranno eseguiti automaticamente in base alla pianificazione. È possibile aggiungere pianificazioni multiple e fornire impostazioni di conservazione.

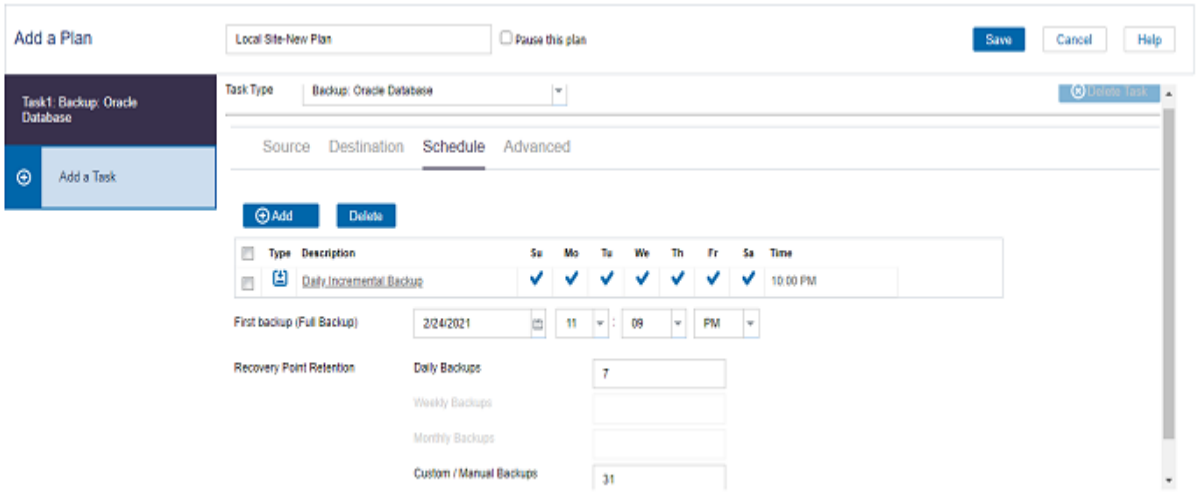
Una Pianificazione di backup fa riferimento a una pianificazione regolare ripetuta quotidianamente a intervalli regolari in base al numero di ore e minuti selezionati. Oltre alla pianificazione regolare, una pianificazione di backup consente inoltre di aggiungere pianificazioni giornaliere, settimanali e mensili.

Se il server RPS è la destinazione di backup, il valore predefinito è un backup incrementale giornaliero di tutti i tipi di file alle 22:00 ogni giorno.

È possibile modificare o eliminare una pianificazione del processo di backup.

Effettuare le operazioni seguenti:

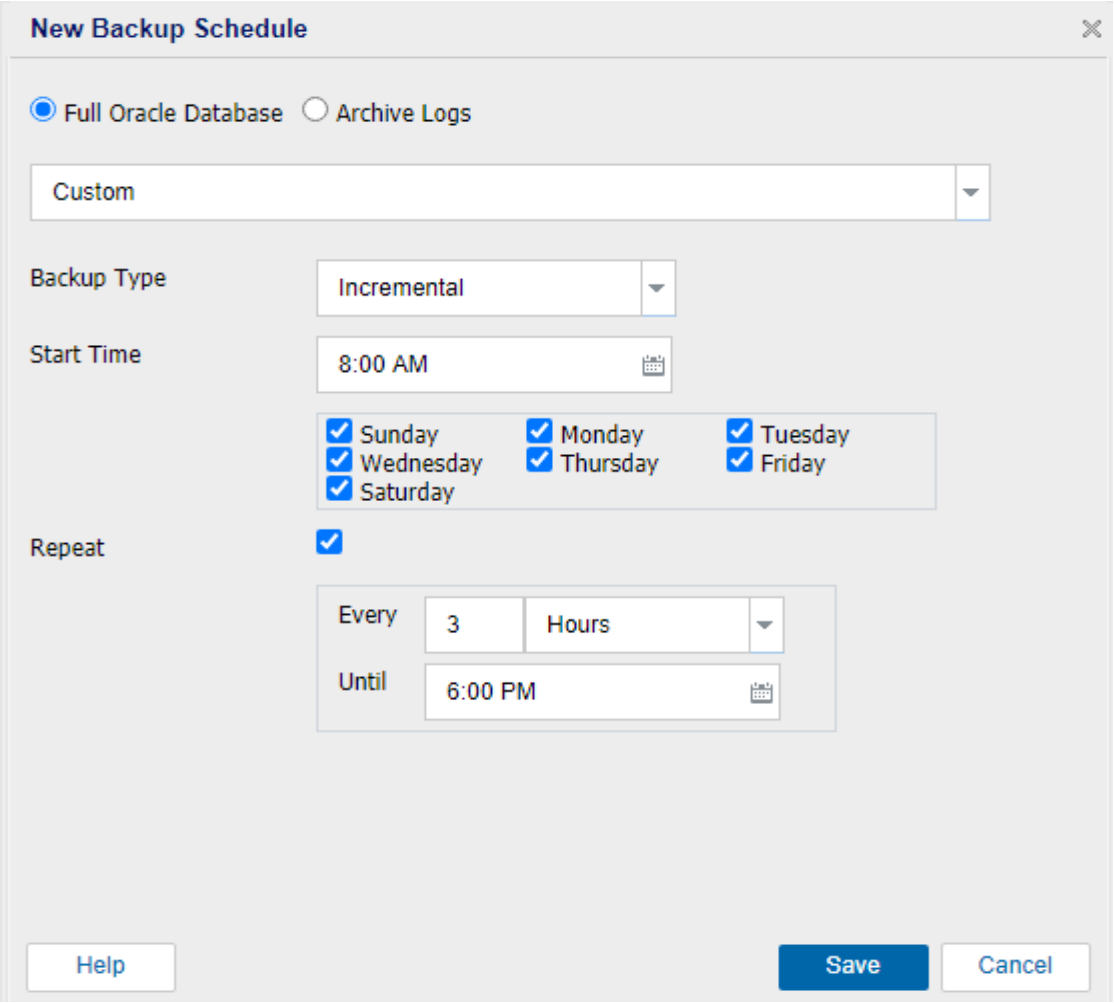
1. Fare clic sulla scheda **Pianificazione**, quindi aggiungere le pianificazioni di backup, unione e lettura del disco.



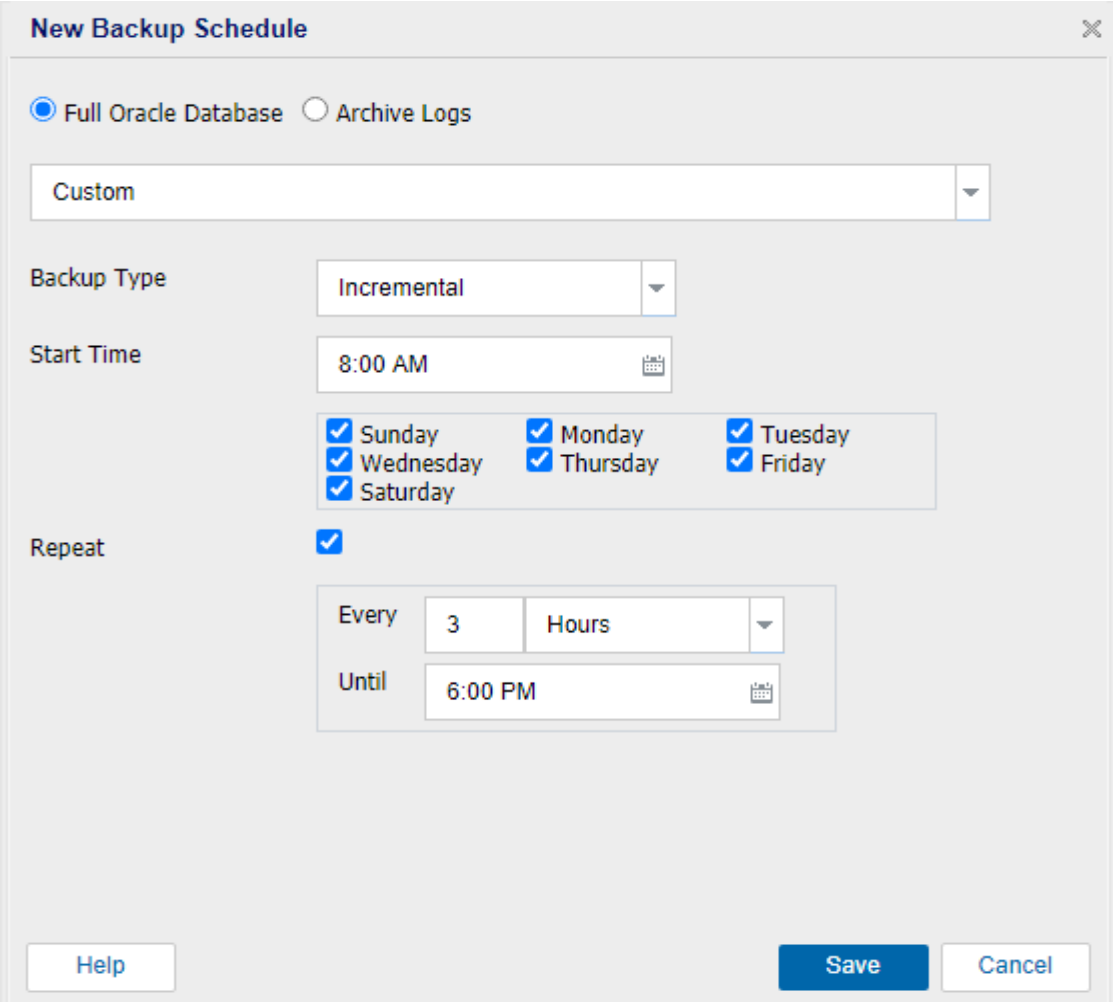
2. Per aggiungere un backup alla pianificazione, procedere come segue:
   a. Fare clic su **Aggiungi**, quindi selezionare l'opzione **Aggiungi pianificazione di backup**.

      Viene visualizzata la finestra di dialogo Nuova pianificazione di backup.

   b. Nella finestra di dialogo Nuova pianificazione di backup, selezionare una delle seguenti voci:



Database Oracle completo



Procedere come segue:

a. Dall'elenco a discesa, selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

Oraria

Specifica la pianificazione di backup eseguita una volta ogni ora.

Minuto

Consente di specificare la pianificazione del backup che si verifica con un intervallo di tempo minimo di 15 minuti.

b. Dall'elenco a discesa Tipo di backup, selezionare il tipo di backup.

Completo

Determina la pianificazione del backup per i backup completi (Tutti i tipi di file). In base alla pianificazione specificata, Arcserve UDP esegue il backup completo di tutti i tipi di file dal computer di origine. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni del backup.

Incrementale

Specifica la pianificazione dei backup incrementali.

In base alla pianificazione specificata, Arcserve UDP esegue il backup incrementale di tutti i tipi di file dall'ultimo backup eseguito correttamente. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

Nota: viene sempre eseguito il backup completo del file di controllo per qualsiasi tipo di backup.

c. Specificare l'ora di inizio del backup.

d. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

Nota: assicurarsi che il tempo di ripetizione della pianificazione non sia inferiore a 15 minuti.

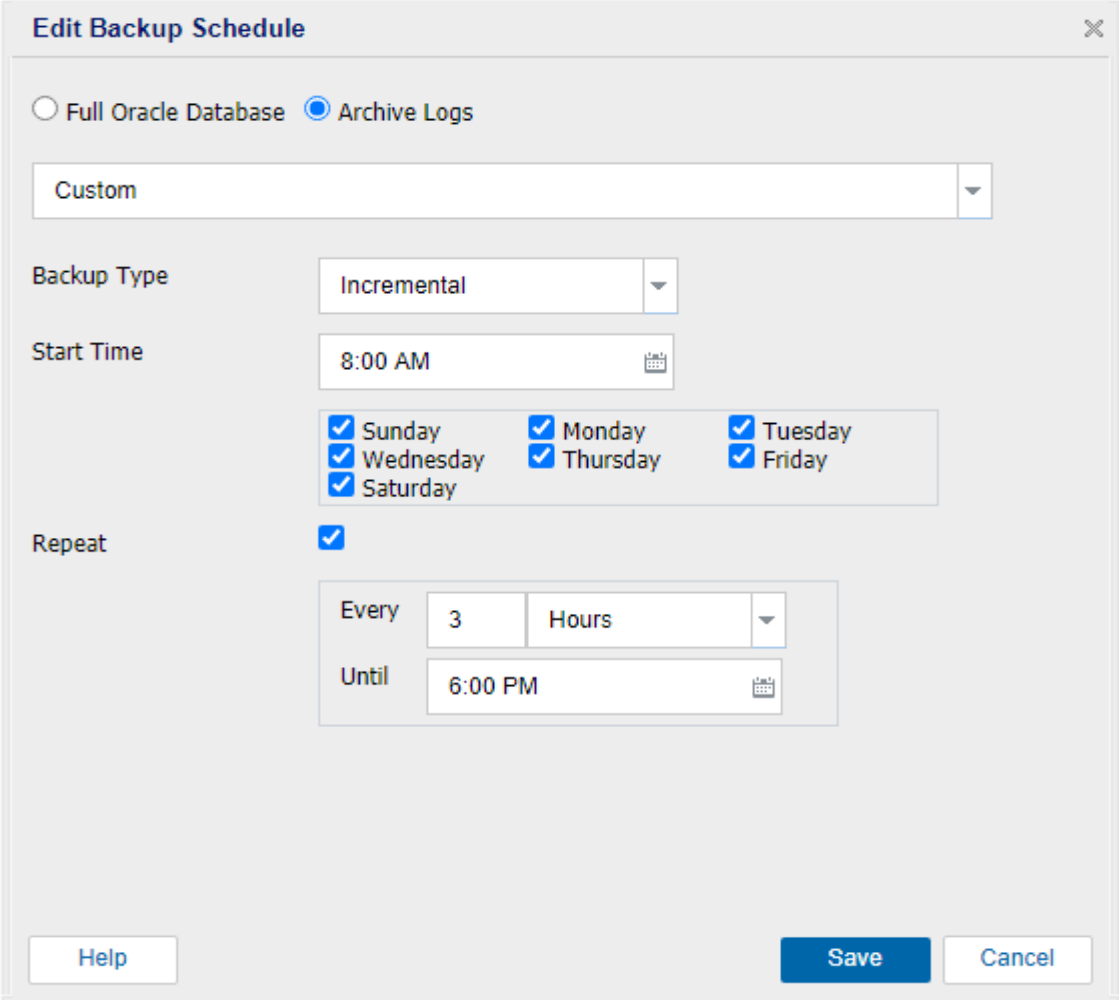
e. Se è stata selezionata l'opzione **Ogni ora** dall'elenco a discesa, procedere come segue:

1. Selezionare il tipo di backup dall'elenco a discesa Tipo di backup.
2. Specificare l'ora di inizio del backup.
3. Specificare l'ora di fine del di backup.
4. Selezionare l'intervallo di backup desiderato dall'elenco a discesa.

Nota: se si desidera personalizzare l'ora di ripetizione del backup, selezionare Personalizzato dall'elenco a discesa, quindi immettere il tempo in ore.

f. Fare clic su **Salva**.

Archiviazione dei registri



Procedere come segue:

a. Dall'elenco a discesa, selezionare una delle seguenti opzioni:

Personalizzato

Specifica la pianificazione di backup ripetuta più volte al giorno.

Ogni giorno

Specifica la pianificazione di backup eseguita una volta al giorno. Per impostazione predefinita, per il backup giornaliero vengono selezionati

tutti i giorni della settimana. Se non si desidera eseguire il processo di backup in un giorno specifico, deselezionare la relativa casella di controllo.

Ogni settimana

Specifica la pianificazione di backup eseguita una volta alla settimana.

Ogni mese

Specifica la pianificazione di backup eseguita una volta al mese.

Oraria

Specifica la pianificazione di backup eseguita una volta ogni ora.

Minuto

Consente di specificare la pianificazione del backup che si verifica con un intervallo di tempo minimo di 15 minuti.

b. Dall'elenco a discesa Tipo di backup, selezionare il tipo di backup.

Completo

Specifica la pianificazione per i backup del registro archiviazione completi. In base alla pianificazione specificata, Arcserve UDP esegue il backup completo di tutti i registri di archiviazione dal computer di origine. Il tempo impiegato da un backup completo dipende generalmente dalle dimensioni del backup.

Incrementale

Specifica la pianificazione per i backup del registro archiviazione incrementali.

In base alla pianificazione specificata, Arcserve UDP esegue il backup incrementale solo dei registri di archiviazione modificati dall'ultimo backup eseguito correttamente. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è la più ottimale.

c. Specificare l'ora di inizio del backup.

d. (Facoltativo) Selezionare la casella di controllo **Ripeti** e specificare la pianificazione di ripetizione.

Nota: assicurarsi che il tempo di ripetizione della pianificazione non sia inferiore a 15 minuti.

e. Se è stata selezionata l'opzione **Ogni ora** dall'elenco a discesa, procedere come segue:

   1. Selezionare il tipo di backup dall'elenco a discesa Tipo di backup.
   2. Specificare l'ora di inizio del backup.
   3. Specificare l'ora di fine del di backup.
   4. Selezionare l'intervallo di backup desiderato dall'elenco a discesa.

      Nota: se si desidera personalizzare l'ora di ripetizione del backup, selezionare **Personalizzato** dall'elenco a discesa, quindi immettere il tempo in ore.

f. Fare clic su **Salva**.

La pianificazione di backup specificata viene visualizzata nella pagina Pianificazione.

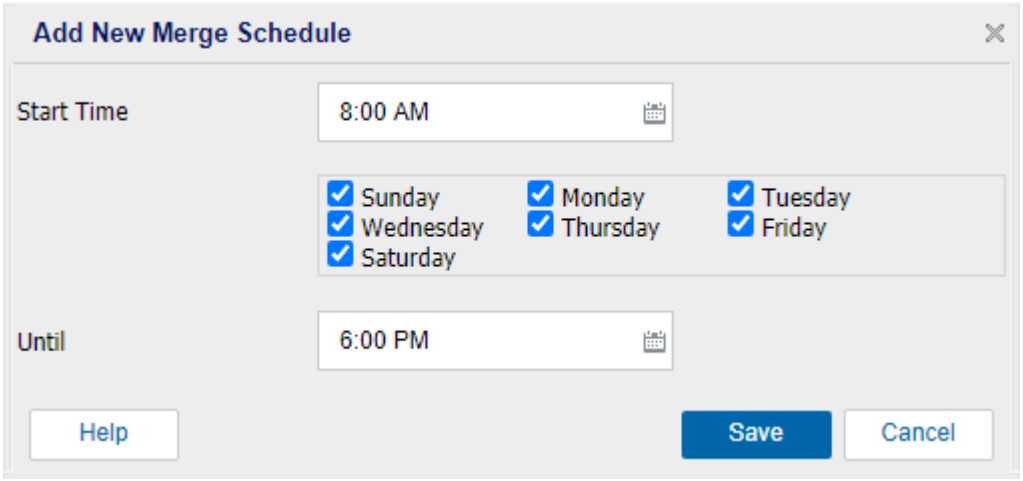
3. Per aggiungere una pianificazione di unione, procedere come segue:

   a. Fare clic su **Aggiungi**, quindi selezionare l'opzione **Aggiungi pianificazione di unione**.

      La finestra di dialogo Aggiungi nuova pianificazione di unione viene chiusa.

   b. Nella finestra di dialogo Aggiungi nuova pianificazione di unione, procedere come segue:

      - **Ora di inizio**: specificare l'ora di inizio per l'avvio del processo di unione.
      - **Fino a**: specificare l'ora di inizio per il processo di unione.



   c. Fare clic su **Salva**.

La pianificazione di unione specificata viene visualizzata nella pagina Pianificazione.

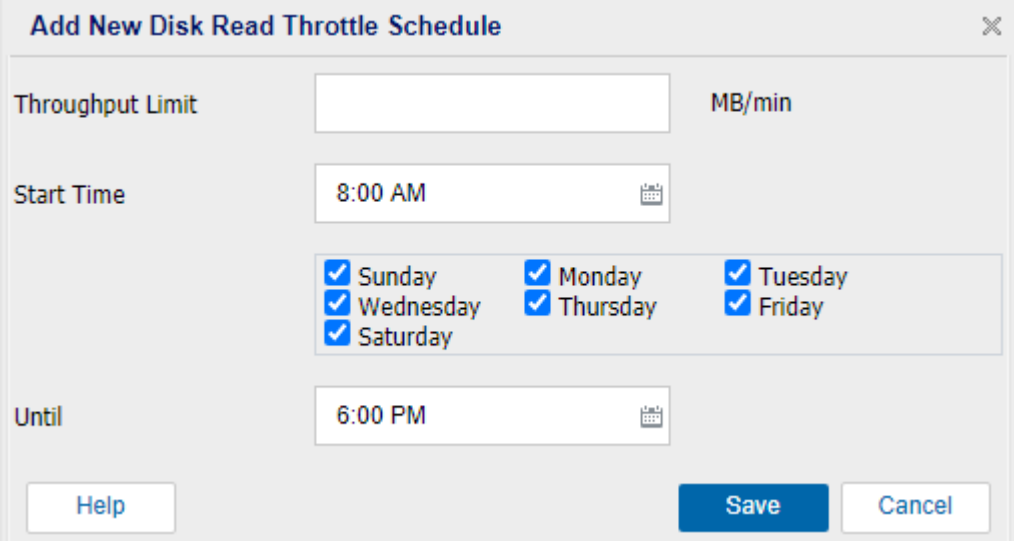
4. Per aggiungere una pianificazione del limite di velocità di lettura del disco, procedere come segue:

   a. Fare clic su **Aggiungi**, quindi selezionare l'opzione **Aggiungi pianificazione di limitazione di lettura del disco**.

      Viene visualizzata la finestra di dialogo Aggiungi nuova pianificazione della limitazione di lettura del disco.

   b. Nella finestra di dialogo Aggiungi pianificazione di limitazione di lettura del disco, procedere come segue:

      - **Limite di velocità effettiva**: specificare il limite di velocità effettiva in MB per unità di minuti.
      - **Ora di inizio**: specificare l'ora di inizio per l'avvio del processo di velocità effettiva del backup.
      - **Fino a**: specificare l'ora di fine per il processo di velocità effettiva del backup.



   c. Fare clic su **Salva**.

   La pianificazione della limitazione di lettura del disco specificata viene visualizzata nella pagina Pianificazione.

5. Specificare l'ora di inizio per il backup pianificato.



Nota: la schermata precedente non è valida per i backup RMAN.

6. Specificare le impostazioni di memorizzazione dei punti di ripristino per la pianificazione Personalizzata, Giornaliera, Settimanale e Mensile.

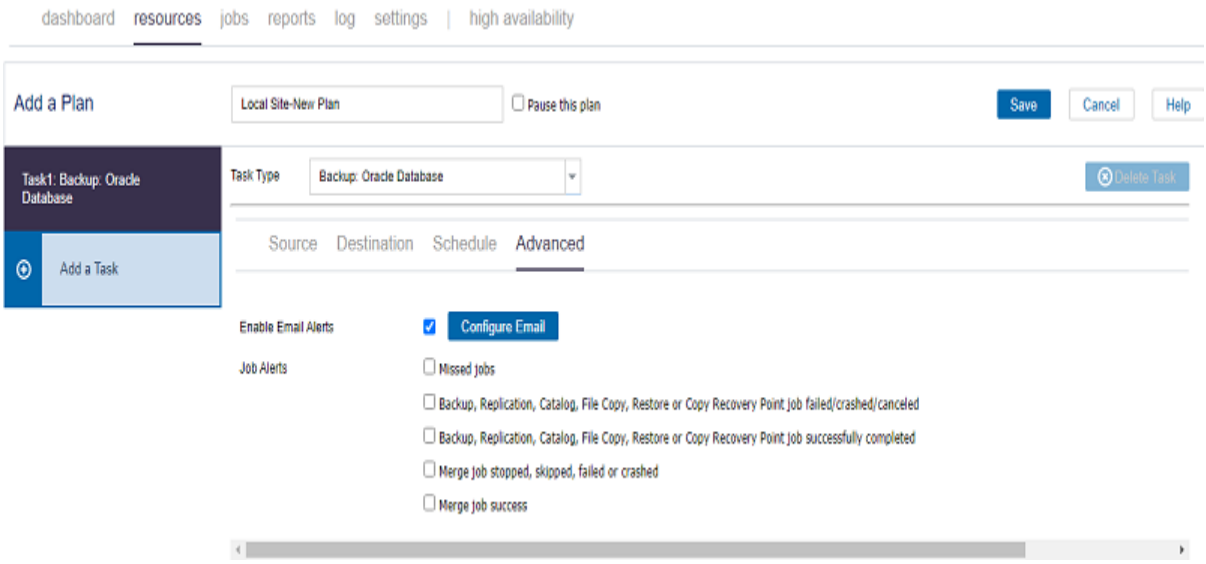
   Le opzioni verranno abilitate se è stata aggiunta la pianificazione di backup corrispondente. Se le impostazioni di memorizzazione vengono modificate sulla pagina, tali modifiche verranno visualizzate nella finestra di dialogo Pianificazione di backup.



   Viene specificata la pianificazione.

Definizione delle impostazioni avanzate

La scheda Avanzate consente di specificare alcune impostazioni avanzate per il processo di backup.



Effettuare le operazioni seguenti:

1. Specificare i seguenti dettagli:

   Abilitazione degli avvisi di posta elettronica

   Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere mediante posta elettronica. Quando si seleziona questa opzione, le opzioni seguenti vengono abilitate per la selezione.

   Configurazione della posta elettronica

   Consente di configurare le impostazioni di posta elettronica.

   Per configurare i dettagli del server di posta elettronica e del server proxy, fare clic su **Configura posta elettronica**.

   Avvisi di processo

   Consente di specificare i tipi di messaggi di posta elettronica del processo che si desidera ricevere.

2. Fare clic su **Salva**.

Le impostazioni avanzate sono state specificate.

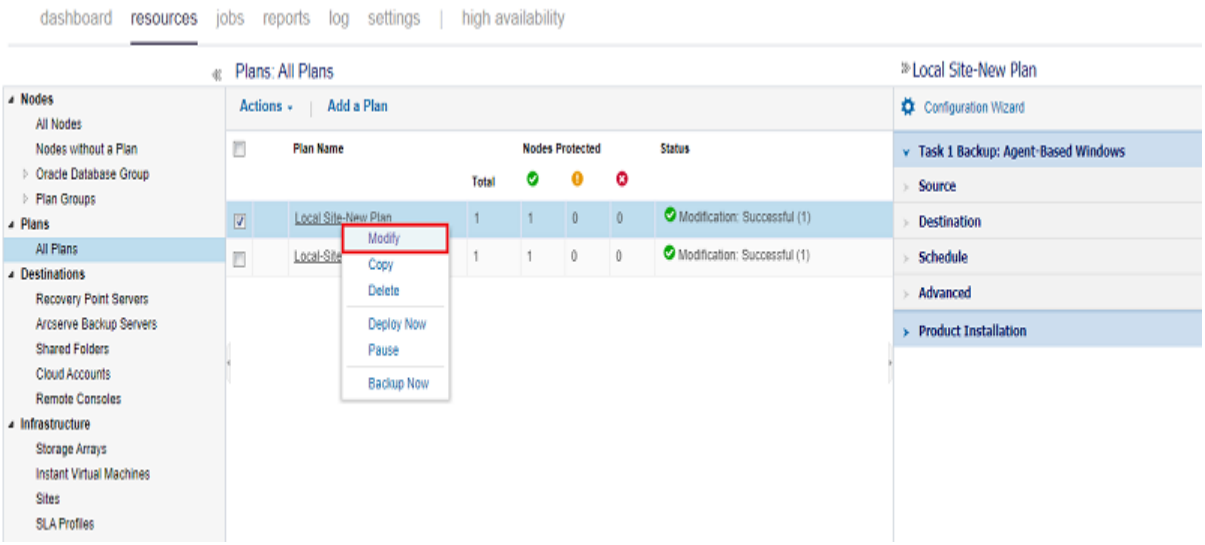
Aggiunta di un'attività Assured Recovery al piano

L'aggiunta di un'attività Assured Recovery consente di aggiungere un'attività Assured Recovery a un piano di replica o di backup esistente. Ciascuna attività consiste di parametri che definiscono l'origine, le impostazioni di test, la pianificazione e le impostazioni avanzate. Creare un'attività Assured Recovery in base all'attività di backup/replica per verificare l'accessibilità e il valore di Assured Recovery dai dati, nonché per eseguire la verifica dell'integrità dei dati.

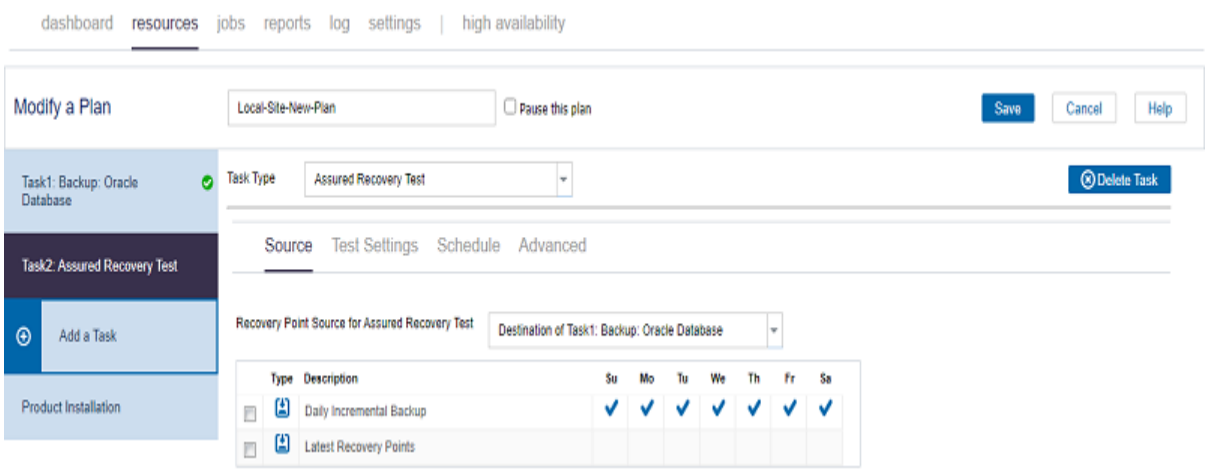
Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della console.
2. Dal riquadro sinistro, accedere a **Piani**, quindi fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Dal riquadro centrale, fare clic con il pulsante destro del mouse sul piano di backup esistente, quindi selezionare **Modifica**.



4. Nella pagina Modifica un piano, fare clic su **Aggiungi un'attività** dal riquadro sinistro.



5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se il piano viene interrotto, il processo Assured Recovery non verrà avviato. Quando il piano viene ripreso, il processo Assured Recovery non viene ripreso automaticamente. Per avviare il processo Assured Recovery è necessario eseguire un altro processo di backup manualmente.

6. Dall'elenco a discesa Tipo di attività, selezionare **Verifica Assured Recovery**.
7. Specificare i dettagli Origine, Impostazioni verifica, Pianificazione e Avanzate.
8. Fare clic su **Salva**

   Le modifiche vengono salvate e l'attività Assured Recovery viene distribuita automaticamente.

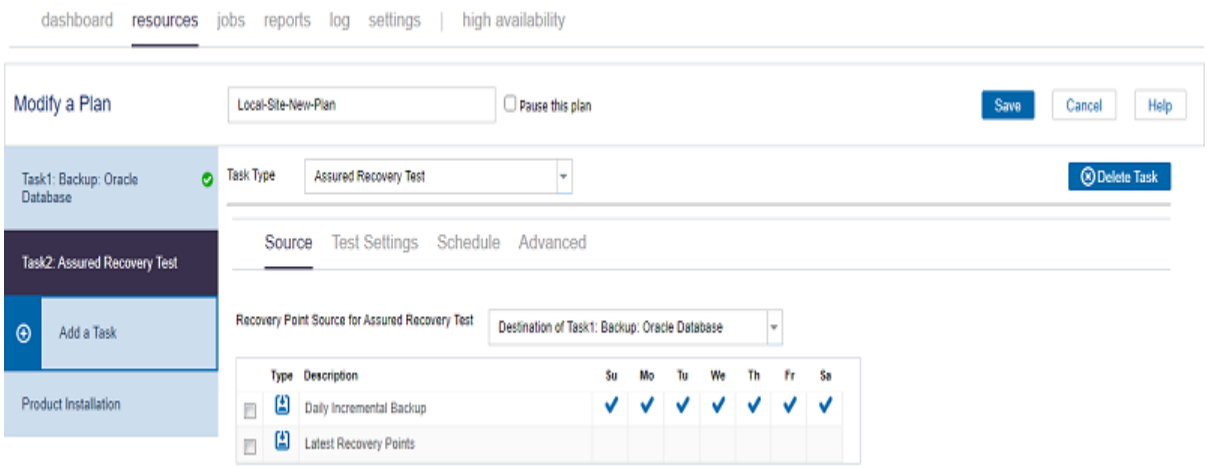
   Nota: per controllare e verificare l'integrità dei dati di backup di Oracle quali file di controllo, file di dati, registri di archivio e file SP, il processo Assured Recovery esegue il comando RMAN di convalida del ripristino sul Recovery Point Server.

Definizione dell'origine

La scheda Origine consente di specificare i punti di ripristino di origine che si desidera proteggere.

Effettuare le operazioni seguenti:

1. Nella scheda Origine, dall'elenco a discesa Origine punto di ripristino per verifica Assured Recovery, selezionare l'opzione desiderata.



2. Selezionare i tipi di punti di ripristino per la verifica Assured Recovery. È possibile selezionare una delle due opzioni seguenti:

   - Verifica Assured Recovery da tipi di backup selezionati

     È possibile selezionare Backup giornalieri, Backup settimanali e Backup mensili. Le opzioni relative alla frequenza giornaliera, settimanale o mensile sono abilitate in base alla pianificazione del backup di origine. Ad esempio, se per il backup di origine è pianificato soltanto un backup mensile, per la verifica Assured Recovery da tipi di backup selezionati sono attivi soltanto i backup mensili.

   - Verifica Assured Recovery dai punti di ripristino più recenti

L'origine viene specificata

Passaggi successivi:

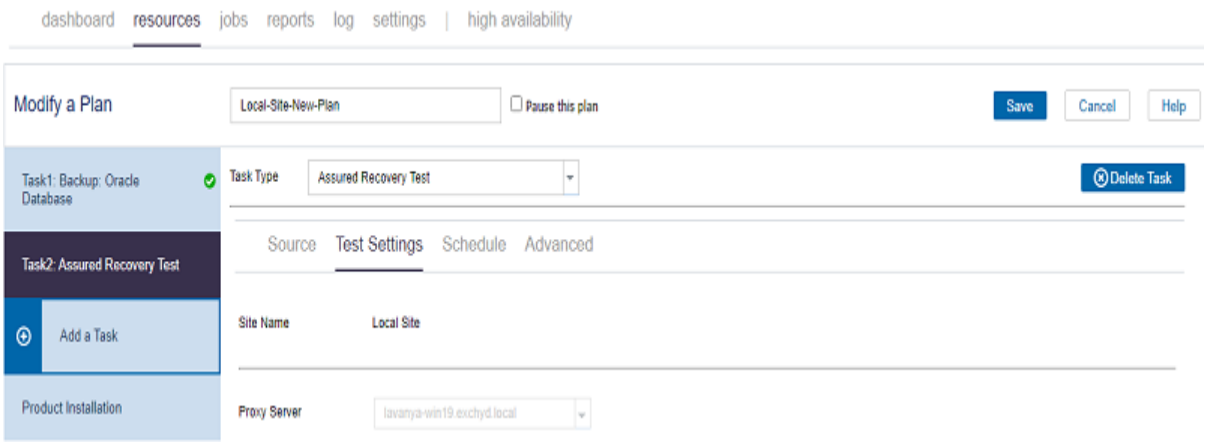
- Definizione delle impostazioni di verifica
- Definizione di una pianificazione del processo di verifica Assured Recovery
- Definizione delle impostazioni avanzate

Definizione delle impostazioni di verifica

La scheda Impostazioni verifica consente di specificare il server proxy.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Impostazioni verifica**.



2. Dall'elenco a discesa Server proxy, selezionare il nodo proxy.

   Nota: per Oracle, il Recovery Point Server funge da server proxy durante la verifica Assured Recovery.

   Le impostazioni di verifica sono state specificate.

Passaggi successivi:

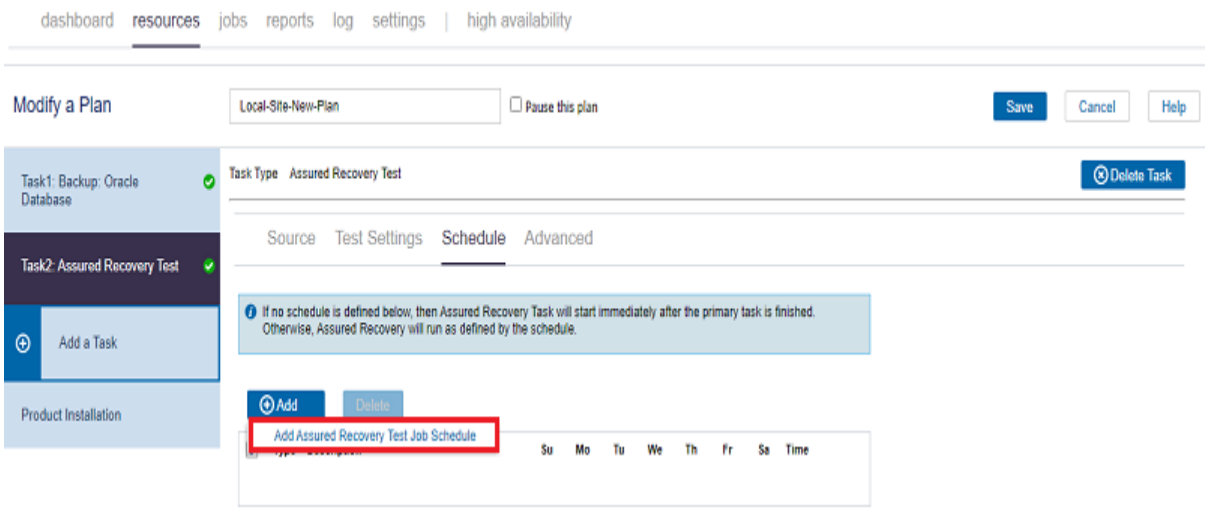
- Definizione di una pianificazione del processo di verifica Assured Recovery
- Definizione delle impostazioni avanzate

Definizione di una pianificazione del processo di verifica Assured Recovery

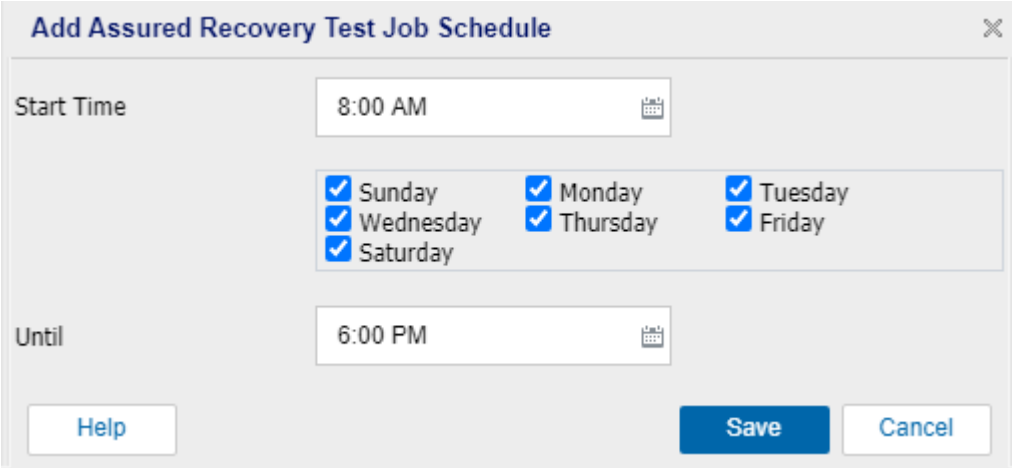
La scheda Pianificazione consente di specificare la pianificazione del processo di verifica di Assured Recovery. Se non si specifica una pianificazione, l'attività viene avviata immediatamente una volta completata l'attività principale.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Pianificazione**.



2. Fare clic su **Aggiungi**, quindi selezionare **Aggiungi pianificazione processo di verifica Assured Recovery**.
3. Nella finestra di dialogo Aggiungi pianificazione processo di verifica Assured Recovery, eseguire le operazioni seguenti, quindi fare clic su **Salva**:
   - **Ora di inizio**: specificare l'ora di inizio per avviare il processo di verifica Assured Recovery.
   - **Fino a**: specificare l'ora di fine per il processo di verifica Assured Recovery.



Il processo di verifica Assured Recovery viene pianificato e visualizzato nella pagina Pianificazione.

Note:

- Se l'origine Assured Recovery è Punti di ripristino più recenti e si abilita la pianificazione di Assured Recovery, il valore predefinito è 1. Di conseguenza, viene verificato il più recente per impostazione predefinita.

  Se il valore è <=0, vengono provati tutti i punti di ripristino non verificati.

- Se l'origine Assured Recovery è Giornaliero/Settimanale/Mensile e si abilita la pianificazione di Assured Recovery, il valore predefinito è 9 (7 giornalieri + 1 settimanale + 1 mensile).

  Se il valore è <=0, vengono provati tutti i punti di ripristino non verificati.

- Se non si desidera utilizzare il valore predefinito, è possibile aggiungere una chiave del Registro di sistema DWORD a 32 bit nella posizione seguente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AssuredRecovery\MaxNumberOfRecoveryPoint

Passaggio successivo:

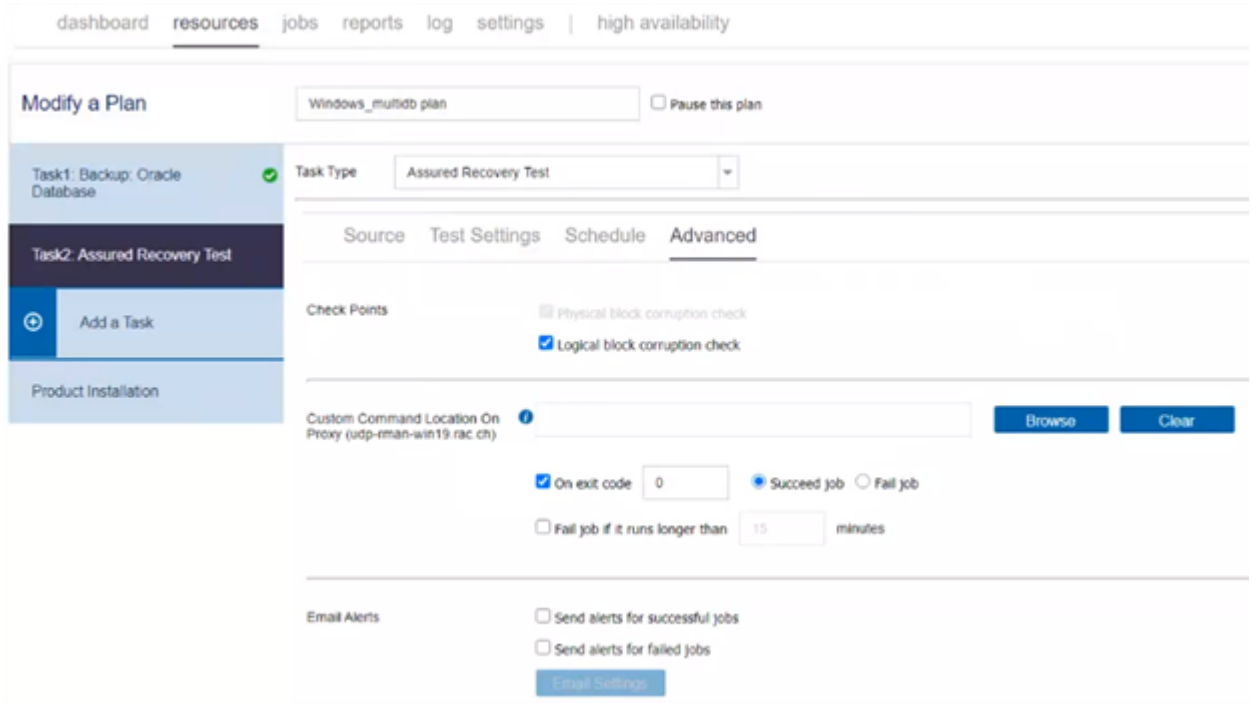
- Definizione delle impostazioni avanzate

Definizione delle impostazioni avanzate

La scheda Avanzate consente di applicare altre impostazioni necessarie per completare il piano. Questo parametro è facoltativo se non si desidera aggiungere ulteriori impostazioni.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Avanzate**.



2. Procedere come segue:

   Punti di verifica

   Verifica del danneggiamento del blocco fisico

   RMAN rileva solo i blocchi fisicamente danneggiati con ogni backup e archivia le informazioni relative al danneggiamento nel file di controllo e nel file alert.log. Per impostazione predefinita, l'opzione **Verifica del danneggiamento del blocco fisico** è attivata.

   Verifica del danneggiamento del blocco logico

   Per impostazione predefinita, RMAN non rileva automaticamente i blocchi danneggiati dal punto di vista logico. Selezionare la casella di controllo **Verifica del danneggiamento del blocco logico** insieme a quello fisico. Se viene rilevato un danneggiamento logico, RMAN archivia le informazioni sul danneggiamento nel file alert.log.

Posizione del comando personalizzato su proxy

Nota: questa opzione non è visibile se è stato selezionato il backup o la replica di Linux basati sull'agente come Origine punto di ripristino per la verifica di Assured Recovery.

Specifica lo script personalizzato archiviato sul server proxy. È possibile esplorare le informazioni sul volume del server proxy. Se è selezionato il tipo Assured Recovery del computer virtuale, lo script viene copiato nel computer virtuale ed eseguito con l'avvio del computer virtuale. Se è selezionato il tipo Assured Recovery IVHD, lo script viene eseguito sul server proxy.

Nota: il processo Assured Recovery è in grado di supportare soltanto lo script bat eseguibile di Windows o il file binario eseguibile. Tuttavia, questa restrizione non limita l'utilizzo del processo di Assured Recovery. È possibile utilizzare uno script in batch di Windows per avviare lo script Powershell, ad esempio test.bat con il contenuto seguente:

Powershell.exe -NoProfile -ExecutionPolicy ByPass -Command "& '%ScriptPath%\AR-check.ps1'"

I seguenti argomenti vengono trasmessi allo script in base alle proprie esigenze.

- set PlanName=%1%

- set NodeName=%2%

- set ProxyServer=%3%

- set RecoveryPointName=%3%

- set MountPointRootPathName=%5% (applicabile solo al tipo di test Disco virtuale istantaneo)

Di conseguenza, lo script bat viene richiamato ed eseguito come indicato sotto:

Per il tipo di test Computer virtuale istantaneo:

"%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName

Per il tipo di test Disco virtuale istantaneo:

%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName MountPointRootPathName

Per codice di uscita

Specifica il codice di uscita in caso di esito positivo o di errore del processo.

Processo Procedura completata

Specifica che il processo Assured Recovery viene impostato su Procedura completata quando lo script restituisce il codice di uscita.

Processo con errore

Specifica che il processo Assured Recovery viene impostato sulla restituzione di un errore se lo script restituisce il codice di uscita.

Interrompi processo se richiede più di

Specifica se l'esecuzione dello script richiede tempi più lunghi rispetto al tempo specificato.

Valore predefinito: 15 minuti.

Avvisi di posta elettronica

Consente di abilitare avvisi di posta elettronica. È possibile configurare le impostazioni di posta elettronica e specificare i tipi di avvisi che si desidera ricevere in un messaggio di posta elettronica.

- Se si desidera ricevere avvisi di posta elettronica per garantire la riuscita del processo Assured Recovery, selezionare la casella di controllo **Invia avvisi per processi completati**.
- Se si desidera ricevere avvisi di posta elettronica in caso di errore del processo Assured Recovery, selezionare la casella di controllo **Invia avvisi per processi non riusciti**.

  Nota: non è disponibile per i processi in esecuzione con il server di backup Linux.

Impostazioni di posta elettronica

Consente di configurare le impostazioni di posta elettronica.

Per configurare i dettagli del server di posta elettronica e del server proxy, fare clic su **Impostazioni di posta elettronica**. Per ulteriori informazioni sulla configurazione delle impostazioni di posta elettronica, consultare la sezione Configurazione di posta elettronica e avvisi.

Le impostazioni avanzate sono state specificate.

(Facoltativo) Esecuzione di un backup manuale

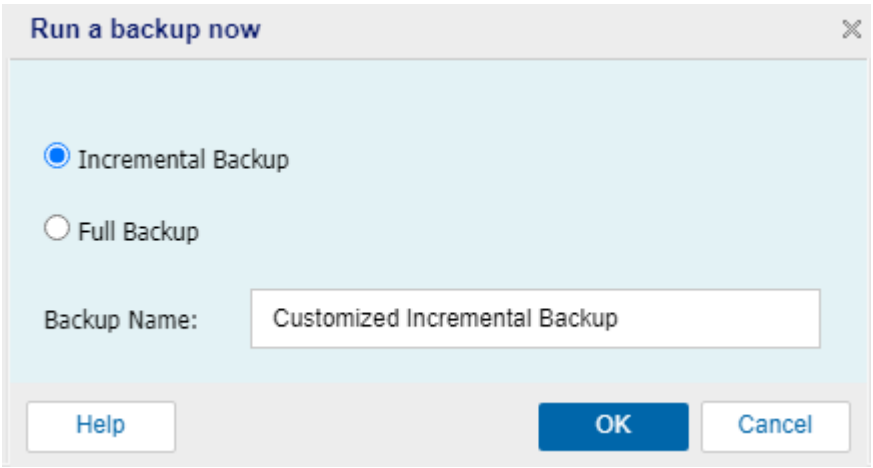
In genere, i backup vengono eseguiti automaticamente e vengono controllati attraverso le impostazioni di pianificazione. In aggiunta al backup pianificato, un backup manuale fornisce la possibilità di eseguire il backup dei nodi a seconda delle esigenze. Se ad esempio si dispone di una pianificazione di ripetizione per backup completi e incrementali e si desidera apportare modifiche sostanziali al computer, è necessario eseguire un backup manuale immediato senza attendere l'esecuzione del backup pianificato successivo.

Effettuare le operazioni seguenti:

1. Accedere alla console Arcserve UDP.
2. Accedere a **Risorse** > **Piano** > **Tutti i piani**.

   Nel riquadro centrale viene visualizzato un elenco di tutti i piani.
3. Fare clic con il pulsante destro del mouse sul piano, quindi selezionare **Esegui backup**.

   Verrà visualizzata la finestra di dialogo Esegui un backup immediato.
4. Nella finestra di dialogo Esegui un backup immediato, selezionare il tipo di backup che si desidera eseguire, quindi specificare il nome del backup, se necessario.



Le opzioni disponibili sono:

Backup incrementale

Avvia un backup incrementale del computer. Un backup incrementale esegue il backup solo dei blocchi modificati dopo l'ultimo backup.

Nota: se si esegue un backup per la prima volta, il backup completo viene avviato automaticamente anche se è stata selezionata l'opzione Backup incrementale.

I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup con dimensioni molto ridotte. Questa modalità di esecuzione backup è ottimale.

Backup completo

Avvia un backup completo dell'intero computer o dei volumi selezionati.

Note:

- È inoltre possibile eseguire il backup manualmente dalla pagina Nodi.
- Se non viene specificato alcun nome di backup, per impostazione predefinita viene automaticamente denominato Backup completo personalizzato o Backup incrementale.

5. Fare clic su **OK**.

   Viene visualizzata la finestra di dialogo Informazioni avanzamento.

6. Attendere il completamento del processo di backup, quindi fare clic su **OK**.
7. Per monitorare i processi di backup, accedere a **Processi** > **Processi in corso**.

   Attendere fino al completamento del primo processo.

   Nota: è possibile eseguire un solo processo alla volta. Se si tenta di avviare manualmente un processo di backup durante l'esecuzione di un altro processo, verrà visualizzato un messaggio di avviso indicante che un altro processo è in esecuzione, per cui sarà necessario riprovare in un momento successivo.

   Il backup manuale è stato eseguito correttamente.

Ripristino di un database Oracle mediante RMAN

È possibile ripristinare l'intero database Oracle o eseguire il recupero granulare di spazi tabella e tabelle. È inoltre possibile ripristinare il database dal punto di ripristino nella posizione di base Oracle, in una posizione alternativa o in un nodo.

Per ripristinare il database Oracle, procedere come segue:

1. Selezione degli elementi del database Oracle da ripristinare
2. Definizione delle opzioni di ripristino

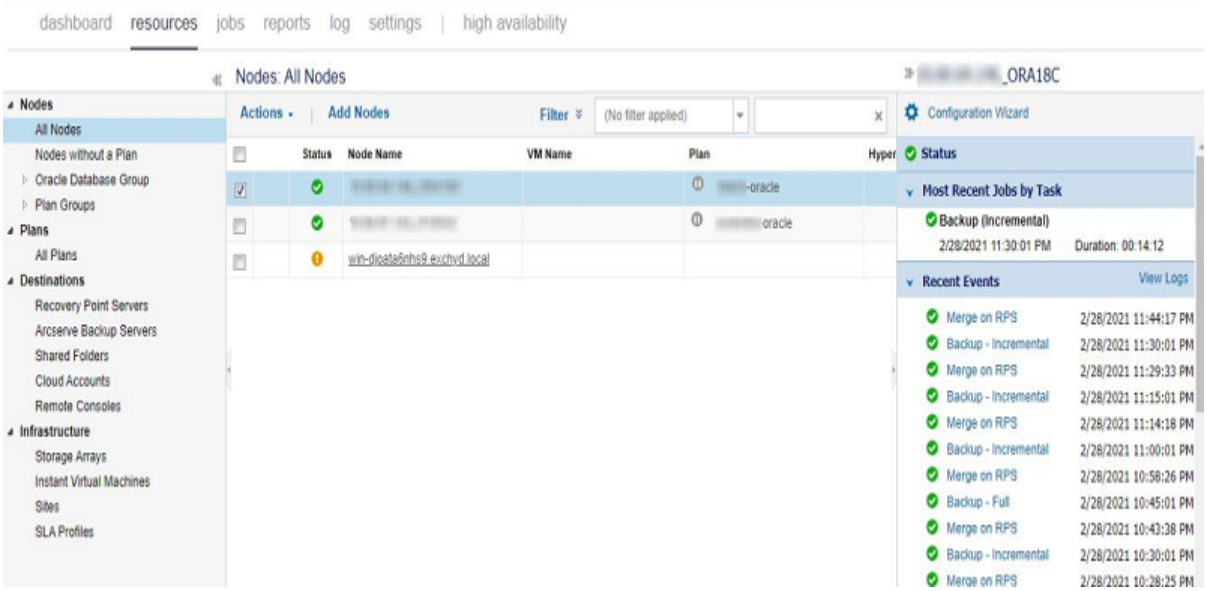
Selezione degli elementi del database Oracle da ripristinare

In questa sezione vengono fornite informazioni su come ricercare e selezionare gli elementi del database Oracle da ripristinare.

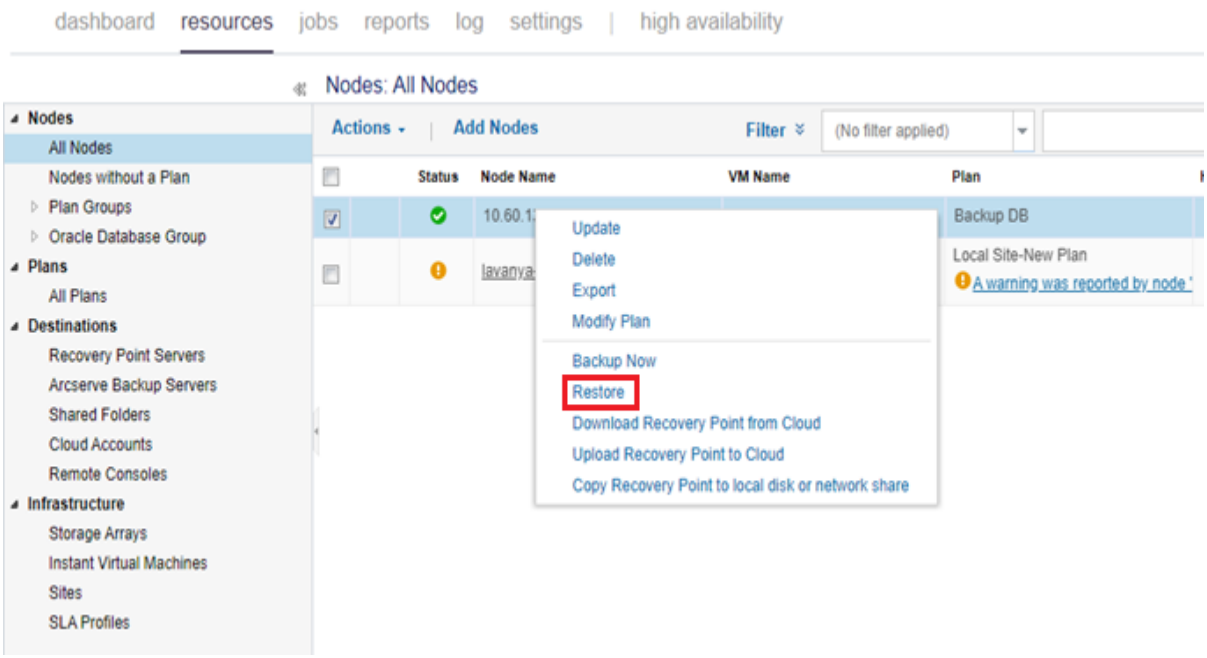
Effettuare le operazioni seguenti:

1. Accedere all'account della console UDP.
2. Dalla pagina della console UDP, fare clic sulla scheda **Risorse.**
3. Dal riquadro sinistro, accedere a **Nodi** > **Tutti i nodi**.

   L'elenco dei nodi esistenti viene visualizzato nel riquadro centrale.



4. Fare clic con il pulsante destro del mouse sul nodo Oracle, quindi selezionare l'opzione **Ripristina**.

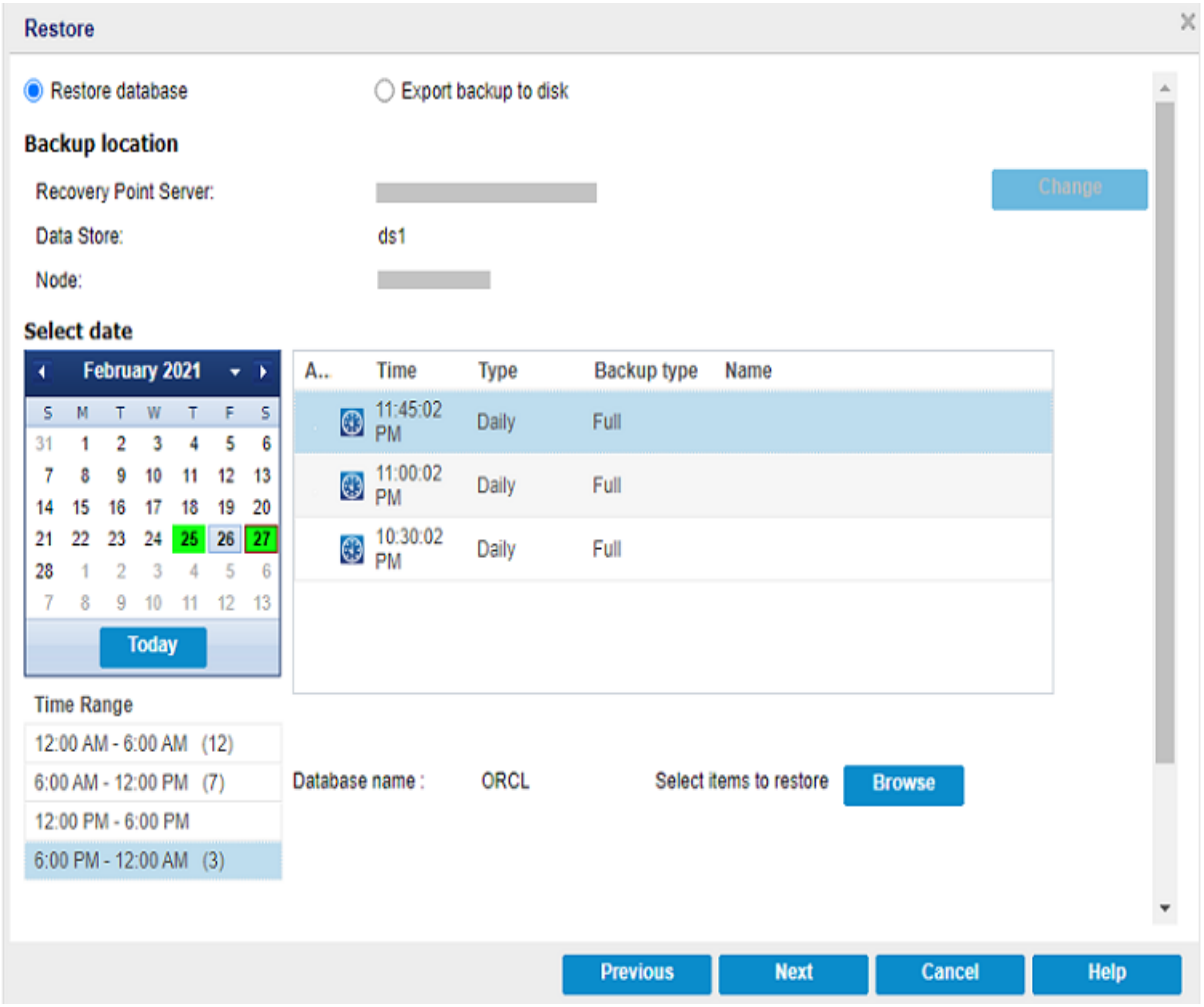


L'utente verrà indirizzato automaticamente al nodo dell'agente e verrà visualizzata la procedura guidata di ripristino.

5. Nella procedura guidata di ripristino, selezionare una delle seguenti voci:

   Ripristina database

   Il ripristino del database include i passaggi sia per il ripristino completo del database che per il ripristino granulare.



Per selezionare gli elementi del database Oracle, procedere come segue:

a. (Facoltativo) Per modificare i dettagli della posizione di backup, fare clic su **Modifica**.

   Nota: questa opzione è valida solo quando è selezionata l'opzione Esporta backup su disco.

b. Dalla sezione Seleziona data, selezionare una data.

   In base alla selezione, viene visualizzato l'elenco dei punti di ripristino del backup con l'ora del backup, il tipo di backup eseguito (completo o incrementale) e il nome del backup.

c. Dall'elenco dei punti di ripristino di backup, selezionare un punto di ripristino di backup che si desidera ripristinare.

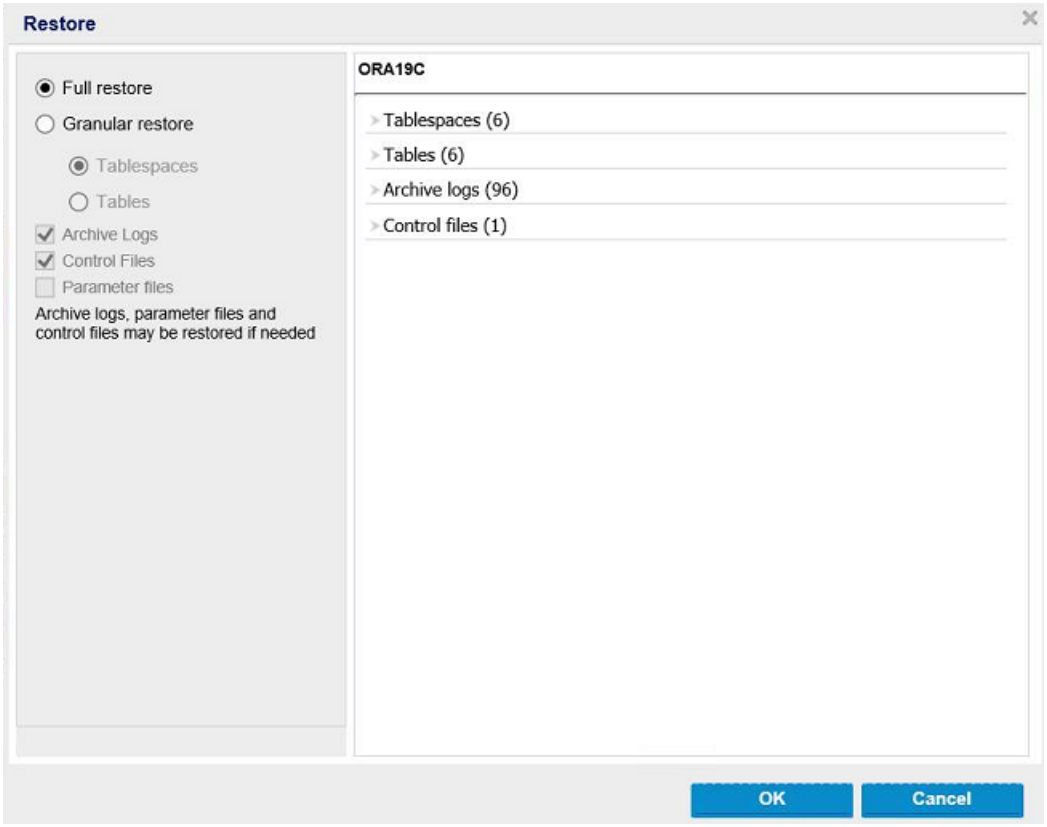
   Nota: per impostazione predefinita, viene selezionato il punto di ripristino più recente.

d. Per selezionare gli elementi del database, procedere come segue:

- Fare clic sul pulsante **Sfoglia**.

  Viene visualizzata la finestra di dialogo Ripristina.

- Nella finestra di dialogo Ripristina, eseguire la seguenti operazioni:



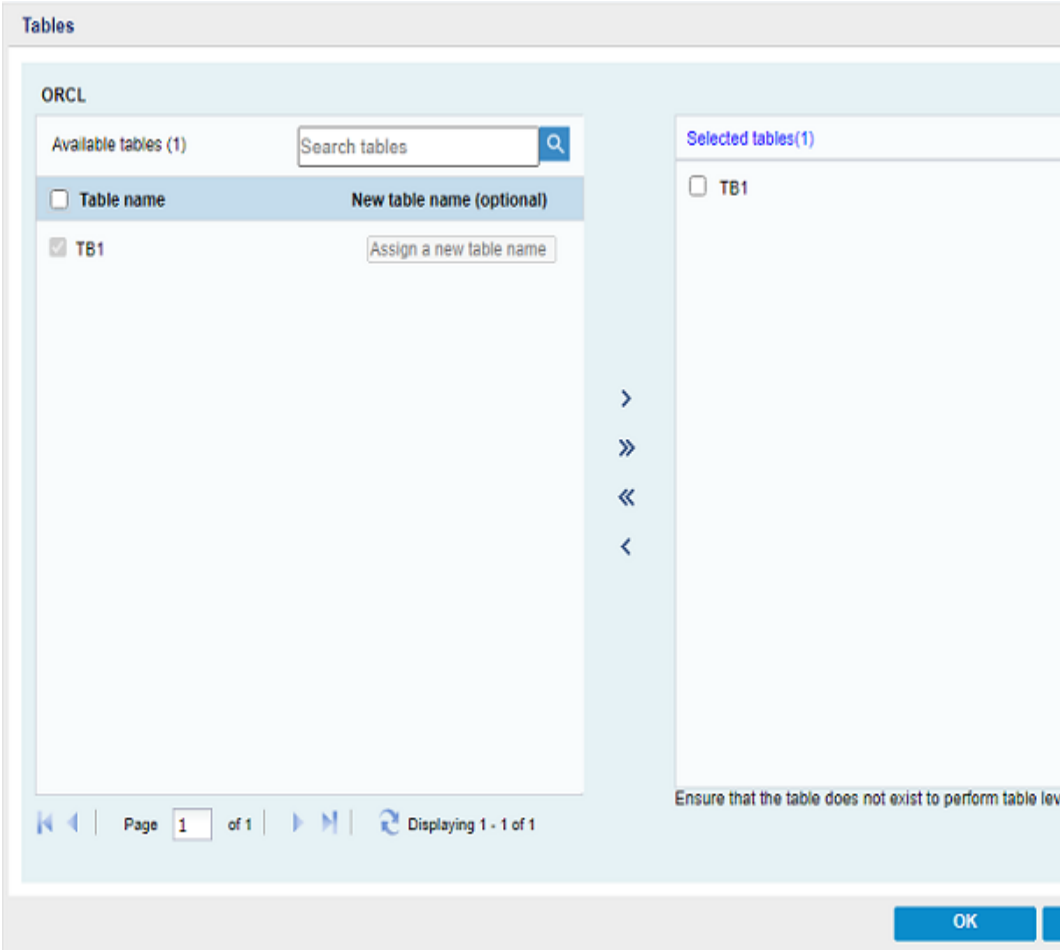
  - Dal riquadro sinistro, procedere come segue:
    - Per eseguire il ripristino completo di interi elementi del database, selezionare **Ripristino completo**.
    - Per eseguire il ripristino di spazi tabella e tabelle, selezionare **Ripristino granulare**.

    Nota: gli elementi del database Oracle, quali i registri archivio, i file di controllo e i file di parametro sono selezionati per impostazione predefinita quando viene visualizzata la finestra di dialogo Ripristino. Inoltre, questi elementi vengono ripristinati se necessario.
  - Dal riquadro destro, fare clic su ciascun file da espandere, quindi visualizzare i dettagli.

- (Facoltativo) Per selezionare le tabelle specifiche, dal riquadro destro fare clic sull'opzione **Tabelle**.

  Viene visualizzata una finestra di dialogo per la selezione della tabella.

  Nella finestra di dialogo per la selezione della tabella, eseguire le seguenti operazioni, quindi fare clic su **OK**:



  - Dal riquadro sinistro, procedere come segue:
    - Per cercare le tabelle disponibili, nella casella di ricerca selezionare il nome della tabella, quindi fare clic sull'icona di ricerca.
    - Selezionare le tabelle che si desidera ripristinare.
    - (Facoltativo) Digitare il nuovo nome della tabella che si desidera ripristinare.

Dopo aver selezionato le tabelle, fare clic sulla freccia destra (>) per spostarle nell'elenco delle tabelle selezionate ().

- Dal riquadro destro, deselezionare le tabelle che non si desidera ripristinare, quindi fare clic sulla freccia sinistra (<) per spostarle nell'elenco Tabelle disponibili ().

- Fare clic su **OK**.

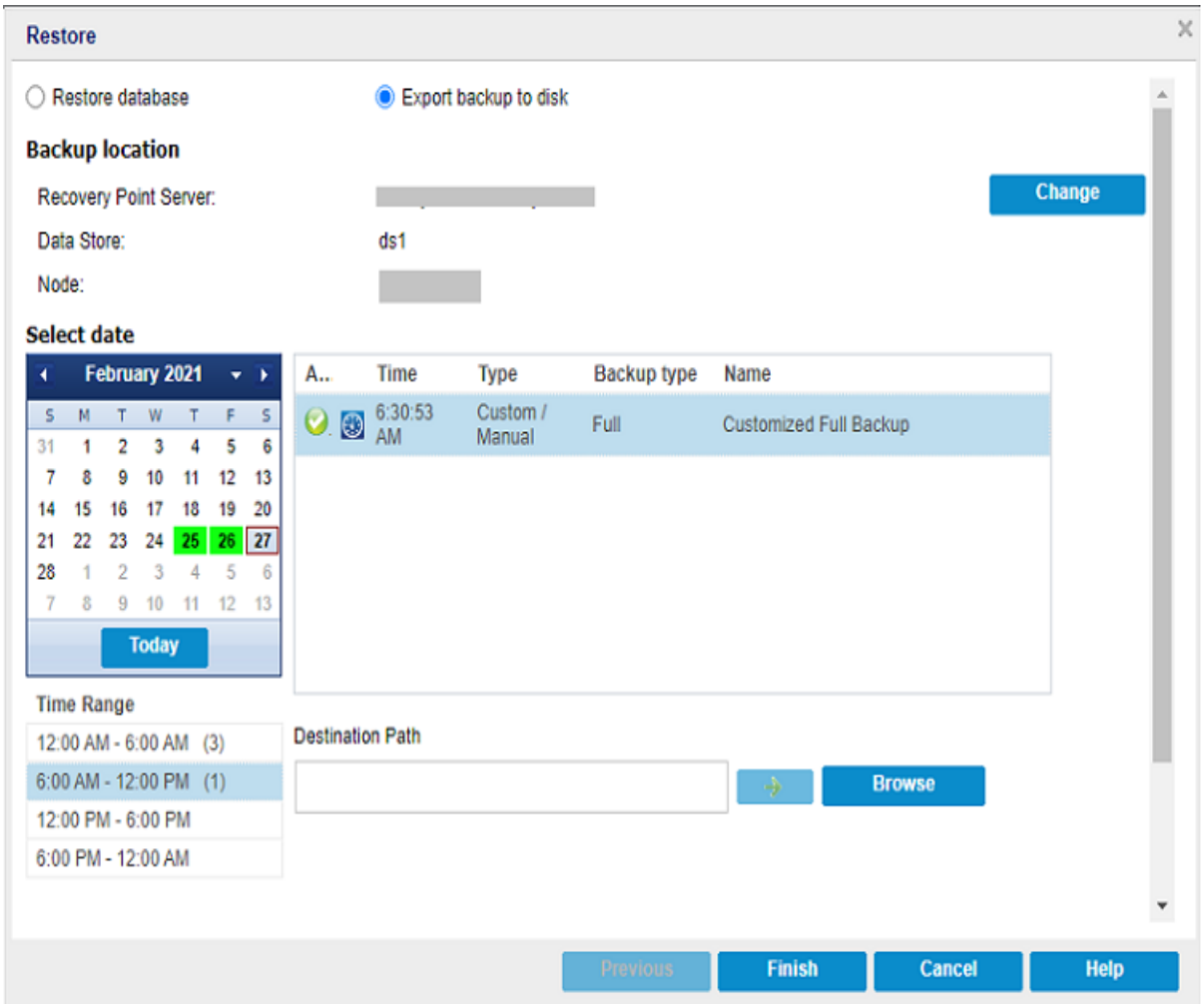
e. Fare clic su **Avanti**.

Viene visualizzata la finestra di dialogo Server di ripristino.

Vengono selezionati gli elementi del database Oracle da ripristinare. A questo punto, è possibile definire le opzioni di ripristino.

Esporta backup su disco

Ripristina gli elementi del database Oracle nella cartella o nella cartella condivisa sul disco.



Per esportare il backup su disco, procedere come segue:

a. (Facoltativo) Per modificare i dettagli della posizione di backup, fare clic su **Modifica**.

b. Dalla sezione Seleziona data, selezionare una data.

   In base alla selezione, viene visualizzato l'elenco dei punti di ripristino del backup con l'ora del backup, il tipo di backup eseguito (completo o incrementale) e il nome del backup.

c. Dall'elenco dei punti di ripristino di backup, selezionare un punto di ripristino di backup che si desidera ripristinare.

   Nota: per impostazione predefinita, viene selezionato il punto di ripristino più recente.

d. Nel campo Percorso di destinazione, fornire il percorso completo della condivisione di rete remota.

e. Per convalidare la connessione, fare clic sull'icona di freccia verde accanto al campo Percorso di destinazione, immettere il nome utente e la password necessari, quindi fare clic su **OK**.

f. Una volta stabilita la connessione alla condivisione di rete remota, fare clic sul pulsante **Sfoglia**.

   Viene visualizzata la finestra di dialogo Selezionare la posizione di backup.

g. Nella finestra di dialogo Selezionare la posizione di backup, selezionare una cartella da ripristinare, quindi fare clic su **OK**.

h. Fare clic su **Fine**.

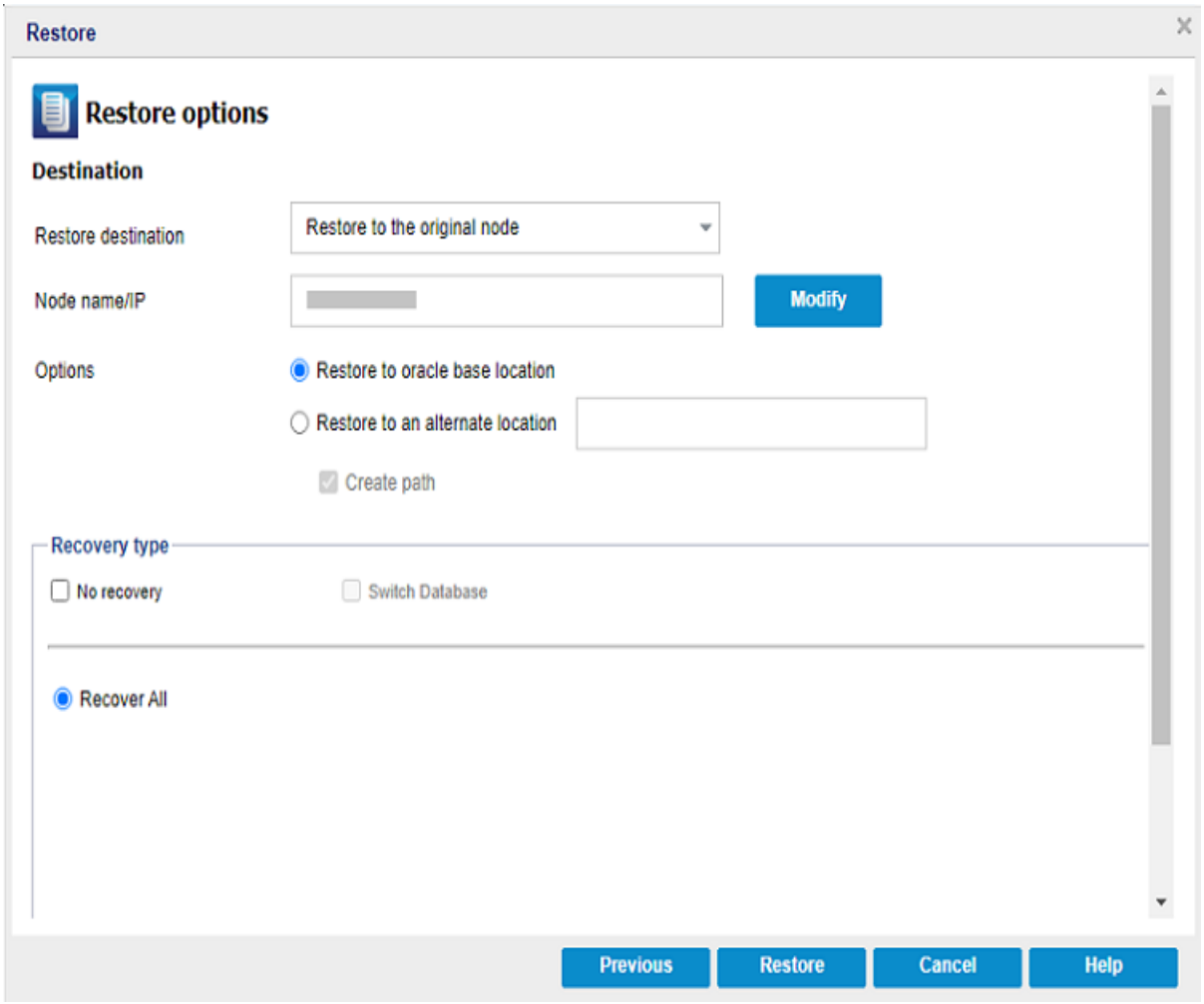
   Gli elementi del database Oracle vengono esportati sul disco.

Definizione delle opzioni di ripristino

In questa sezione vengono fornite informazioni su come definire le opzioni di ripristino per gli elementi del database Oracle selezionati.

Effettuare le operazioni seguenti:

1. Nella finestra di dialogo Opzioni di ripristino, selezionare la destinazione di ripristino.



Note:

- Durante il ripristino, per qualsiasi punto di ripristino di backup completo è disponibile solo l'opzione Ripristina tutto.
- I punti di ripristino associati ai backup incrementali includono tutte le opzioni quali Ripristina tutto, Ripristino temporizzato, Fino a SCN e Fino al numero di sequenza del registro del tipo di ripristino.

Le opzioni di destinazione disponibili sono:

Ripristino nella posizione originale

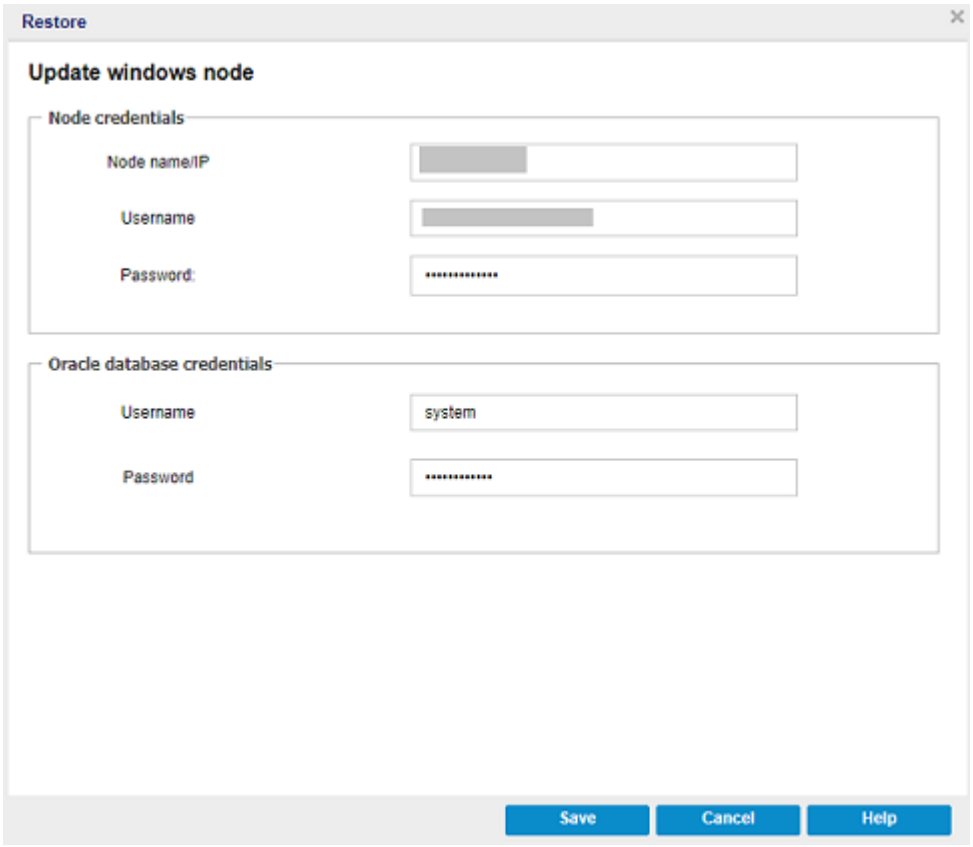
Per eseguire il ripristino nella posizione originale, eseguire le seguenti operazioni:

- I dettagli del nome del nodo/indirizzo IP esistente vengono visualizzati automaticamente. Nel caso in cui sia necessario modificare i dettagli del nome del nodo o dell'indirizzo IP, fare clic su **Modifica**.

  In base al tipo di nodo, viene visualizzata la finestra di dialogo Aggiorna nodo Windows o Aggiorna nodo Linux.

  #### Aggiorna nodo Windows

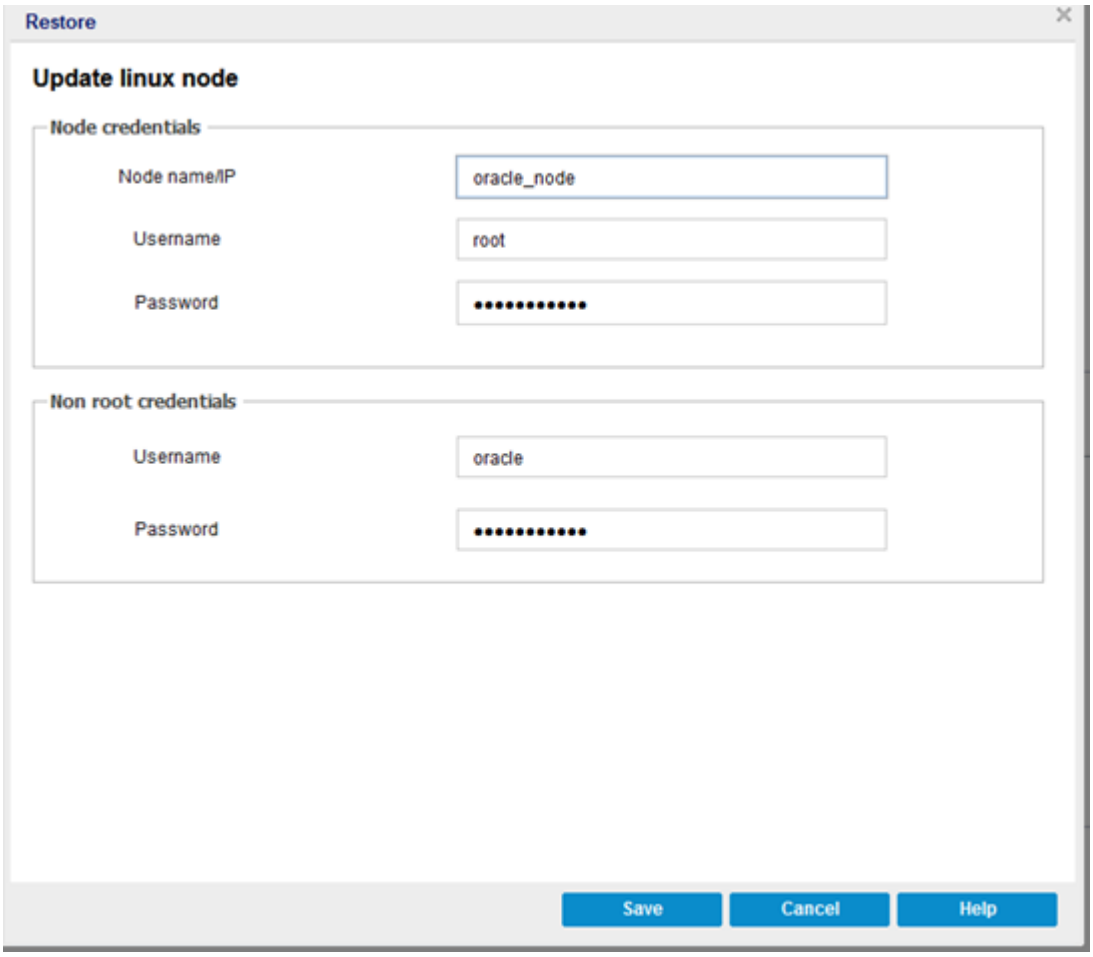
  Nella finestra di dialogo Aggiorna nodo Windows, immettere il nome o l'IP del nodo, il nome utente e la password, quindi fare clic su **Salva**.



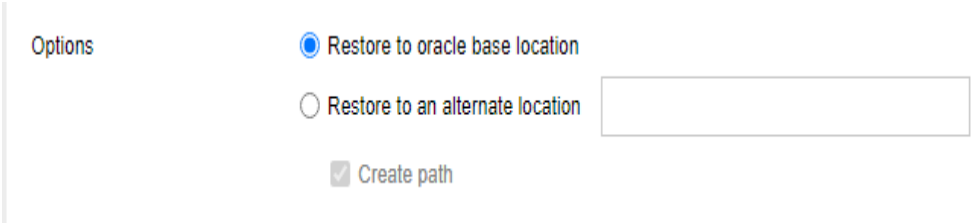
  #### Aggiorna nodo Linux

  Nella finestra di dialogo Aggiorna nodo Linux, aggiornare i seguenti dettagli, quindi fare clic su **Salva**:

- Per le credenziali del nodo, immettere il nome o l'IP del nodo, il nome utente e la password.
- Per le credenziali non root, immettere il nome utente e la password necessari.



- Per le opzioni, selezionare una delle seguenti opzioni:



Le opzioni disponibili sono:

Ripristina in Oracle Base Location

Ripristina gli elementi del database selezionati nella posizione di base Oracle da cui è stato eseguito il backup.

Ripristina in posizione alternativa

Esegue il ripristino in una posizione alternativa. Quando si seleziona questa opzione, è necessario aggiungere un percorso della posizione alternativa.

Nota: la casella di controllo **Crea percorso** viene selezionata automaticamente quando si seleziona l'opzione **Ripristina in posizione alternativa**.

Ripristina sul nodo alternativo

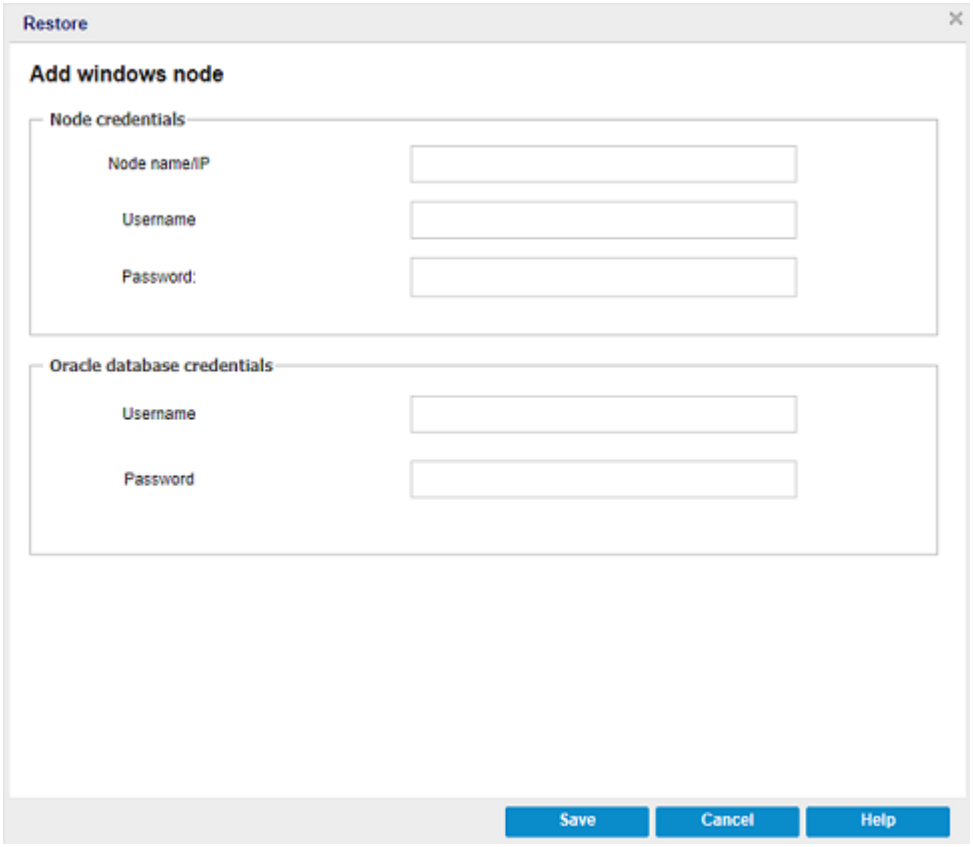
Per eseguire il ripristino sul nodo alternativo, procedere come segue:

- Per aggiungere un nuovo nodo o un indirizzo IP, fare clic sul pulsante **Aggiungi**.

  In base al tipo di nodo, viene visualizzata la finestra di dialogo Aggiungi nodo Windows o Aggiungi nodo Linux.

  Aggiungi nodo Windows

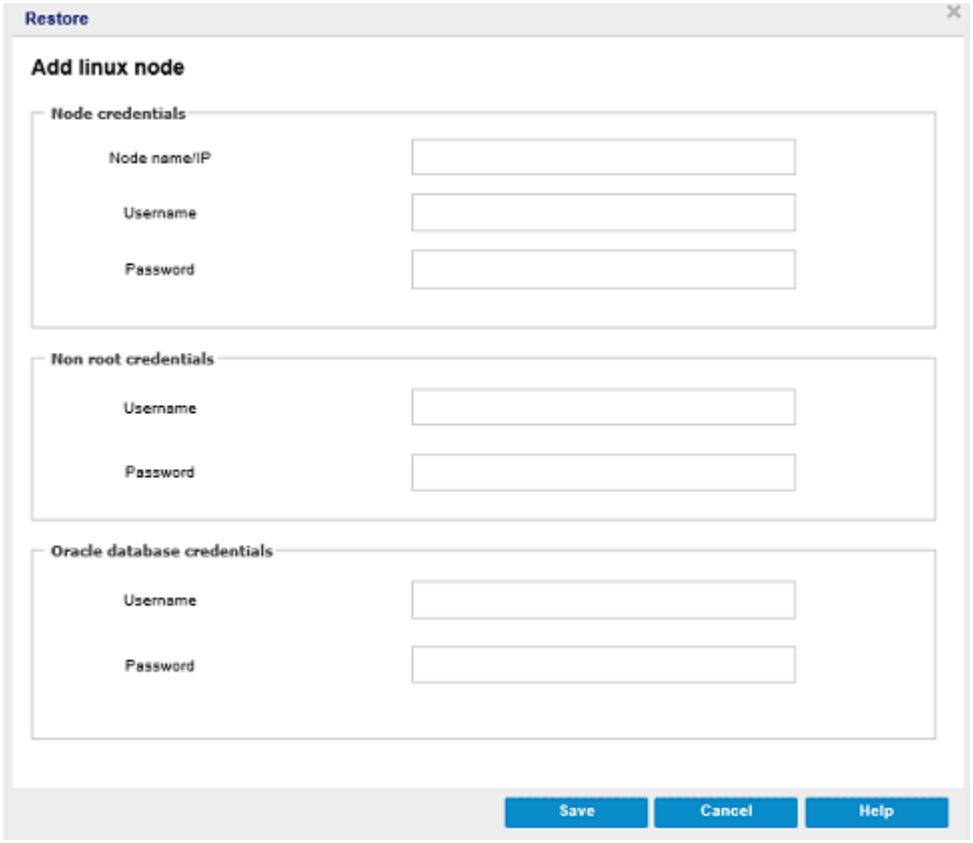
  Nella finestra di dialogo Aggiungi nodo Windows, immettere il nome o l'IP del nodo, il nome utente e la password, quindi fare clic su **Salva**.



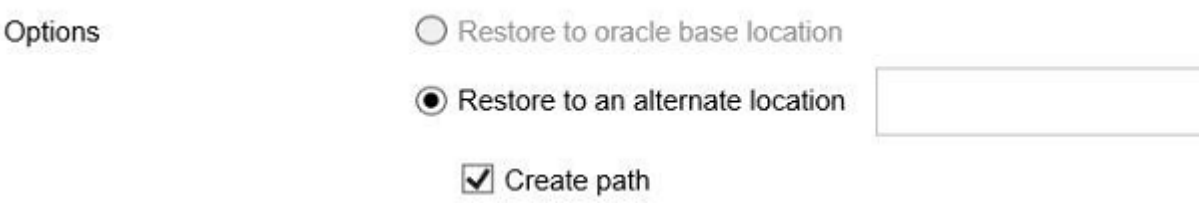
Aggiungi nodo Linux

Nella finestra di dialogo Aggiungi nodo Linux, aggiungere i seguenti dettagli, quindi fare clic su **Salva**:

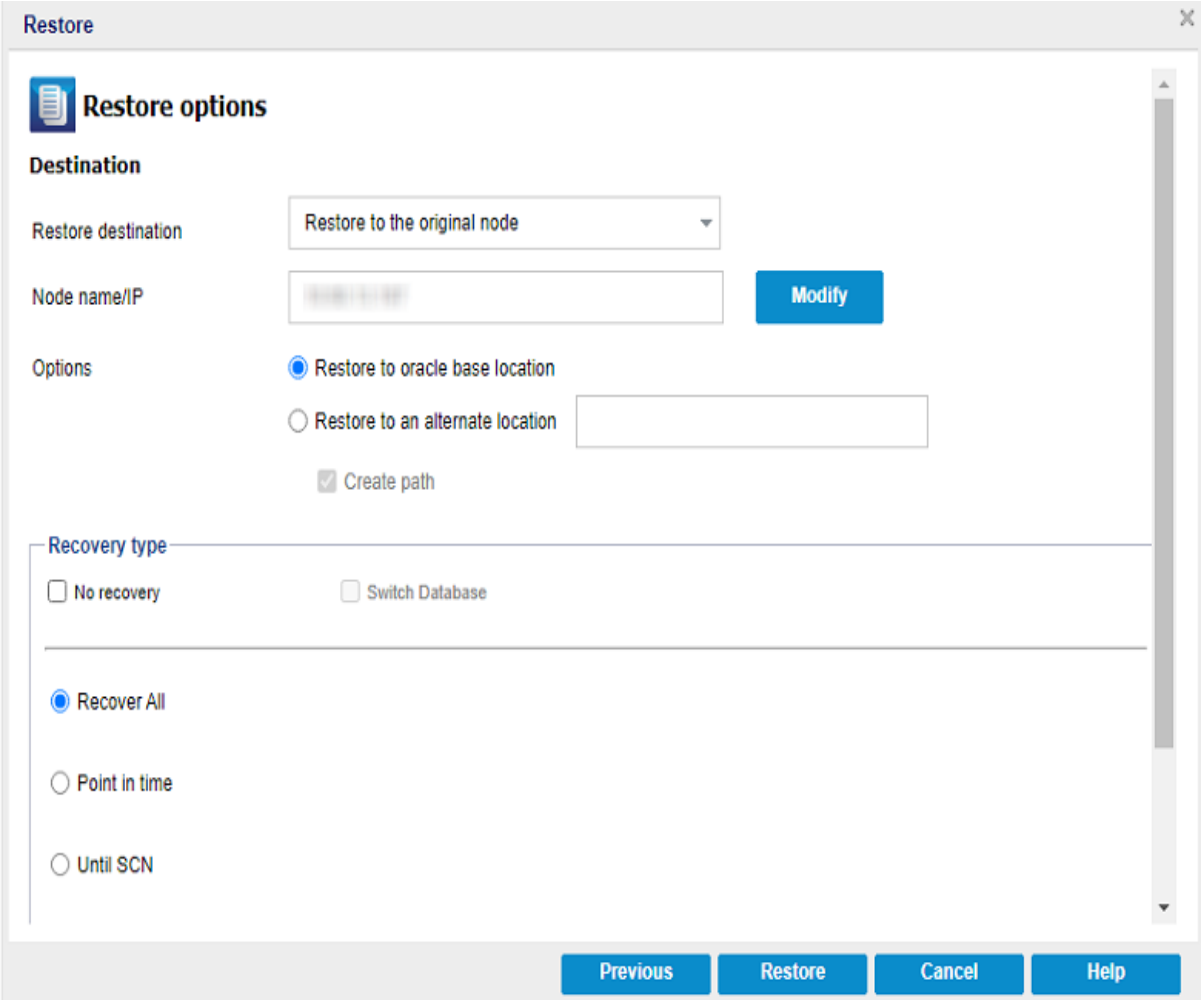
- Per le credenziali del nodo, immettere il nuovo nome o il nuovo IP del nodo, il nome utente e la password in base alle proprie esigenze.
- Per le credenziali non root, immettere il nuovo nome utente e la password necessari.



- Per le opzioni, l'opzione **Ripristina in posizione alternativa** è selezionata per impostazione predefinita. Immettere il percorso della posizione alternativa.



2. Nella sezione Tipo di ripristino, procedere come segue:



- Se non si desidera eseguire il ripristino, selezionare la casella di controllo **Nessun ripristino**. In base alla selezione, viene attivata la seguente opzione:

  Modifica database

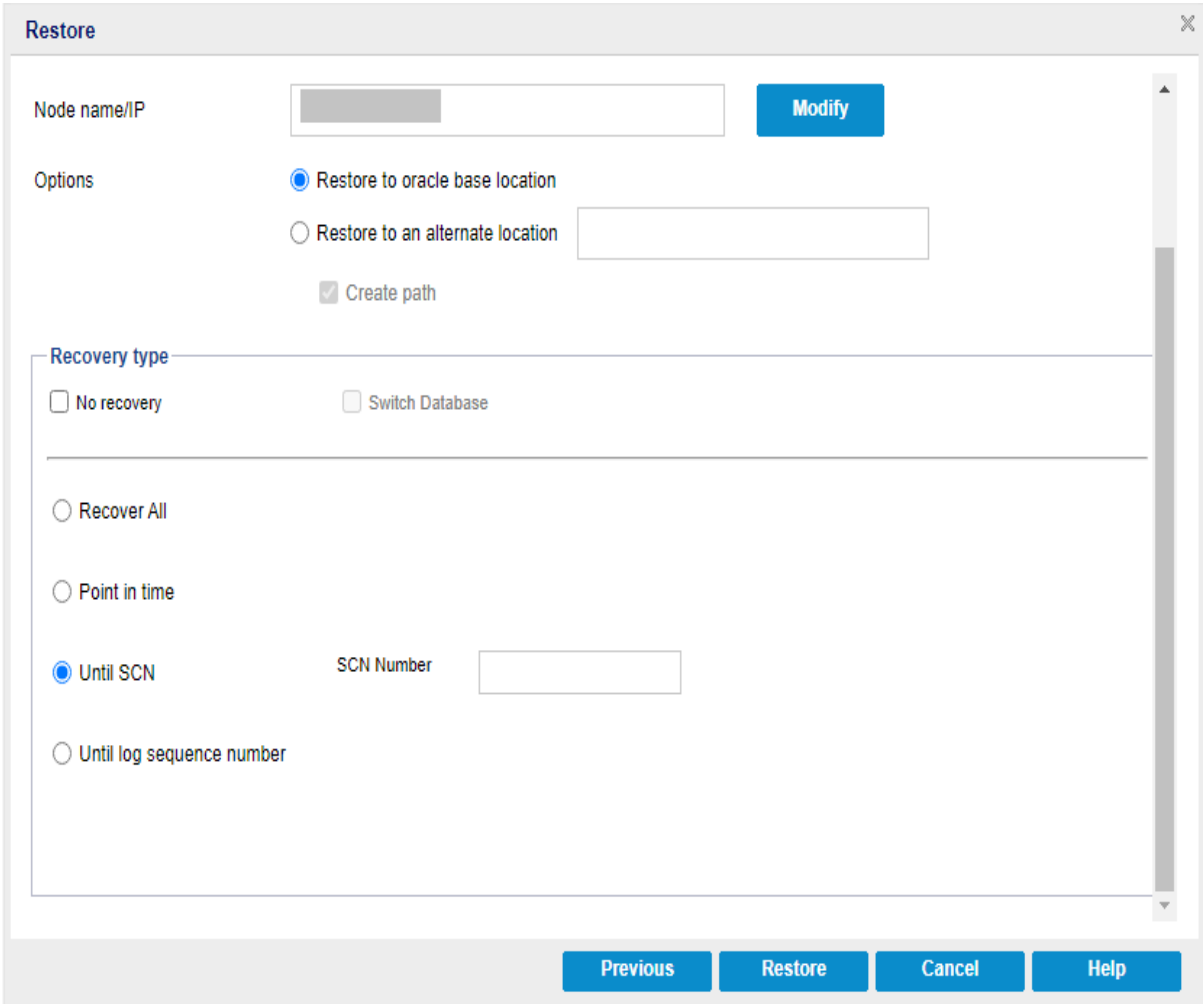
  Se si desidera spostare gli elementi del database nella nuova posizione, selezionare la casella di controllo **Modifica database**.

  Nota: l'opzione Cambia database è supportata solo quando viene eseguito il ripristino in una posizione alternativa o in un nodo alternativo.

- Se si desidera eseguire il ripristino temporizzato, selezionare l'opzione **Ripristino temporizzato**, quindi specificare le seguenti informazioni:
  - Selezionare una data per eseguire il ripristino temporizzato.
  - Selezionare l'ora di inizio desiderata.

Nota: la data e l'ora di inizio per il ripristino temporizzato devono essere inferiori al punto di ripristino del backup selezionato e superiori al punto di ripristino precedente.

- Se si desidera ripristinare tutti gli elementi del database fino alla data e all'ora del Numero SCN (System Change Number), selezionare **Fino a SCN**, quindi immettere il valore per il numero SCN.



- Se si desidera ripristinare tutti gli elementi del database fino al numero di sequenza del registro specificato, selezionare l'opzione **Fino al numero di sequenza del registro**, quindi immettere i valori per Sequenza registro e Numero di thread.

3. Fare clic su **Ripristina**.

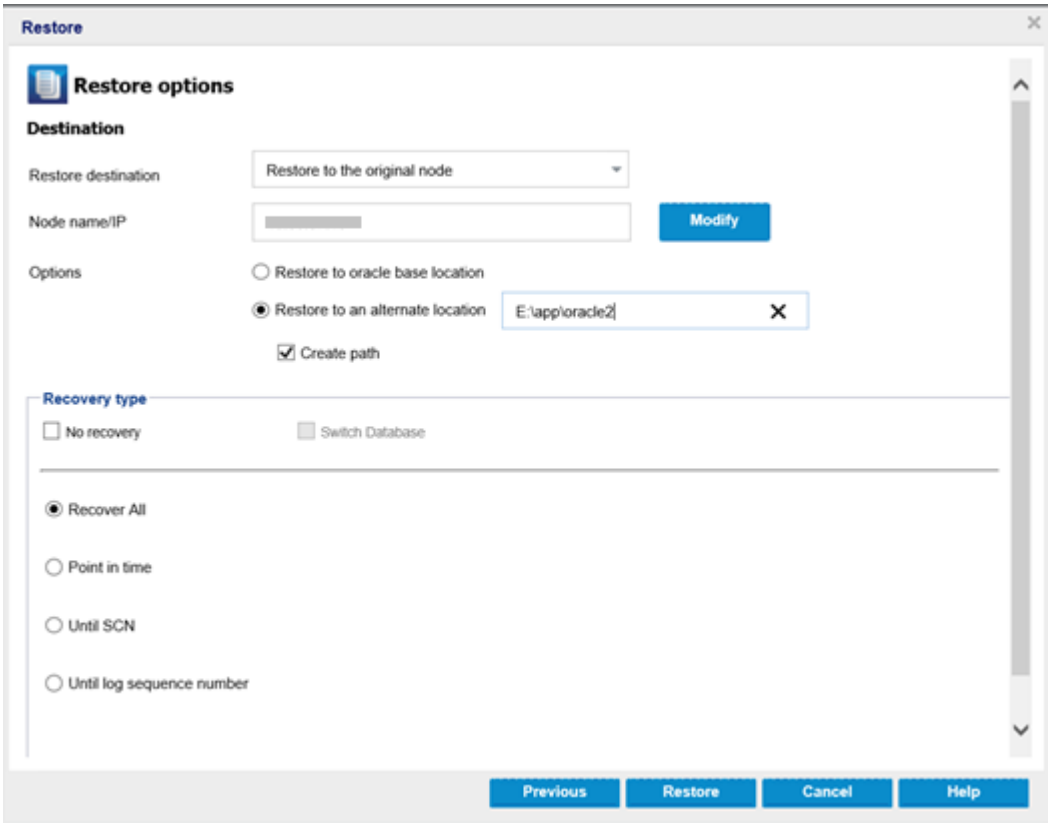
Gli elementi del database Oracle vengono ripristinati.

Ripristino del database in una posizione alternativa su Windows

La presente sezione fornisce informazioni su come ripristinare il database in una posizione alternativa su Windows.

Effettuare le operazioni seguenti:

1. Dalla console UDP, selezionare il punto di ripristino da cui eseguire il ripristino. Per ulteriori informazioni, consultare la sezione Definizione delle opzioni di ripristino.
2. Nella finestra di dialogo Opzioni di ripristino, dall'elenco a discesa Destinazione di ripristino, selezionare **Ripristina sul nodo originale**.



3. Per il nome del nodo o l'indirizzo IP, immettere il nome del nodo o l'indirizzo IP.
4. Per Opzioni, selezionare l'opzione **Ripristina in posizione alternativa**, quindi aggiungere il percorso della posizione alternativa.

   Note:

- Assicurarsi che il percorso aggiunto non contenga caratteri speciali o spazi.
- La casella di controllo **Crea percorso** viene selezionata automaticamente quando si seleziona l'opzione **Ripristina in posizione alternativa**.
- Se il database non è già stato chiuso, viene visualizzata una notifica in cui viene richiesto di chiudere il database. Per confermare, fare clic su **OK**.

5. Verificare che il processo di ripristino sia stato eseguito correttamente dalla console UDP.
6. Connettersi a **sqlplus** e verificare che il database sia attivo e in esecuzione.

   Il database ripristinato è operativo con la posizione alternativa specificata. Tuttavia, dopo il riavvio del database, il database potrebbe tornare alla copia precedente o potrebbero verificarsi degli errori a causa di un problema noto. Per evitare ulteriori problemi in seguito al ripristino in una posizione alternativa, si consiglia di procedere come segue. Questi passaggi consentono di creare o posizionare una copia corretta di spfile/pfile.

   a. Accedere al database **%ORACLE_HOME%\database e rinominare il file spfile<SID>.ora**.
   b. Connettersi a **sqlplus**.
   c. Accedere al prompt SQL ed eseguire il seguente comando:

      sqlplus > create pfile from spfile.
   d. Accedere al database **%ORACLE_HOME%\database**, aprire il file **init<SID>.ora** in qualsiasi editor di testo ed eseguire le seguenti operazioni:

      1. Aggiornare il valore "db_create_file_dest" con il percorso specificato per la posizione alternativa ripristinata.
      2. Rimuovere le virgolette aggiuntive '\' dalla parte finale del percorso nel parametro *diagnostic_dest*.

         Modificare quanto segue:

         Da *diagnostic_dest='E:\app\oracle2\ORA19C280220211833\'*

         In *diagnostic_dest='E:\app\oracle2\ORA19C280220211833'*
      3. Salvare il file.
   e. Accedere al prompt SQL ed eseguire i seguenti comandi:

Sqlplus > shutdown immediate

sqlplus > startup

sqlplus > create spfile from pfile

Nota: se il database non viene avviato dal file *spfile*, i ripristini dai backup corrispondenti sono limitati al nodo originale. Per evitare questo comportamento, riavviare il database dopo la creazione del file *spfile*. Per riavviare, eseguire i seguenti comandi:

Sqlplus > shutdown immediate

sqlplus > startup

Ripristino del database su un nodo alternativo su Windows

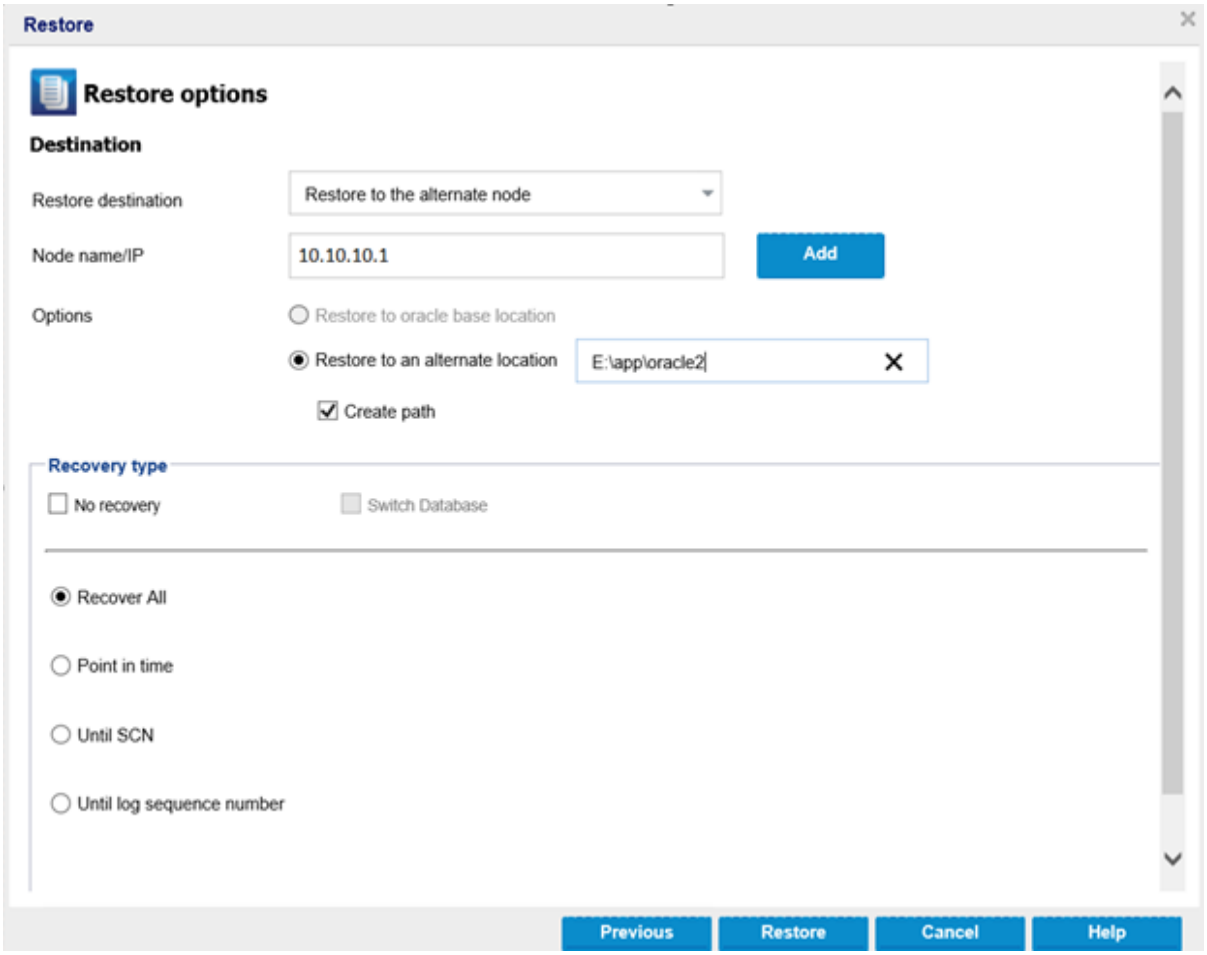
La presente sezione fornisce informazioni su come ripristinare il database su un nodo alternativo su Windows.

Note:

- Se l'opzione di **rilevamento delle modifiche dei blocchi** è disattivata e viene eseguito il ripristino del nodo alternativo, il ripristino potrebbe non riuscire. Pertanto, selezionare l'opzione di ripristino solo quando si dispone dei registri necessari ed è possibile recuperare il database manualmente dopo il ripristino. Per risolvere il problema, abilitare il **rilevamento delle modifiche dei blocchi** prima di eseguire il ripristino di un nodo alternativo sul nodo di origine.
- Assicurarsi che sia installata la stessa versione del software Oracle e che sia stato creato il database con lo stesso SID sul nodo alternativo in cui si è pianificato di eseguire il ripristino come nodo originale (nodo di origine). Ad esempio, quando il SID del nodo di origine è orcl, creare orcl sul nodo alternativo prima di avviare il ripristino. Questa operazione è necessaria quando il software Oracle viene installato con l'account di dominio. Si tratta di un'operazione non necessaria con l'utilizzo dell'account virtuale.

Effettuare le operazioni seguenti:

1. Dalla console UDP, selezionare il punto di ripristino da cui eseguire il ripristino. Per ulteriori informazioni, consultare la sezione Definizione delle opzioni di ripristino.
2. Nella finestra di dialogo Opzioni di ripristino, dall'elenco a discesa Destinazione di ripristino, selezionare **Ripristina sul nodo alternativo**.



3. Per il nome del nodo o l'indirizzo IP, immettere il nome del nodo o l'indirizzo IP.
4. Per Opzioni, selezionare l'opzione **Ripristina in posizione alternativa**, quindi aggiungere il percorso della posizione alternativa.

   Note:

   - Assicurarsi che il percorso aggiunto non contenga caratteri speciali o spazi.
   - La casella di controllo **Crea percorso** viene selezionata automaticamente quando si seleziona l'opzione **Ripristina in posizione alternativa**.
   - Se il database non è già stato chiuso, viene visualizzata una notifica in cui viene richiesto di chiudere il database. Per confermare, fare clic su **OK**.
5. Verificare che il processo di ripristino sia stato eseguito correttamente dalla console UDP.

6. Connettersi a **sqlplus** su un nodo alternativo e verificare che il database sia attivo e in esecuzione.

   Il database ripristinato è operativo con la posizione alternativa specificata. Tuttavia, dopo il riavvio del database, il database potrebbe tornare alla copia precedente o potrebbero verificarsi degli errori a causa di un problema noto. Per evitare ulteriori problemi in seguito al ripristino in una posizione alternativa, si consiglia di procedere come segue. Questi passaggi consentono di creare o posizionare una copia corretta di spfile/pfile.

   a. Accedere al database **%ORACLE_HOME%\database e rinominare il file spfile<SID>.ora**.

   b. Connettersi a **sqlplus**.

   c. Accedere al prompt SQL ed eseguire il seguente comando:

      sqlplus > create pfile from spfile.

   d. Accedere al database **%ORACLE_HOME%\database**, aprire il file **init<SID>.ora** in qualsiasi editor di testo ed eseguire le seguenti operazioni:

      1. Aggiornare il valore "db_create_file_dest" con il percorso specificato per la posizione alternativa ripristinata.

         Esempio: **.db_create_file_dest='E:\app\oracle2\ORA19C280220211833'*

      2. Rimuovere le virgolette aggiuntive '\' dalla parte finale del percorso nel parametro *diagnostic_dest*.

         Modificare quanto segue:

         Da *diagnostic_dest='E:\app\oracle2\ORA19C280220211833\'*

         In *diagnostic_dest='E:\app\oracle2\ORA19C280220211833'*

      3. Salvare il file.

   e. Accedere al prompt SQL ed eseguire i seguenti comandi:

      Sqlplus > shutdown immediate

      sqlplus > startup

      sqlplus > create spfile from pfile

      Nota: se il database non viene avviato dal file *spfile*, i ripristini dai backup corrispondenti sono limitati al nodo originale. Per evitare questo comportamento, riavviare il database dopo la creazione del file *spfile*. Per riavviare, eseguire i seguenti comandi:

Sqlplus > shutdown immediate

sqlplus > startup

Limitazioni

Nella presente versione sono note le seguenti limitazioni:

- Se il server RPS viene modificato, il backup successivo sarà un backup completo.
- Il ripristino su un nodo alternativo non è supportato se l'origine e la destinazione si trovano su due diverse versioni di Oracle.
- Dopo l'aggiornamento a 8.1, quando viene eseguito il processo di ripristino in una posizione alternativa o in un nodo alternativo, i punti di ripristino del registro di archiviazione creati prima dell'aggiornamento alla versione 8.0 non sono più validi. I punti di ripristino non sono più validi perché non contengono i dettagli relativi al mapping dei file di dati nel database Flash.
- Per i ripristini del registro archiviazione in una posizione alternativa o in un nodo alternativo in 8.1, è necessario eseguire prima il backup incrementale (Tutti i tipi di dati), quindi utilizzare le pianificazioni del registro di archiviazione successive per il ripristino.
- Quando il listener Oracle è configurato nella posizione non predefinita, il database Oracle non viene visualizzato automaticamente nell'elenco dei nodi e deve essere aggiunto manualmente durante la creazione del piano.
- L'opzione Sospendi/Riprendi non è disponibile nel menu Nodo per i nodi Oracle.
- Oracle non supporta lo spazio tabella se il nome dello spazio tabella contiene il simbolo del dollaro ($) in Oracle 19c.
- Il ripristino granulare non è supportato quando il database Oracle viene installato utilizzando un account virtuale.
- UDP 8.1 non supporta il backup di database da diverse versioni di Oracle installate sullo stesso server.
- Ripristino delle tabelle in base alle limitazioni di Oracle:
  - Le tabelle create dagli spazi tabella SYSTEM e SYSAUX non possono essere ripristinate.
  - Le tabelle create dal sistema o dall'utente di sistema non possono essere ripristinate.
- RPS funge da agente di backup, ripristino e Assured Recovery.

- Per la Standard Edition, è supportato solo il ripristino completo del database con il recupero completo e il punto nel tempo (PIT) dai punti di ripristino più recenti e intermedi.
- Per la Standard Edition, il ripristino dello spazio tabella con recupero completo è supportato dal punto di ripristino più recente e la clausola UNTIL non è supportata nello script RMAN.
- Per la Standard Edition, Oracle non supporta i ripristini a livello di tabella.
- In seguito a un ripristino completo del database, il backup incrementale successivo verrà convertito automaticamente in un backup completo.
- Se la dimensione WRP viene modificata, il backup successivo sarà un backup completo.
- Il numero massimo di canali supportati è 10.

Chapter 5: Protezione dell'ambiente Microsoft SharePoint

La presente sezione descrive i seguenti argomenti:

Considerazioni sull'installazione per l'ambiente Microsoft SharePoint

L'argomento seguente contiene le informazioni necessarie per l'installazione e la configurazione dell'agente Arcserve UDP per l'ambiente Microsoft SharePoint. Le informazioni contenute in questa sezione presuppongono una certa familiarità con le caratteristiche e i requisiti della server farm Microsoft SharePoint.

Considerazioni sull'ambiente

Gli ambienti SharePoint possono essere complessi e distribuiti su diversi computer. È necessario che la configurazione della server farm sia supportata da Microsoft. Ad esempio, un ambiente SharePoint distribuito può comprendere i seguenti componenti:

- Uno o più server di front-end Web.
- Uno o più server di database utilizzati da SharePoint Server Farm.
- Nella maggior parte dei casi, SharePoint è installato in un ambiente di dominio. Saranno presenti uno o più server DNS e controller di dominio.

Considerazioni sull'installazione

Durante l'installazione degli agenti, tenere presenti le seguenti informazioni:

- SharePoint è un ambiente distribuito. Si consiglia di installare l'agente UDP su ciascun server nella farm di SharePoint, tra cui il server Web front-end e i server di database.
- Si consiglia inoltre di proteggere l'intero ambiente di dominio, inclusi il controller di dominio e il server DNS. Si tratta di componenti necessari per il ripristino della farm, della configurazione della farm e dell'applicazione Web.

Esecuzione del backup dei server Microsoft SharePoint

È possibile eseguire il backup dei server Microsoft SharePoint Server mediante Arcserve UDP. Per garantire il corretto funzionamento del ripristino, si consiglia di proteggere l'intero computer e non i volumi selezionati su tutti i server SharePoint.

Per i server DNS e di controller di dominio, è possibile eseguire il backup dei volumi selezionati a patto che il servizio di dominio e il servizio DNS funzionino correttamente.

- Revisione delle considerazioni
- Esecuzione di un backup del server SharePoint

Revisione delle considerazioni

Si consiglia di aggiungere tutti i server, inclusi i server Web front-end, i server di database, i server DNS e i controller di dominio in un piano con le stesse pianificazioni del backup. Di conseguenza, tutti i server verranno sottoposti a backup nello stesso momento. Si tratta di un'operazione importante per un ambiente distribuito. Durante il ripristino, è possibile ottenere gli stessi punti di ripristino di cui è stato eseguito il backup nello stesso momento per tutti i server.

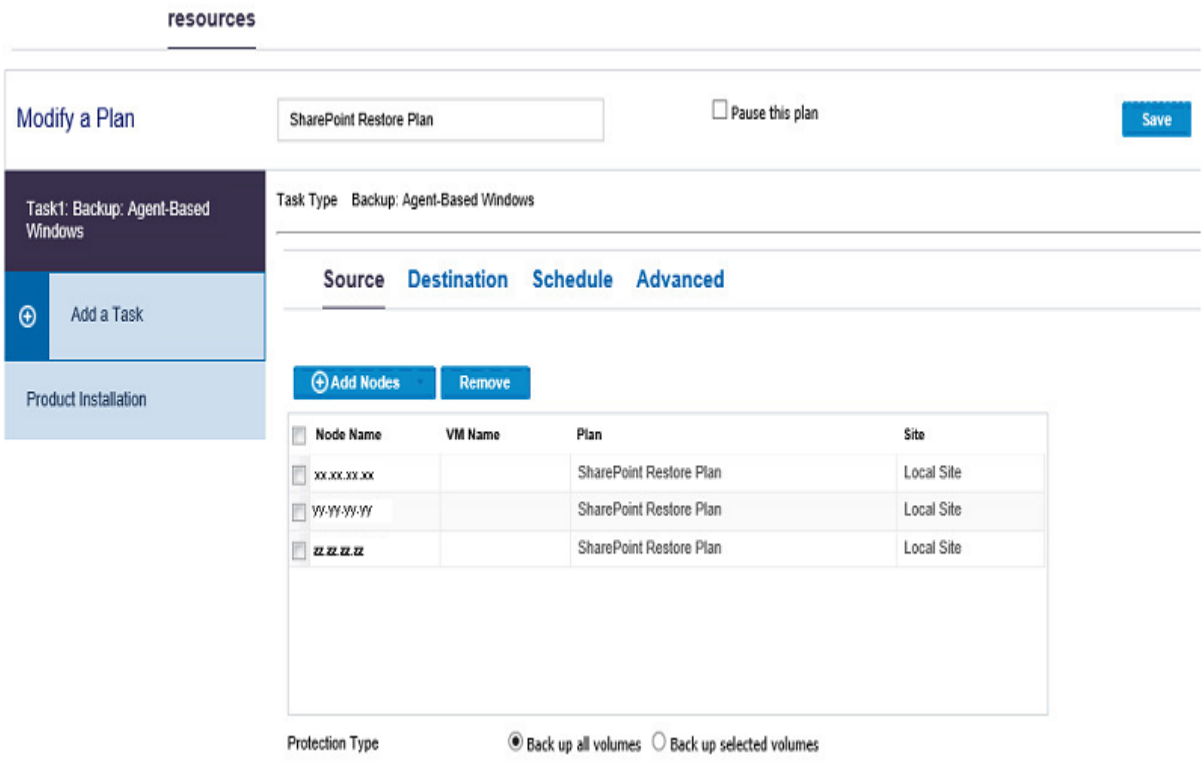
Nota: Se è stata modificata la topologia della Farm di SharePoint, vengono aggiunti nuovi server per eseguire miglioramenti del bilanciamento del carico per SharePoint. È necessario aggiungere immediatamente nuovi server allo stesso piano.

Esecuzione di un backup del server SharePoint

Utilizzare la console Arcserve UDP per eseguire il backup a livello di database nell'ambiente SharePoint.

Effettuare le operazioni seguenti:

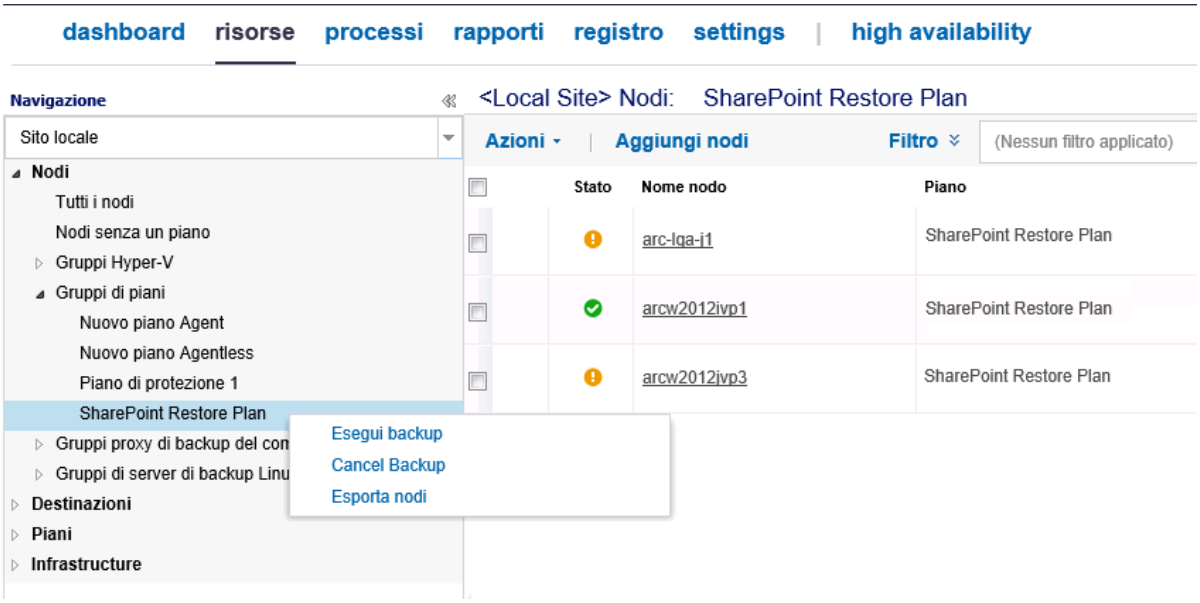
1. Accedere alla console.
2. Fare clic su **Risorse** e accedere a **Nodi** nel riquadro di **navigazione** a sinistra.
3. Fare clic su **Tutti i nodi**.
4. Aggiungere tutti i nodi all'ambiente Farm di SharePoint.
5. (Facoltativo) Creare un archivio dati.
6. Espandere **Piani** nel riquadro **Navigazione**, quindi fare clic su **Tutti i piani**.
7. Fare clic su **Aggiungi** per creare un nuovo piano.
8. Dalla scheda **Origine**, aggiungere tutti i nodi presenti nell'ambiente Farm di SharePoint.



9. Configurare le altre impostazioni e salvare il piano.

Il piano viene creato per gli ambienti Farm di SharePoint. Le impostazioni del piano vengono distribuite a tutti i nodi. Il processo di backup viene avviato nel momento pianificato.

È possibile avviare manualmente il processo di backup facendo clic su Esegui backup. Il processo di backup su tutti i nodi Farm di SharePoint viene avviato. I dati vengono salvati nello stesso archivio dati.



Ripristino di un ambiente SharePoint

Sono supportati i seguenti ripristini granulari:

- Farm
- Farm solo con configurazione
- Servizi SharePoint
- Applicazioni Web
- Database di contenuto
- Raccolte di siti
- Siti
- Elenchi
- Elementi dell'elenco (inclusi i documenti)

Vengono ripristinate granularità diverse con soluzioni differenti:

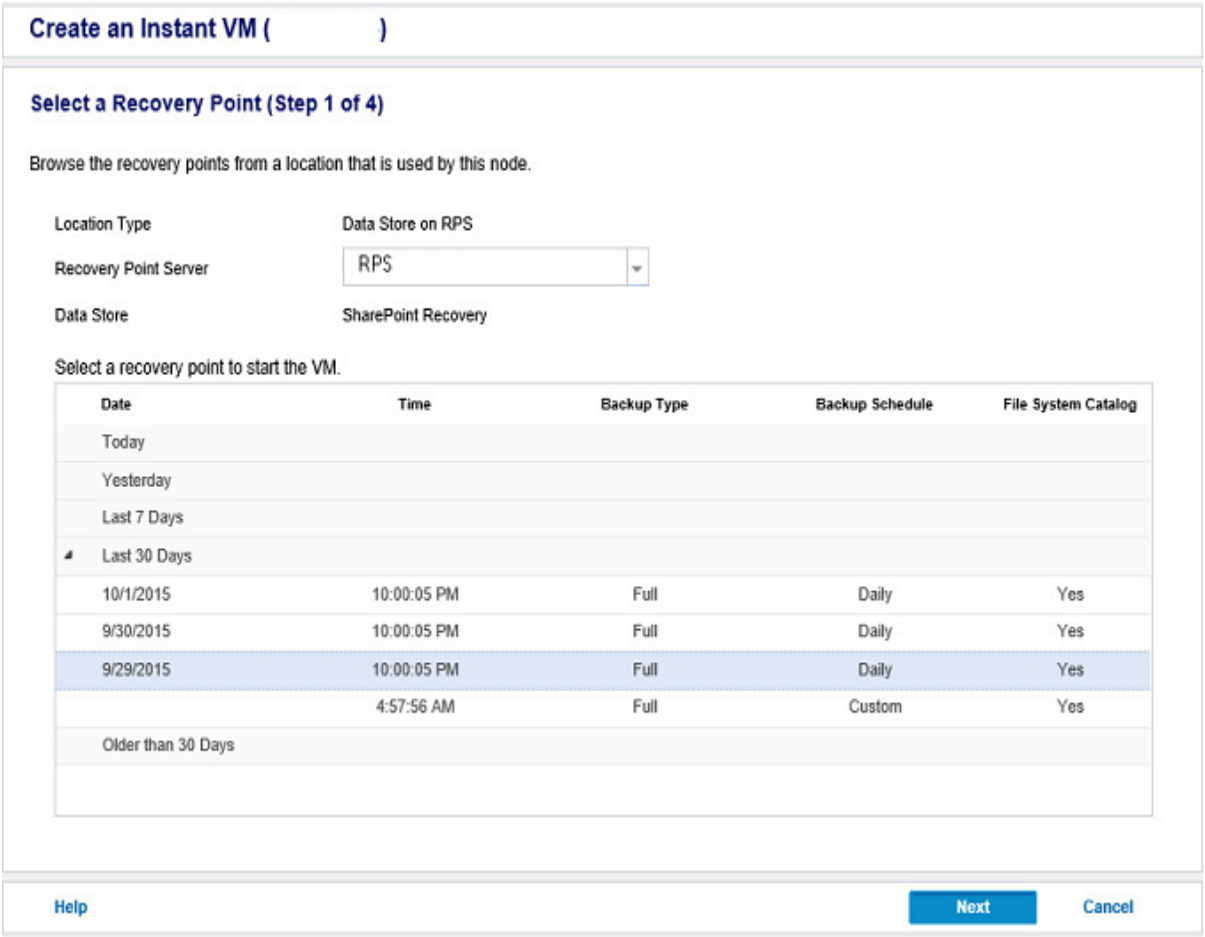
- Ripristino mediante computer virtuale istantaneo: supporta farm, farm soltanto con configurazione, servizi di SharePoint e applicazioni Web.
- Ripristino mediante l'interfaccia utente dell'agente Arcserve UDP: supporta i database del contenuto.
- Ripristino mediante montaggio del database da un punto di ripristino: supporta raccolte di siti, siti, elenchi e voci di elenco.

Ripristino mediante computer virtuale istantaneo

Effettuare le operazioni seguenti:

1. Accedere alla console.
2. Fare clic su **Risorse**, **Nodi**.
3. Fare clic con il tasto destro del mouse sul nodo, il quale è contenuto nel piano per l'ambiente SharePoint.
4. Fare clic su **Crea un computer virtuale istantaneo** per creare computer virtuali istantanei per il computer dell'ambiente SharePoint.

   Viene visualizzata la procedura guidata **Crea un computer virtuale istantaneo**.
5. Scegliere i punti di ripristino da un percorso e selezionare un punto di ripristino per avviare il computer virtuale istantaneo.

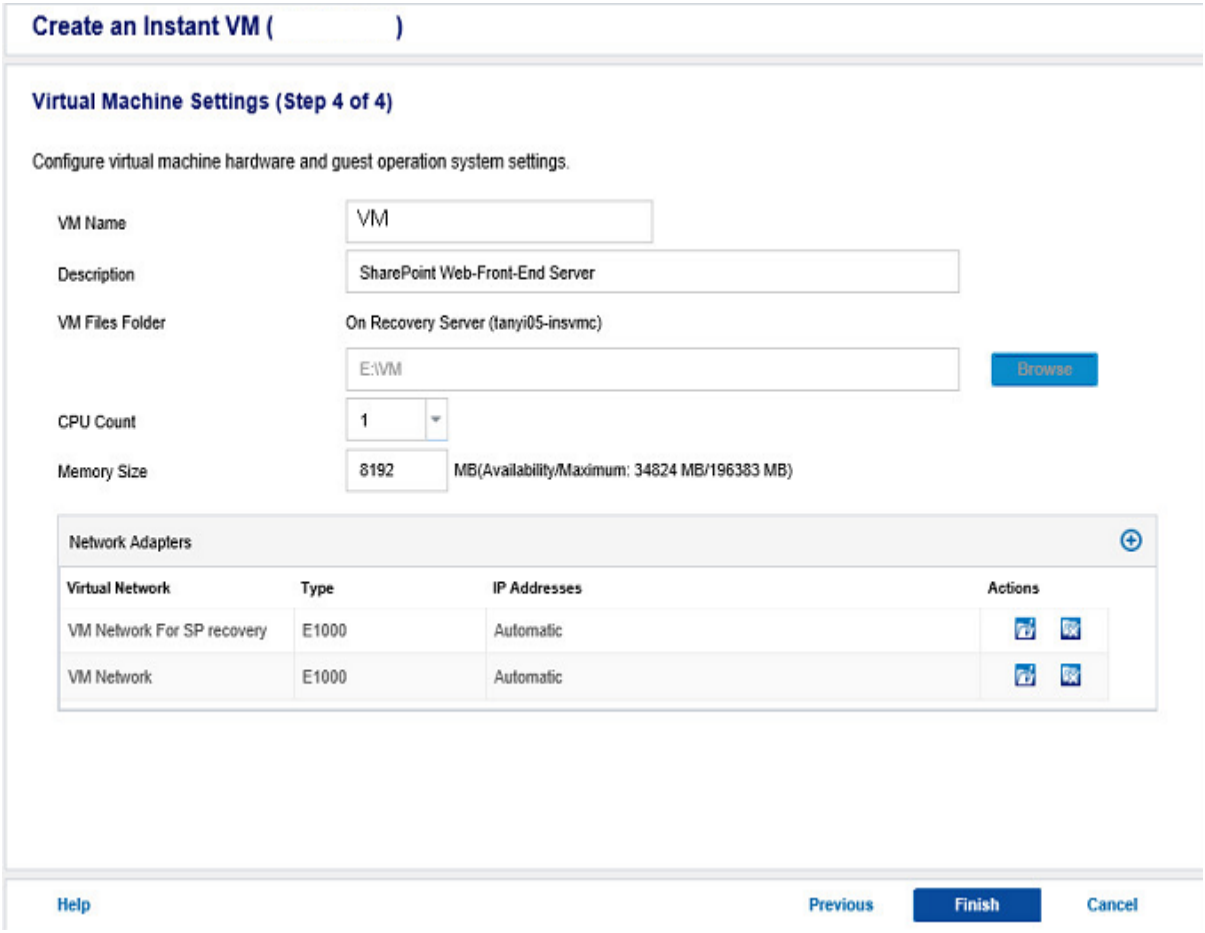


6. Fare clic su **Avanti**.
7. Specificare un percorso su VMware vSphere o Microsoft Hyper-V come host del computer virtuale istantaneo. Ad esempio, il tipo di hypervisor è VMware vSphere.

8. Fare clic su **Avanti**.
9. Specificare un computer per l'esecuzione del computer virtuale istantaneo.

   Ad esempio, utilizzare il server RPS corrente.
10. Fare clic su **Avanti**.
11. Configurare le impostazioni di sistema e dell'hardware del computer virtuale istantaneo.
12. Creare una nuova rete virtuale come ambiente di rete isolata per il ripristino di SharePoint. Per ulteriori informazioni sulla creazione di una rete isolata, consultare la sezione Creazione di una rete isolata per il ripristino di SharePoint.
13. Fare clic sul segno (più) per aggiungere una scheda di rete.
14. Selezionare la rete virtuale corretta, la quale è un ambiente di rete isolata per il ripristino di SharePoint, e utilizzare la configurazione predefinita delle impostazioni TCP/IP "Origine:XXX.XXX.XXX.XXX".

    Importante! Durante la creazione di un computer virtuale istantaneo per un computer corrispondente a un server Web front-end per l'ambiente SharePoint, aggiungere una o più schede di rete per il trasferimento del file dei dati di backup. L'indirizzo IP della nuova scheda deve essere contenuto nella stessa rete virtuale con i server Web front-end originali per SharePoint, e deve condividere lo stesso segmento IP. Quindi, l'ambiente SharePoint originale potrà utilizzare la scheda di rete per accedere a tutte le cartelle condivise con il computer virtuale istantaneo.



15. Fare clic su **Fine**.

    Viene visualizzata la finestra di dialogo Avvia computer virtuale.

16. Fare clic su **Avvia più tardi**.

    Viene creato un nuovo computer virtuale istantaneo visualizzato in **Infrastrutture**, **Computer virtuali istantanei** nella Console.

17. Creare un computer virtuale istantaneo per tutti i nodi dell'ambiente Farm di SharePoint.

18. Dopo aver creato i computer virtuali istantanei di tutti i nodi, avviarli uno per uno.

    - Avviare prima il controller di dominio, quindi il server DNS.
    - Avviare quindi il server di database e solo successivamente i server Web front-end.

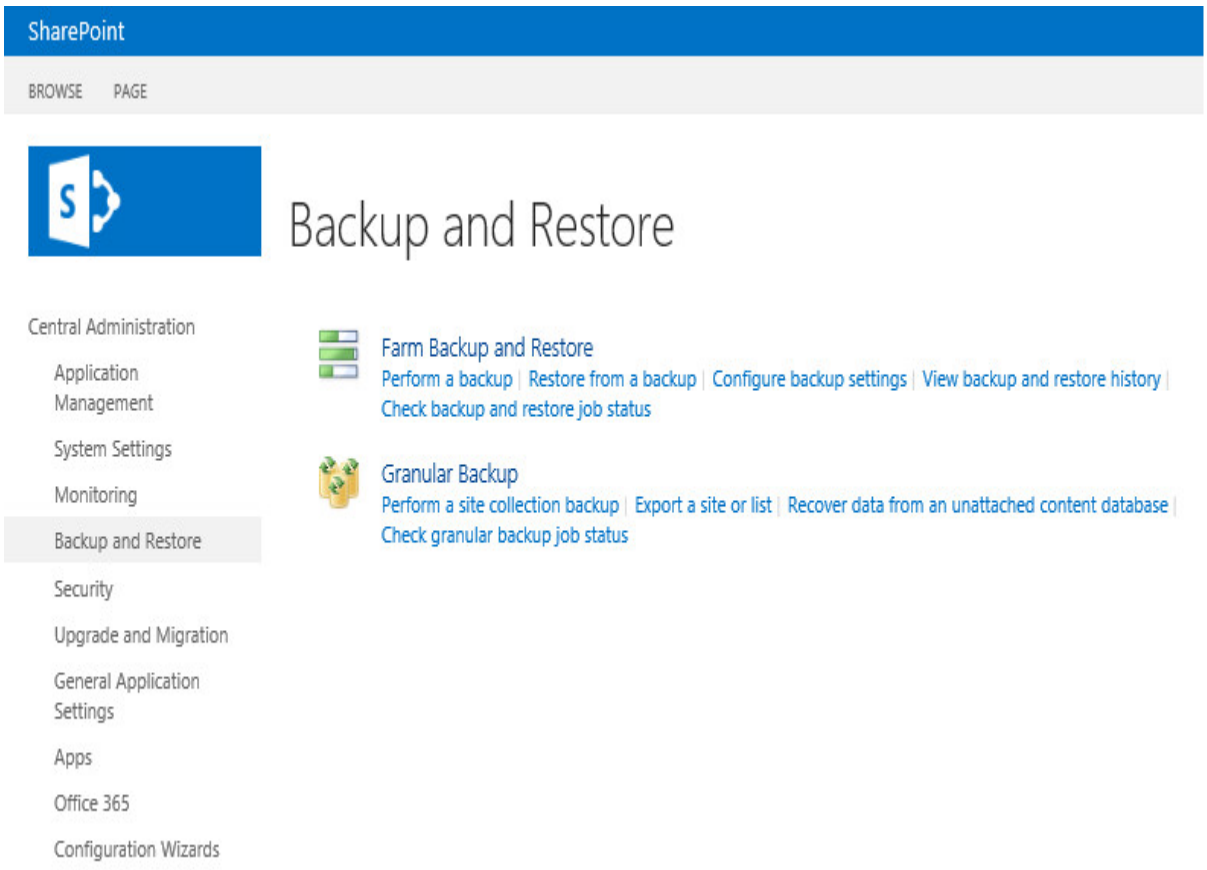
19. Fare clic con il tasto destro del mouse sul computer virtuale istantaneo che si desidera attivare, quindi selezionare **Attiva** per avviare il computer virtuale istantaneo.

20. Attendere l'attivazione dei computer virtuali istantanei per i computer dell'ambiente SharePoint.

    L'ambiente SharePoint temporaneo è stato configurato.

21. Accedere al computer virtuale istantaneo in cui sono stati installati i server Web front-end per l'ambiente SharePoint. Aprire Amministrazione centrale, fare clic sull'intestazione Backup e ripristino, quindi selezionare il collegamento Esegui backup.

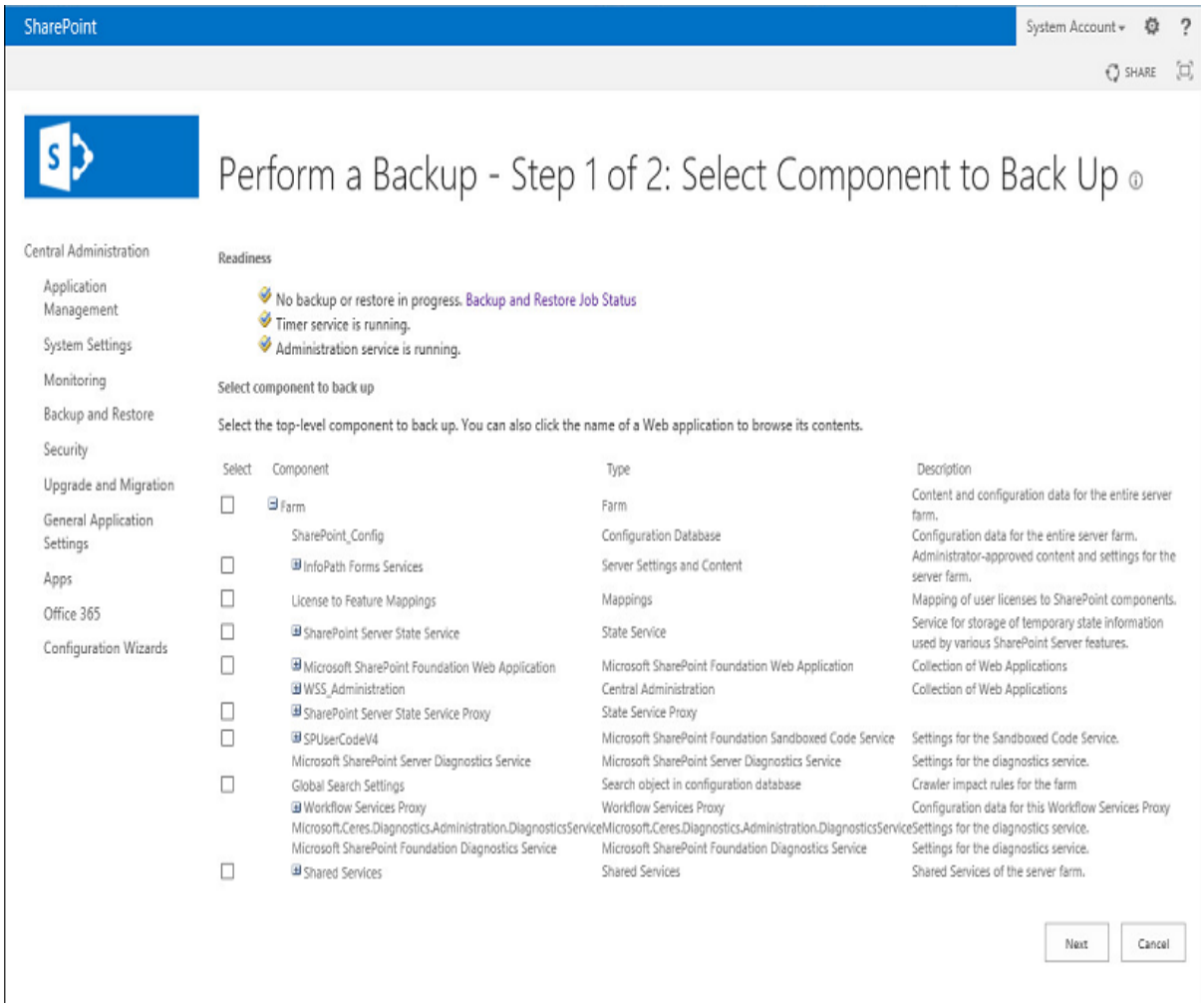
    Nota: Se viene visualizzato l'errore HTTP 404 dopo l'apertura di un'applicazione Web come SharePoint - 80, disabilitare IPv6 e deselezionare la casella di controllo **Protocollo Internet versione 6 (TCP/IP)** dalla finestra delle proprietà di rete dell'area locale.



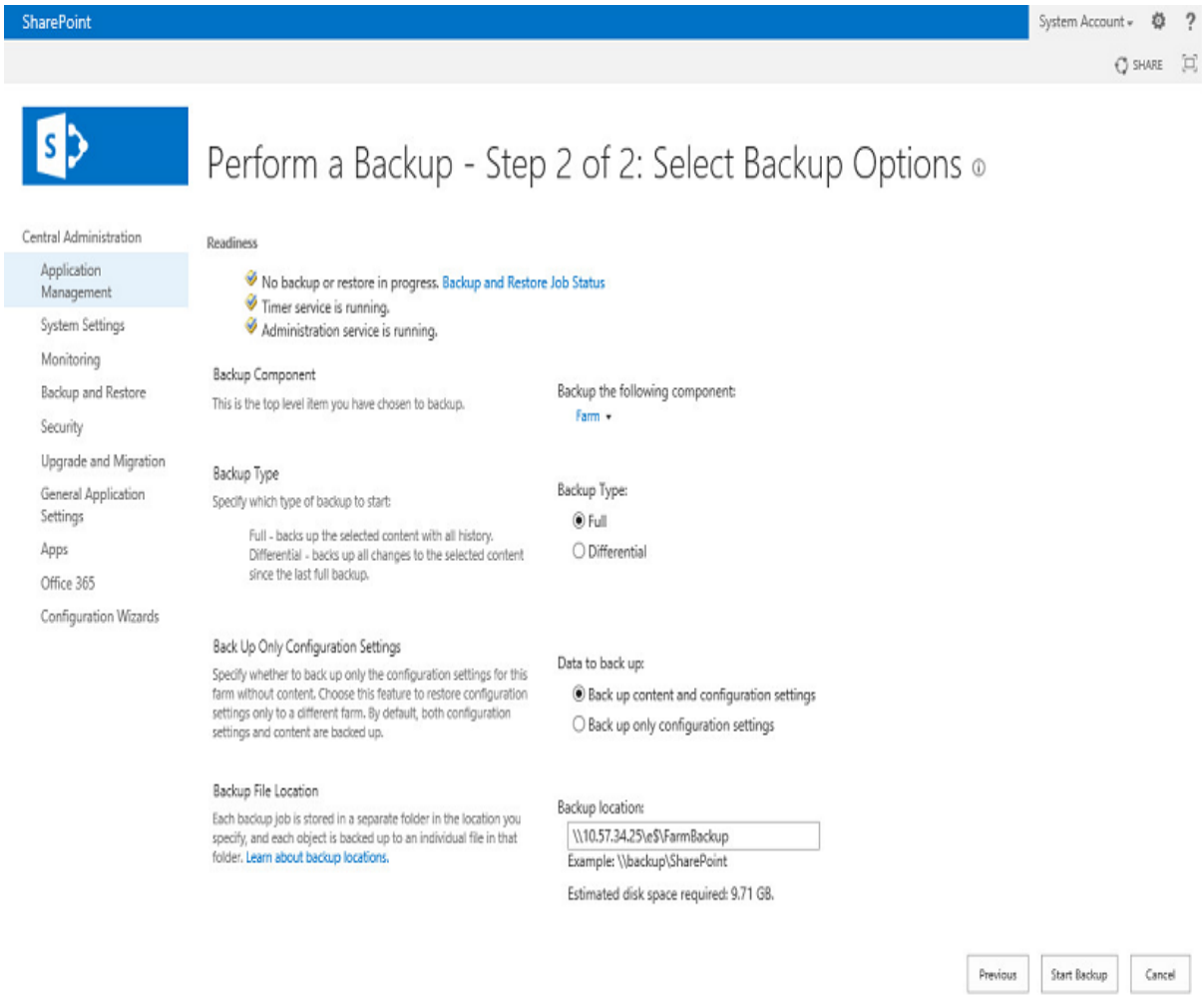
22. Selezionare il componente da ripristinare per la farm e fare clic su **Avanti**.

    Ad esempio, eseguire il backup delle applicazioni Web SharePoint - 80. Espandere il nodo dell'applicazione Web di Microsoft SharePoint Foundation e selezionare il componente SharePoint – 80.

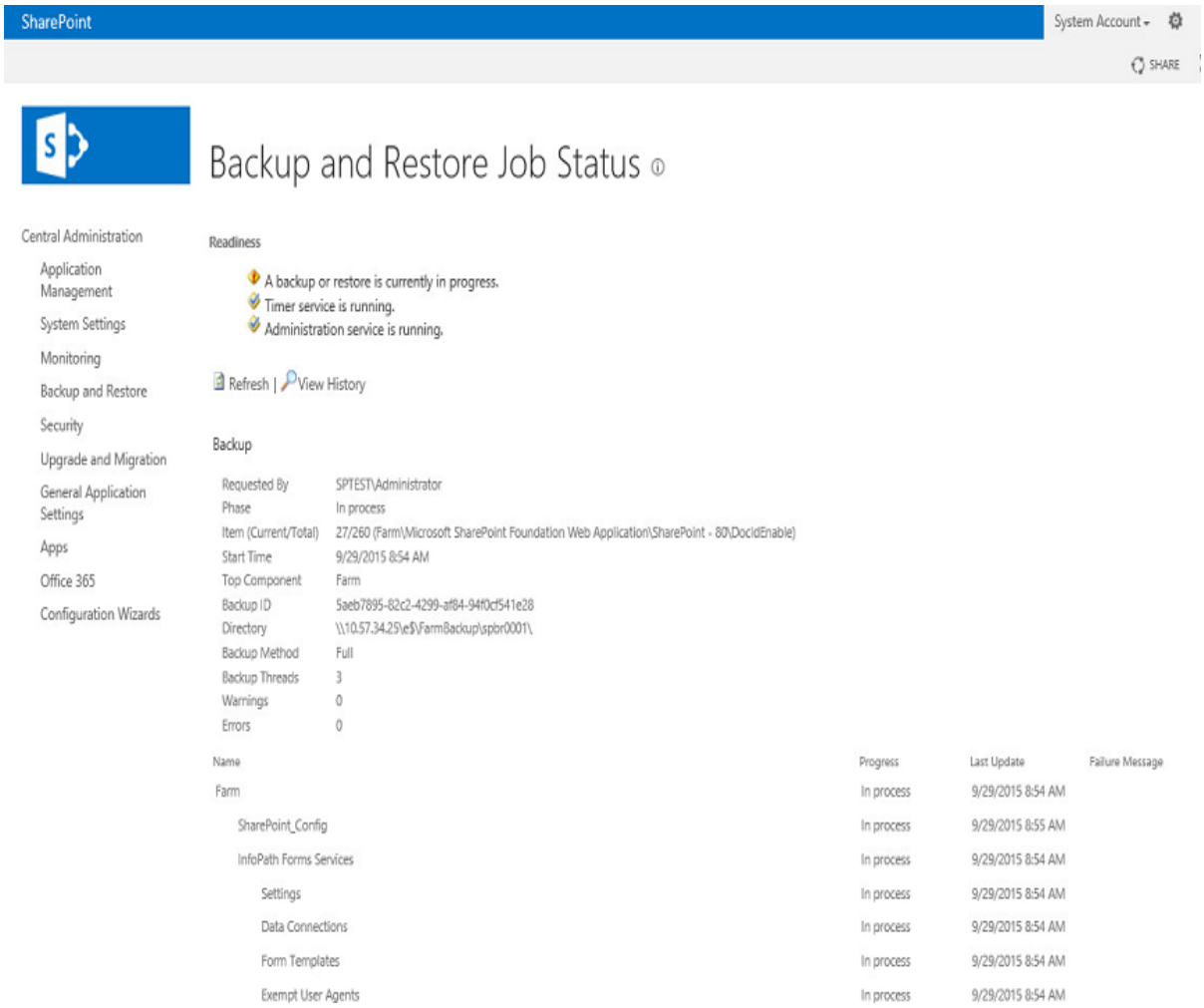
    Eseguire il backup di Access Services. Espandere il nodo delle applicazioni dei servizi condivisi in Servizi condivisi, quindi selezionare il componente Access Services 2010.



23. Specificare il tipo di backup come Completo.
24. Creare una cartella condivisa sul computer virtuale istantaneo, in cui il computer è il server Web front-end per l'ambiente SharePoint.
25. Fornire l'accesso completo a tutti gli utenti della cartella condivisa.
26. Specificare il percorso della cartella condivisa in Percorso file di backup per l'archiviazione del file di backup, quindi fare clic su **Avvia backup**.

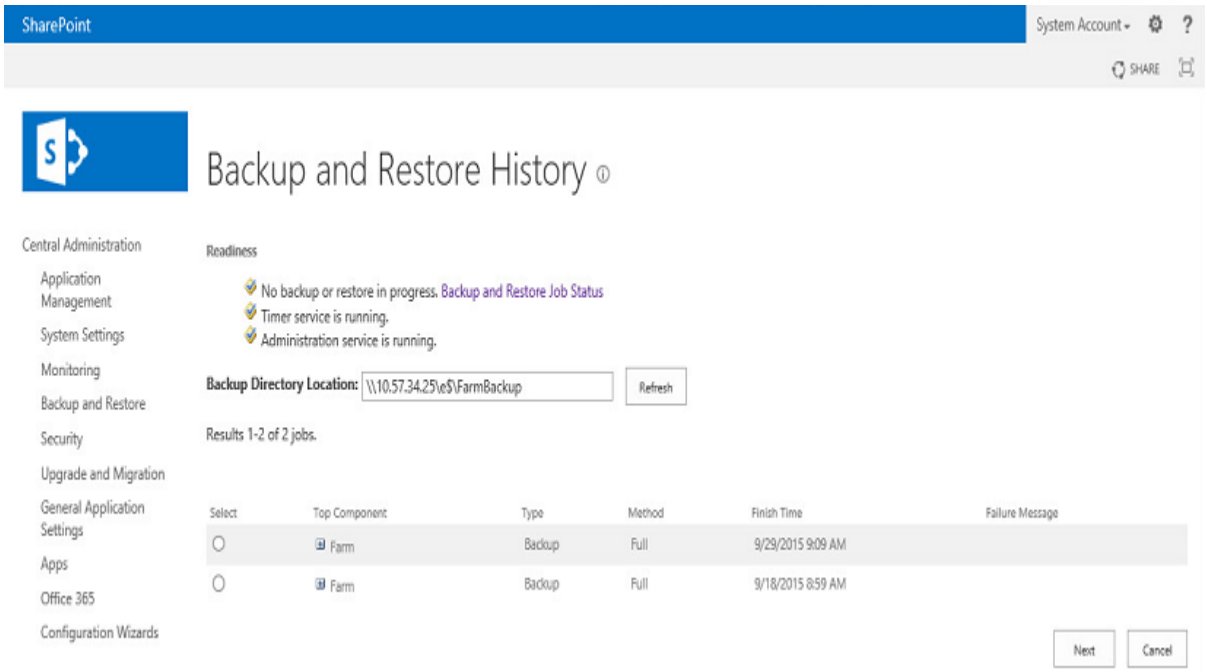


27. Attendere il completamento del processo di backup.



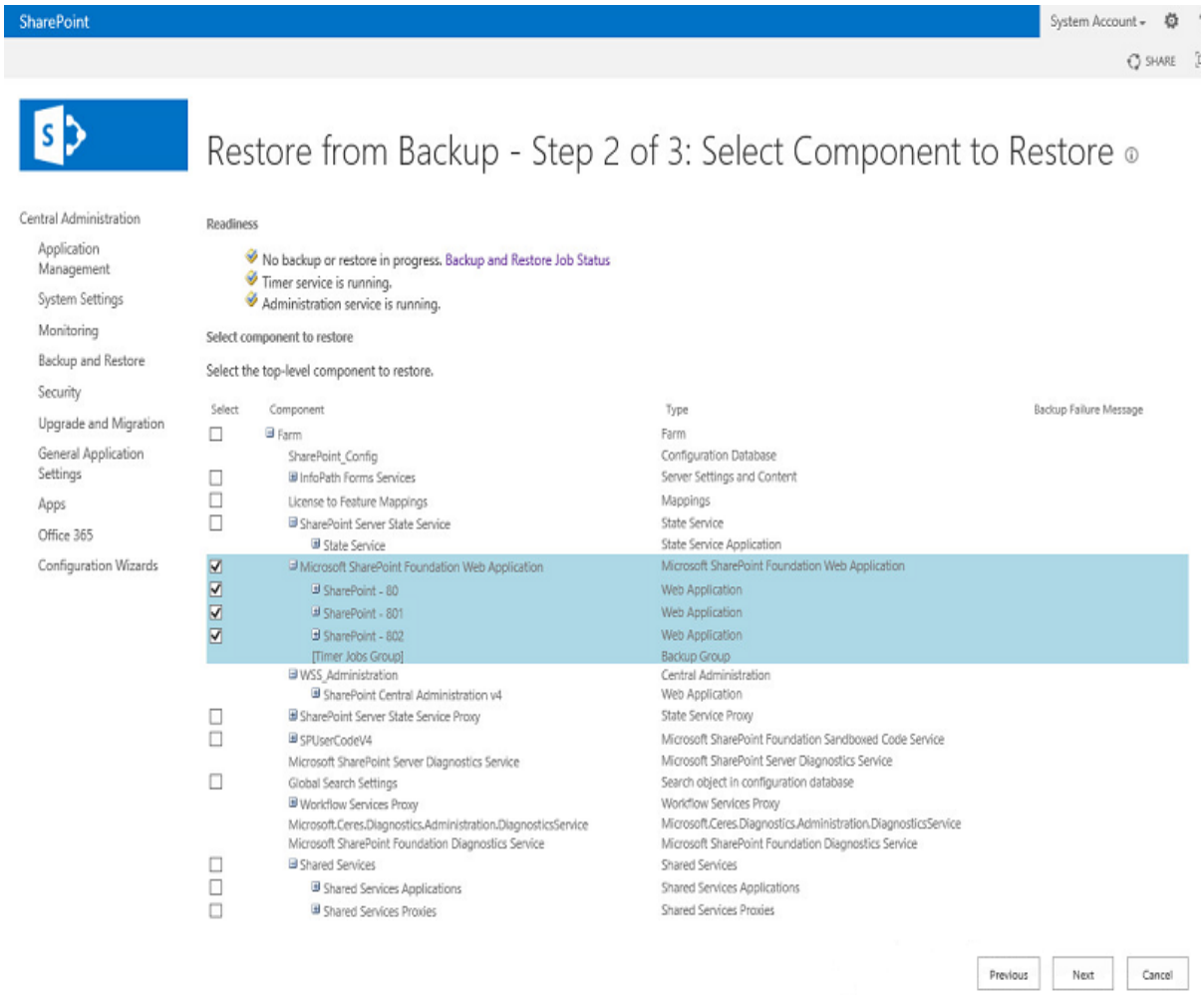
28. In seguito al completamento del processo di backup Farm, accedere al computer dei server Web front-end per l'ambiente SharePoint originale.
29. Aprire Amministrazione centrale, fare clic su Backup e ripristino, quindi selezionare il collegamento Ripristina da backup.
30. Specificare la cartella condivisa nel campo Percorso directory di backup, quindi fare clic su **Aggiorna**.

    Nota: La cartella condivisa è già stata creata in uno dei passaggi precedenti.
31. Selezionare l'istanza di backup dall'elenco della cronologia, quindi fare clic sul pulsante **Avanti**.



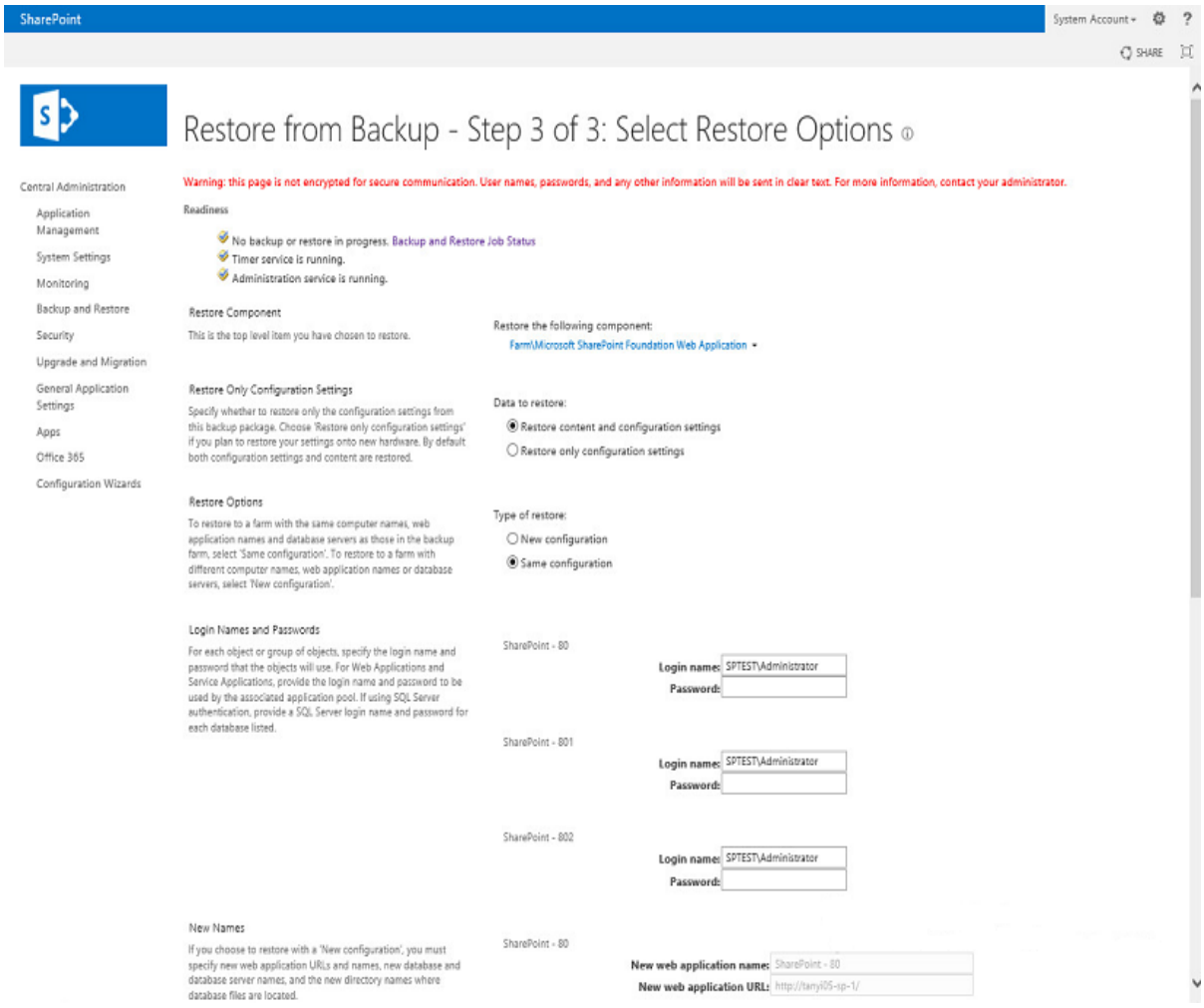
32. Selezionare la configurazione e il contenuto nella farm da ripristinare, quindi fare clic su **Avanti**.

    Ad esempio, selezionare tutti i componenti Farm, SharePoint Services componenti o Web Applications.



La pagina mostra varie opzioni per il servizio selezionato e la configurazione del contenuto.

33. Scegliere l'operazione desiderata:
    - Ripristinare le impostazioni di contenuto e configurazione o ripristinare solo le impostazioni di configurazione.
    - Sovrascrivere la configurazione o crearne una nuova nelle opzioni di ripristino.



34. Fare clic sul pulsante **Avvia ripristino** per avviare il processo corrispondente.

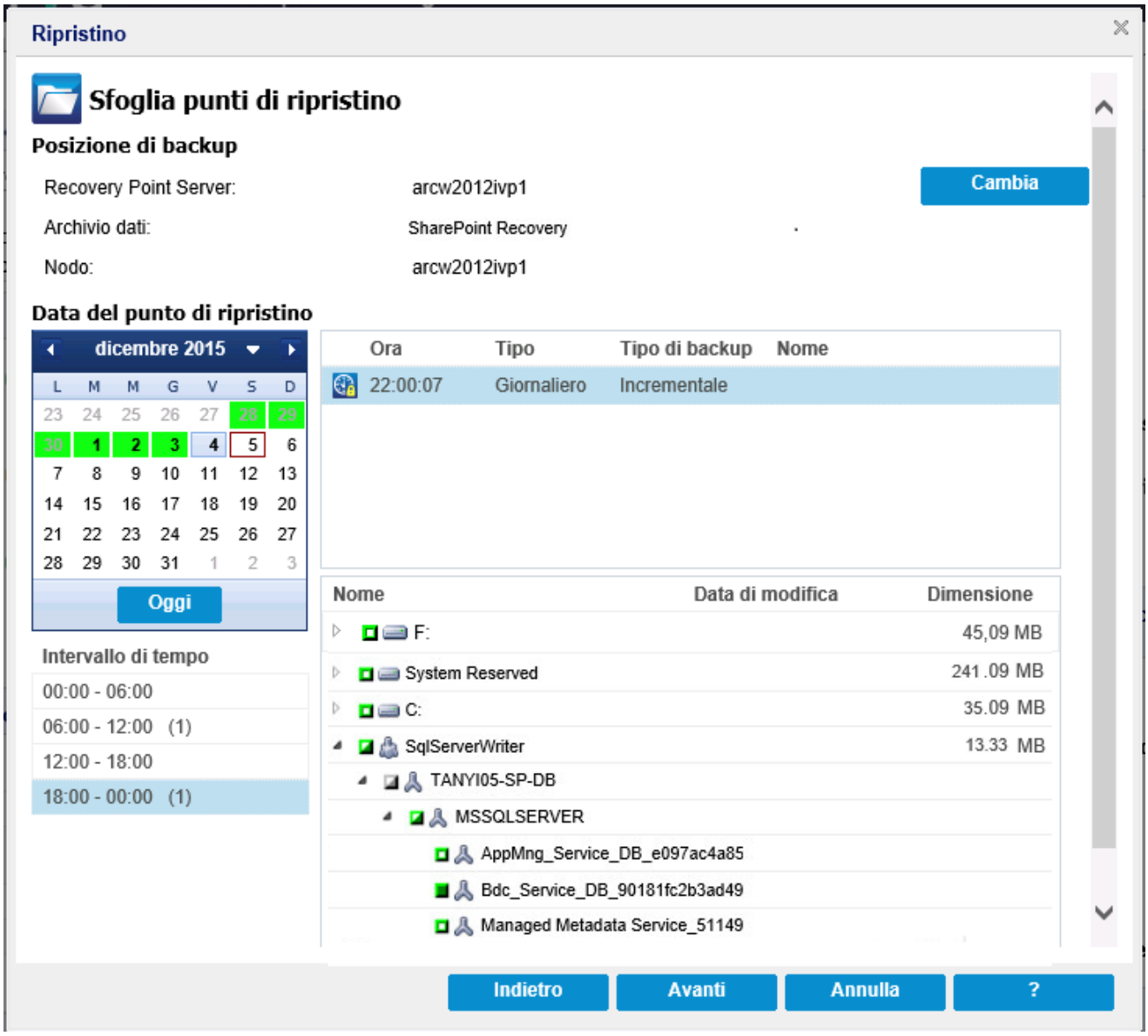
    Al termine del processo di ripristino, i componenti selezionati nella Farm vengono ripristinati.

Ripristino mediante l'interfaccia utente dell'agente Arcserve UDP

Effettuare le operazioni seguenti:

1. Accedere alla Console.
2. Fare clic con il tasto destro del mouse sul server del database utilizzato da SharePoint.
3. Fare clic su Ripristina.

   Viene aperta l'interfaccia utente dell'agente Arcserve UDP contenente il server di database.
4. Selezionare Sfoglia punti di ripristino
5. Fare clic su punto di ripristino che include il database, il quale verrà ripristinato.
6. Selezionare il database in SqlServerWriter/{SqlServerName}/{SqlServerInstantsName} da ripristinare.
7. Fare clic su Avanti.



8. Selezionare la destinazione di ripristino e fare clic su Avanti.

   Se si seleziona Ripristina nella posizione originale, il database viene ripristinato nella posizione originale. Se si seleziona Ripristina in posizione alternativa, il database viene ripristinato nella posizione specificata. Entrambi i database ripristinati verranno aggiunti automaticamente in SQL Server. Se si seleziona Solo file di dettagli, il file di dati del database e i file di registro vengono salvate nella posizione specificata.

9. Fare clic su Fine e attendere il completamento del processo di ripristino.

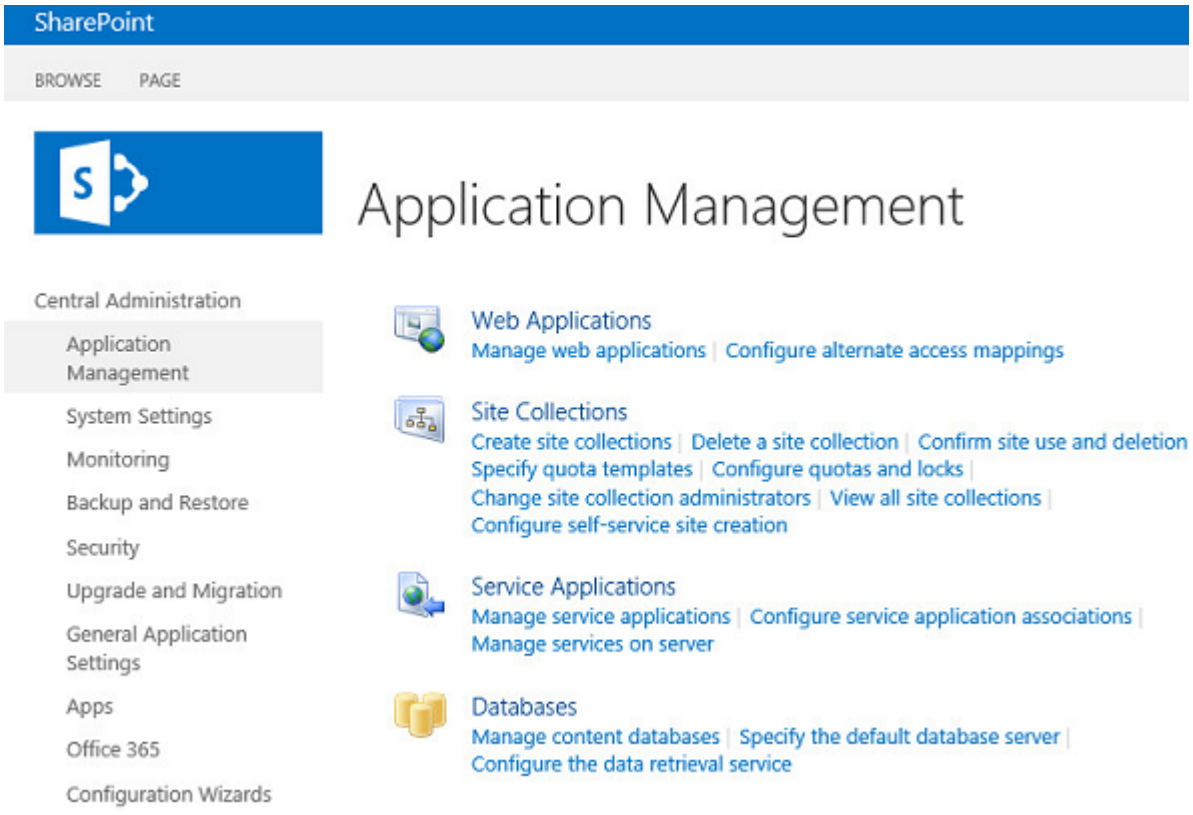
   Nota: Dopo aver selezionato Solo file di dettagli, associare il database. Attenersi alle operazioni riportate nella sezione Ripristino mediante database di montaggio dal punto di ripristino e verificare se il nuovo database di contenuto è associato

all'applicazione Web originale. In caso contrario, aggiungere il database di contenuto ripristinato all'applicazione Web originale.

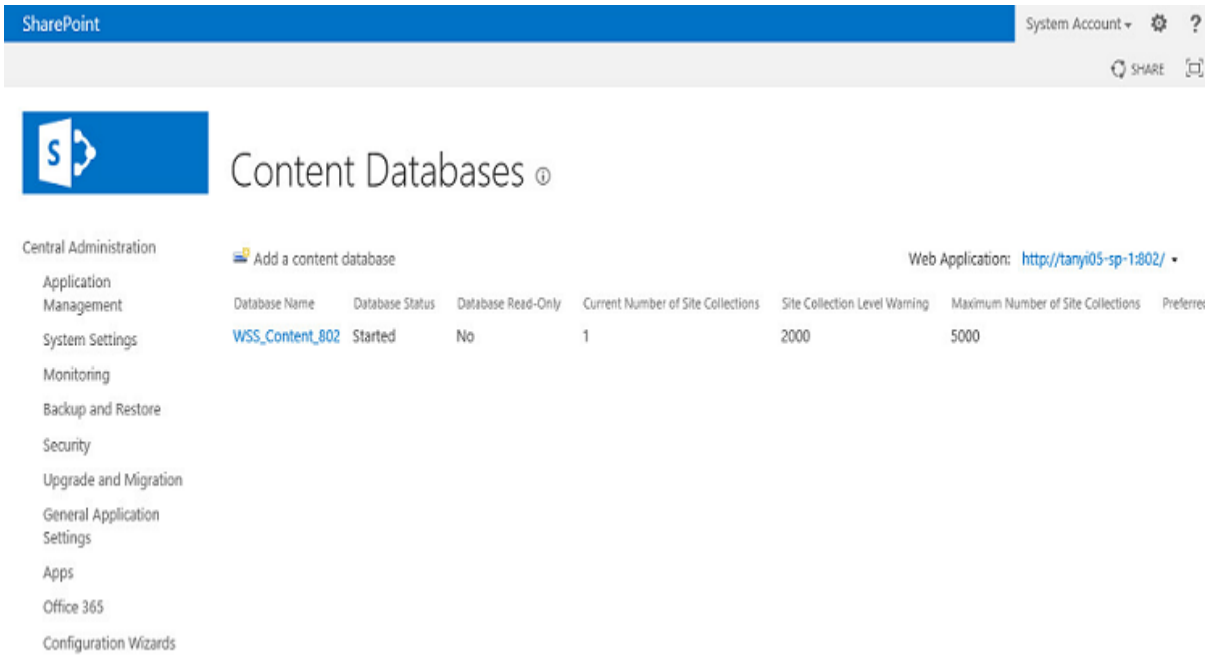
Aggiunta del database del contenuto ripristinato all'applicazione Web originale

Effettuare le operazioni seguenti:

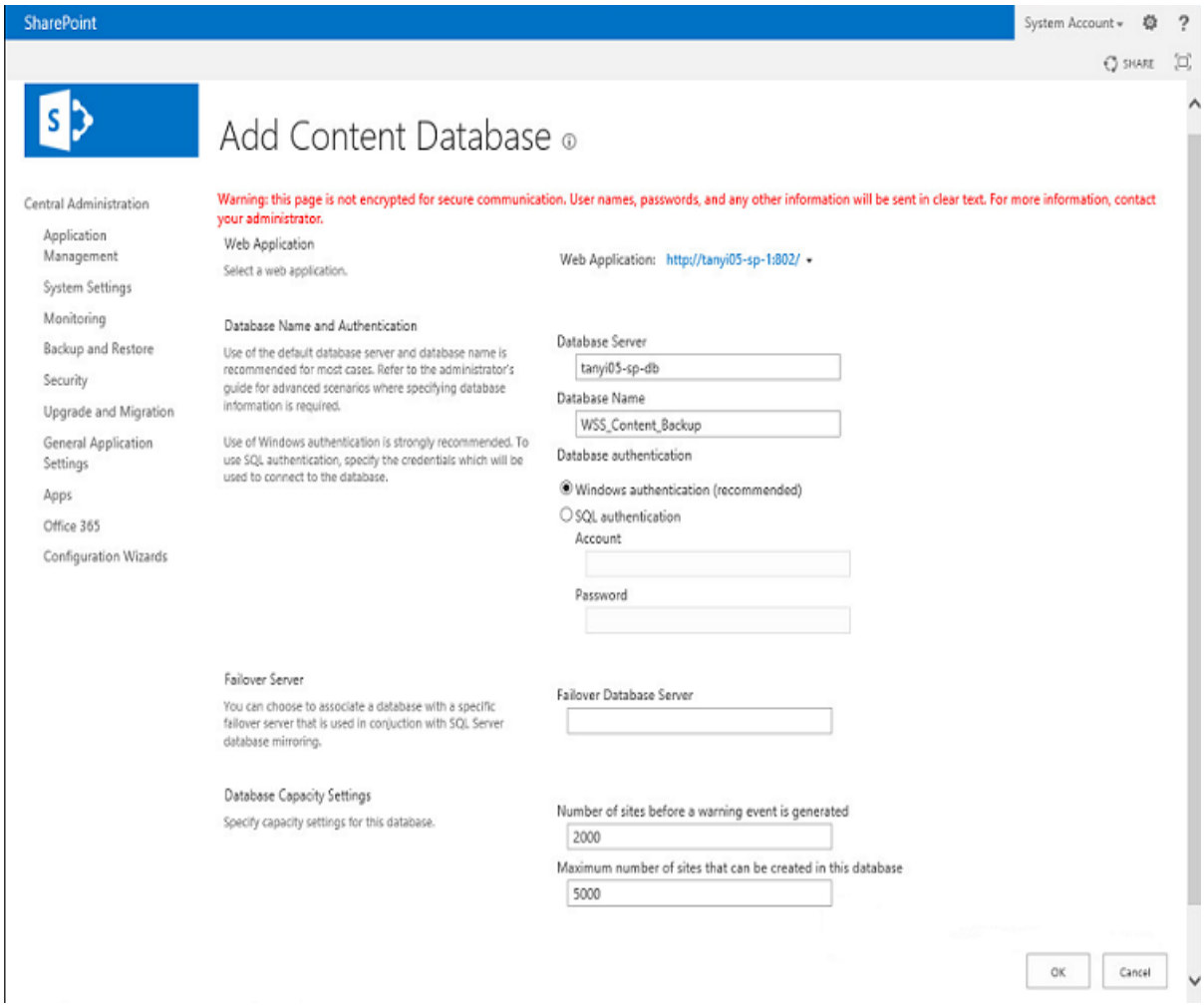
1. Aprire Amministrazione centrale SharePoint e selezionare Gestione applicazioni.



2. Selezionare i database del contenuto di gestione.



3. Selezionare l'applicazione Web e fare clic su Aggiungi database del contenuto.
4. Inserire i valori per il server di database e il nome del database (ad esempio, WSS_ Content_Backup), quindi fare clic su OK.

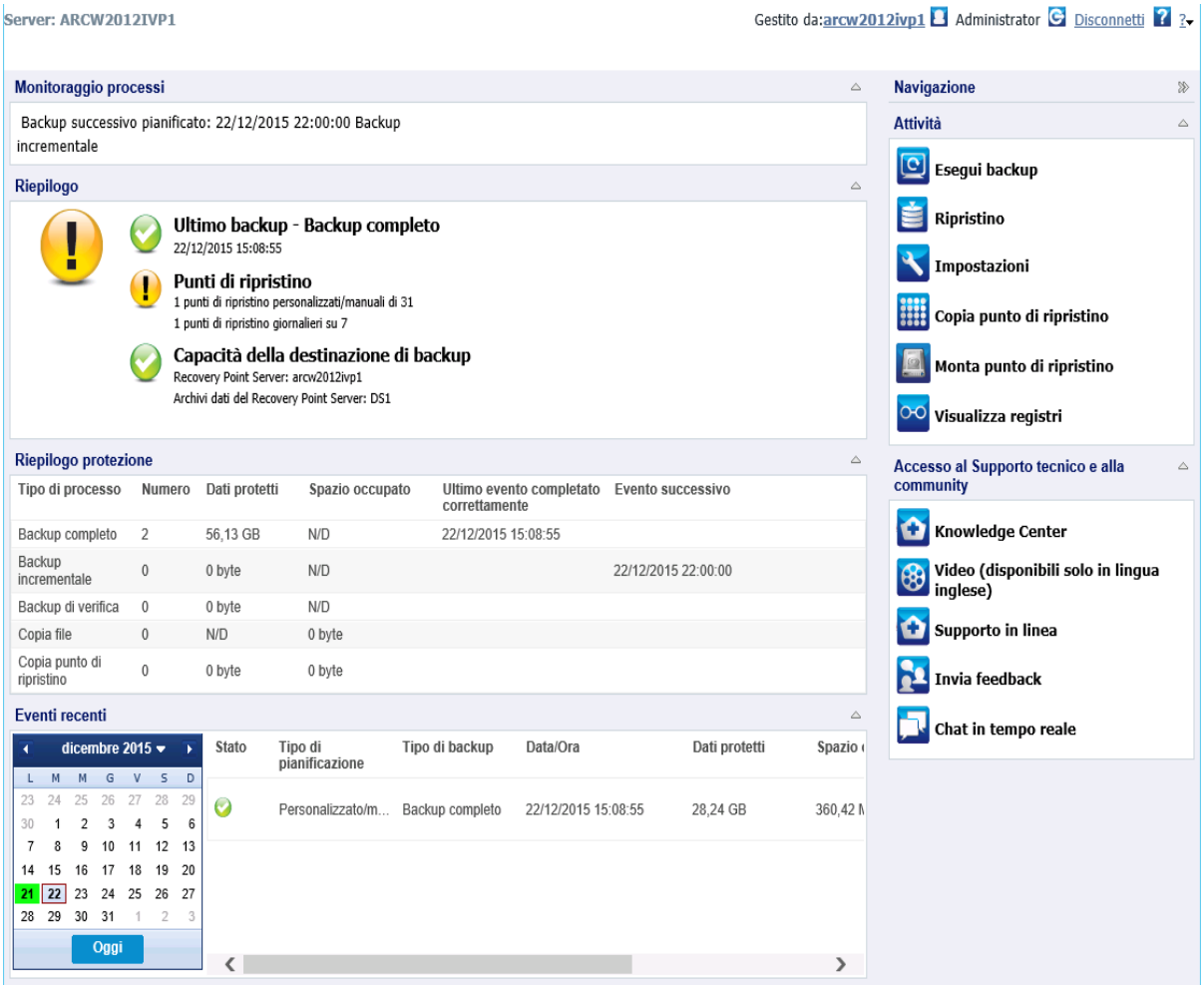


Il database del contenuto è stato associato all'applicazione Web originale.

Ripristino mediante montaggio del database da un punto di ripristino

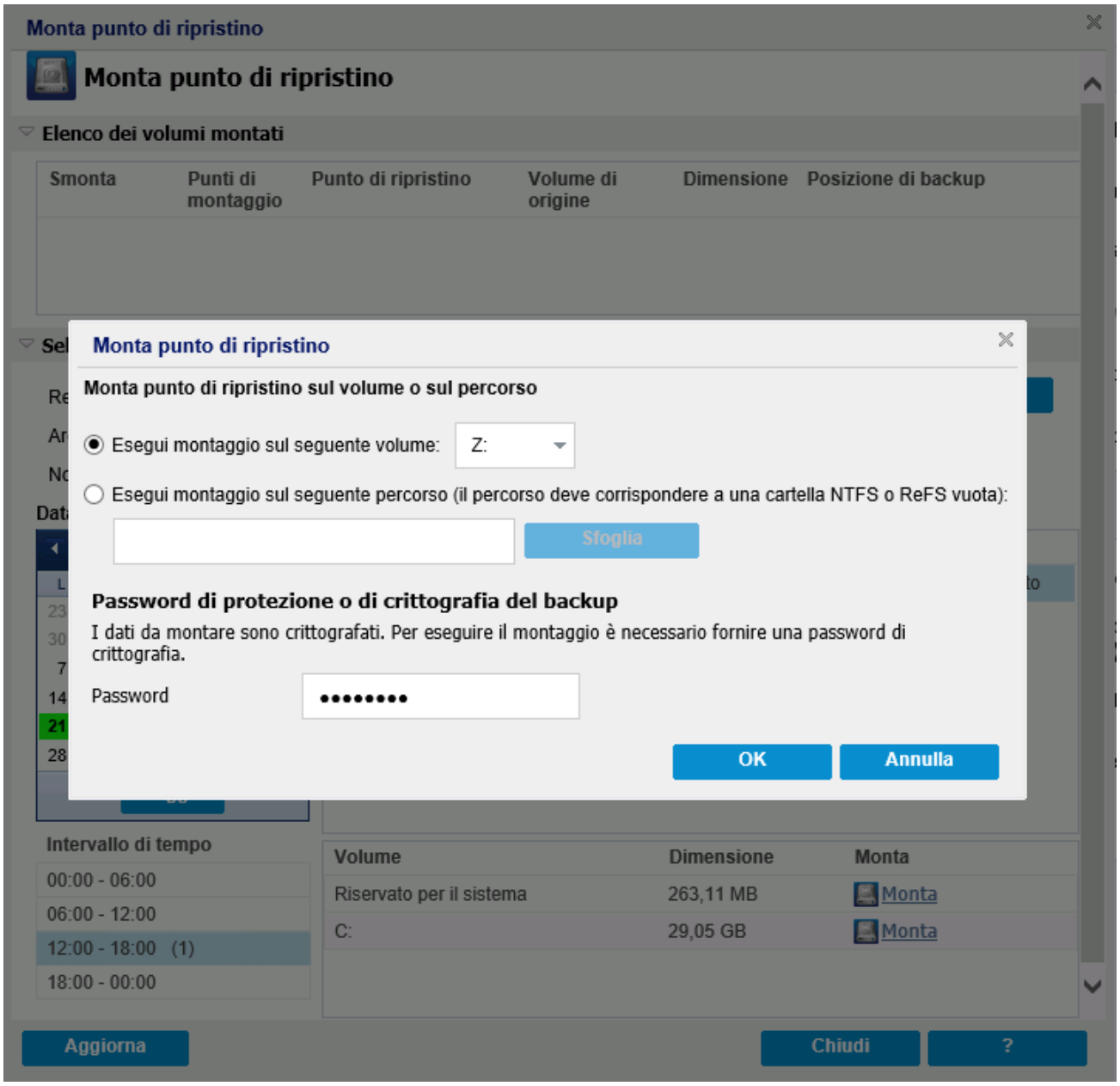
Effettuare le operazioni seguenti:

1. Aprire l'interfaccia utente dell'agente Arcserve UDP ospitato sul server del database.

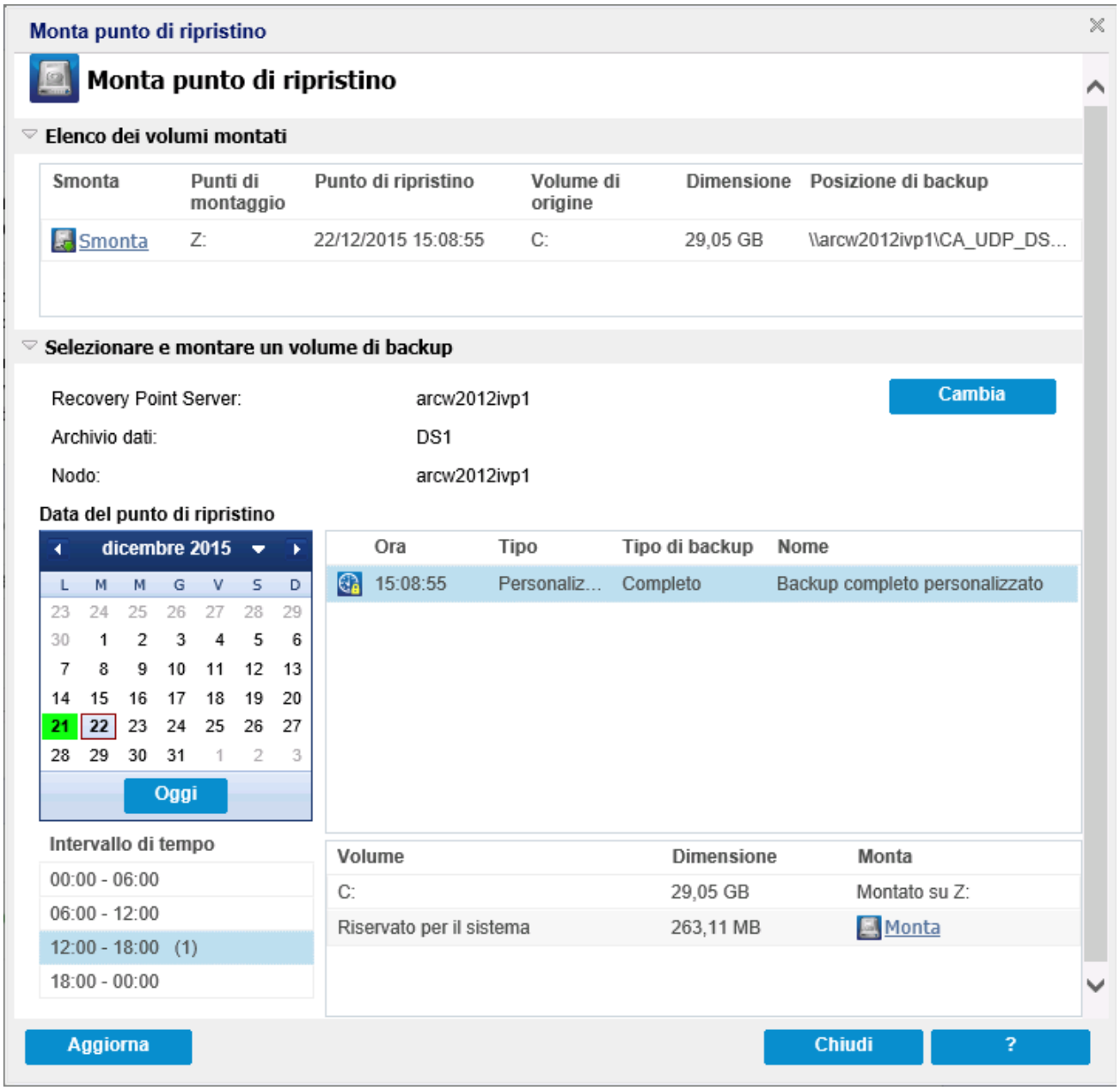


2. Fare clic su **Monta punto di ripristino** nel riquadro Attività.
3. Selezionare il volume in cui risiede il database del server SQL per SharePoint.

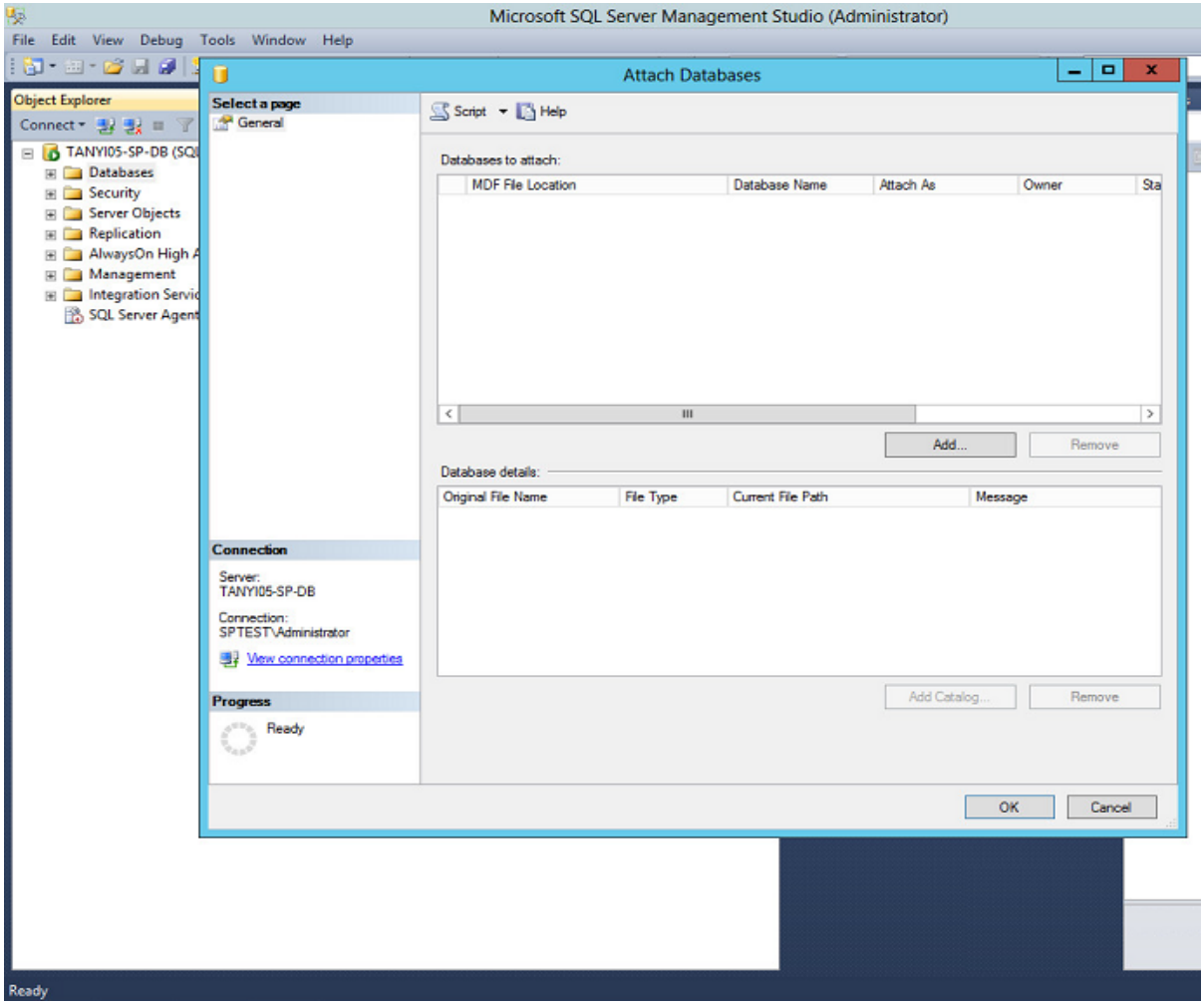
   Ad esempio, per impostazione predefinita, il file del database viene salvato in "C:\Programmi\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA". In tal caso, selezionare il volume C.
4. Selezionare il nome di un nuovo volume da montare nella finestra di dialogo seguente e fare clic su **OK**.



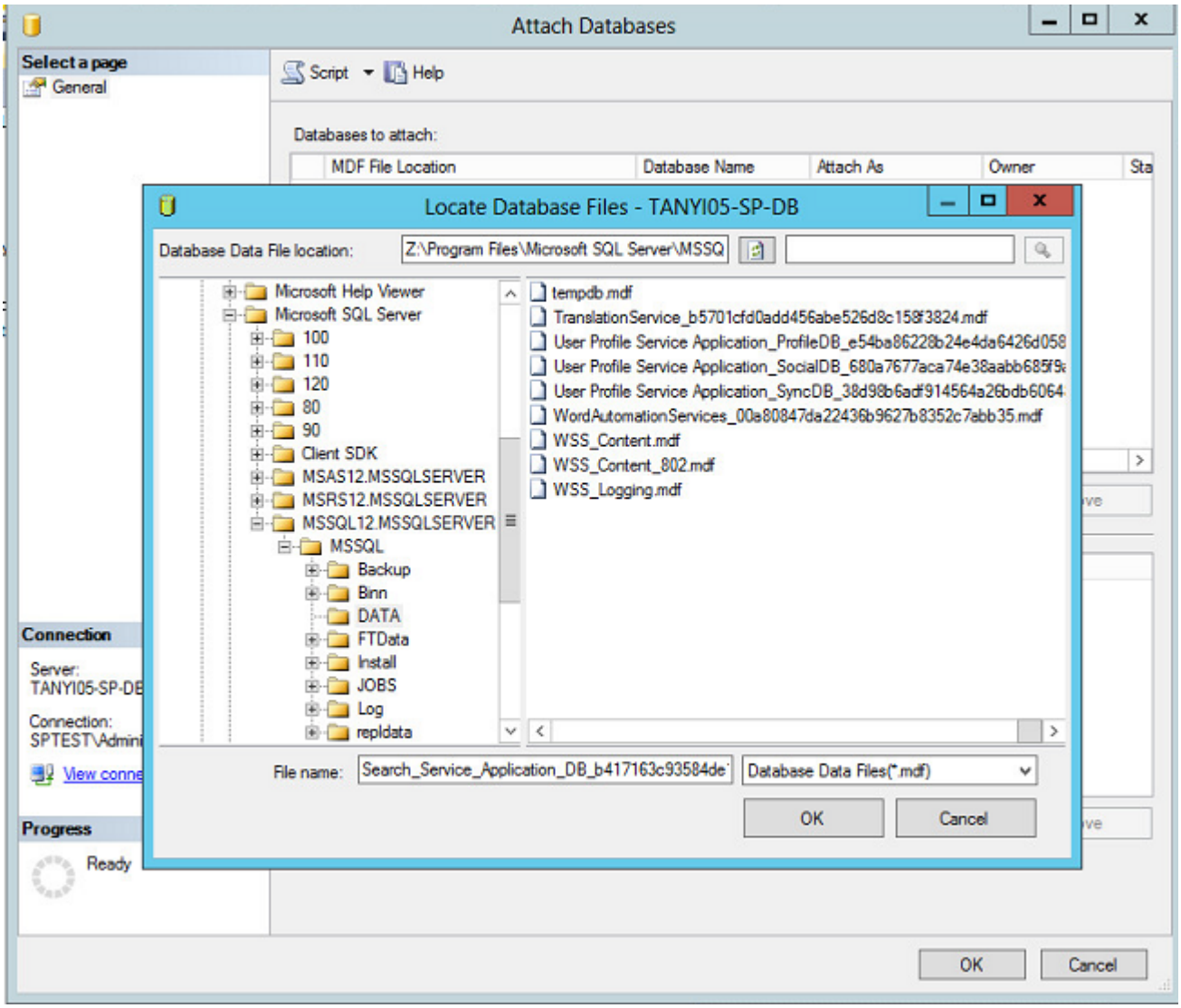
Il nuovo volume viene elencato nei volumi montati nell'interfaccia utente.



5. Aprire SQL Server Management Studio per associare il database di backup.
6. Fare clic con il pulsante destro del mouse sulla cartella del database, quindi selezionare Attach (Associa).



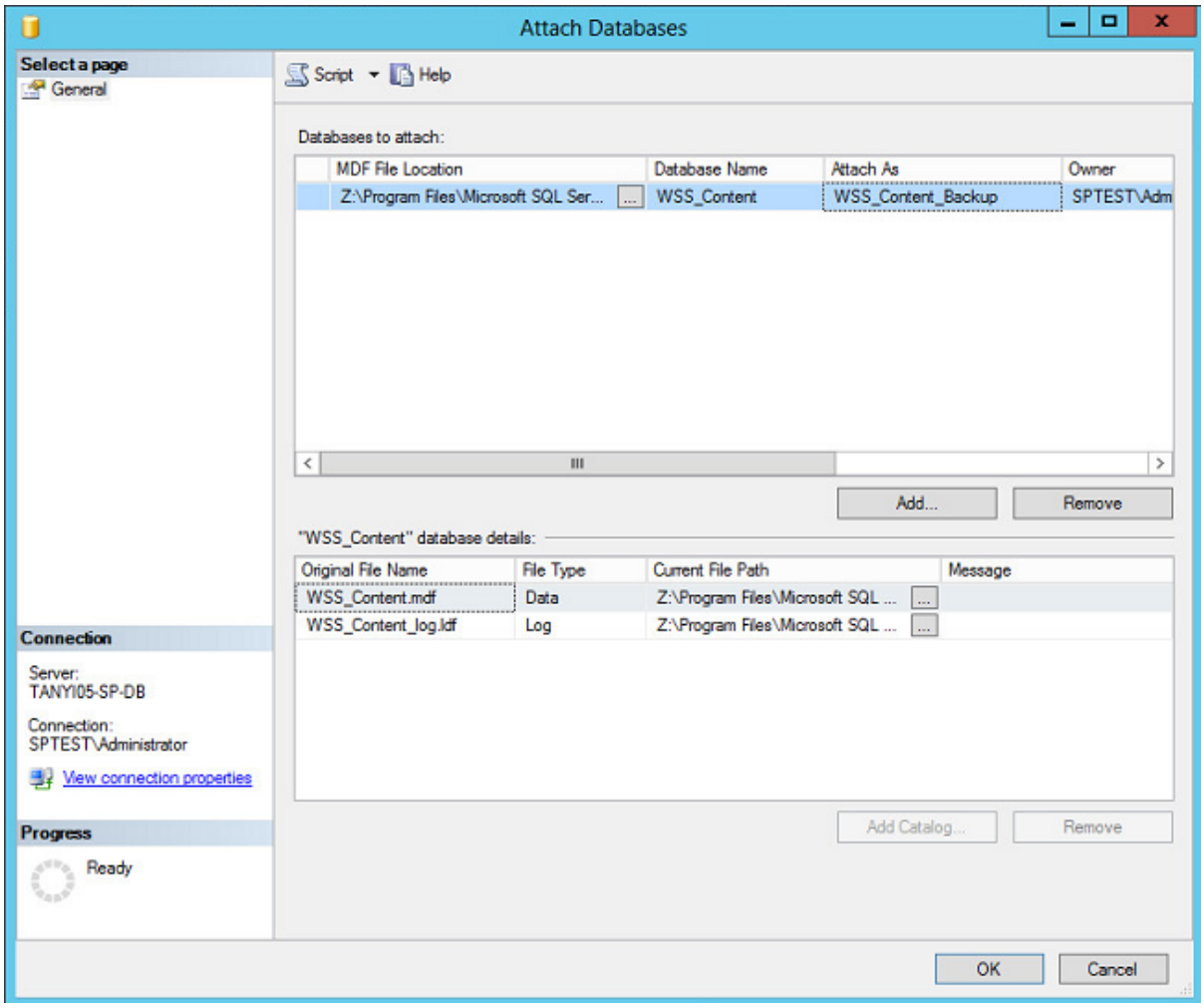
7. Fare clic su Aggiungi per selezionare il file del database che si desidera associare.



8. Se il volume montato è Z, selezionare la posizione del file di dati del database "Z:\Programmi\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA".
9. Selezionare il file denominato "WSS_Content.mdf" e fare clic su OK.

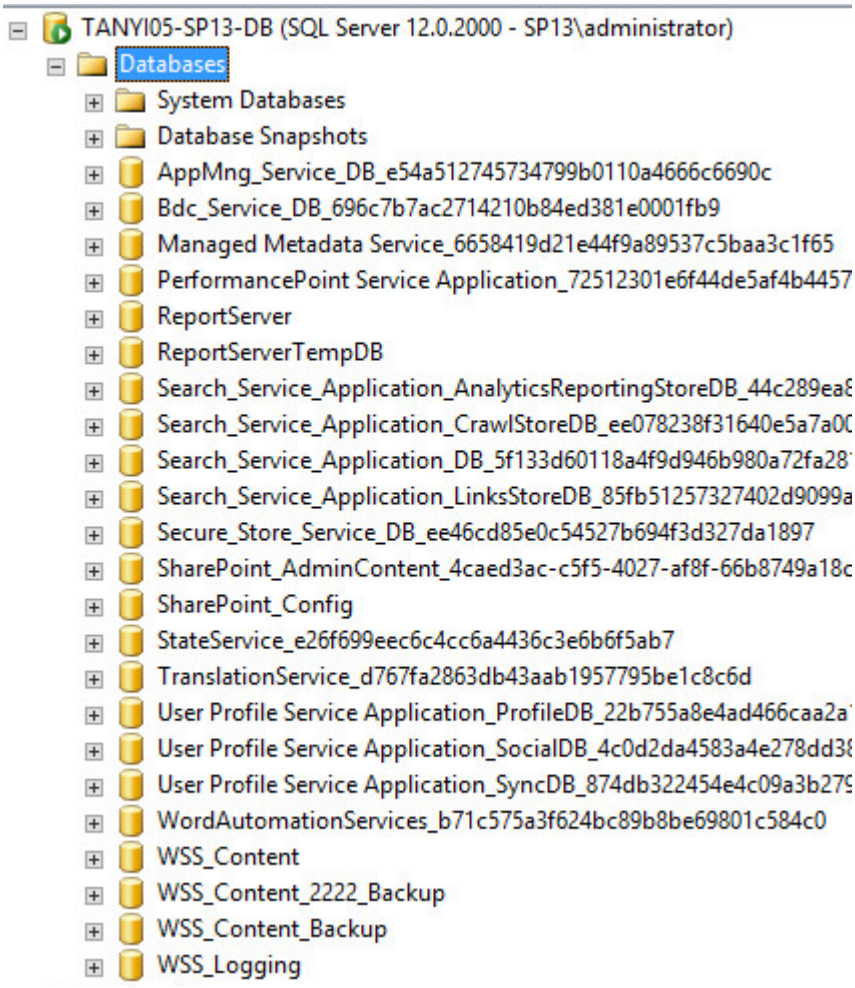
   Nota: "WSS_Content.mdf" è il nome del file di dati del database predefinito per l'applicazione Web SharePoint. Se si desidera ripristinare un altro database creato da una nuova applicazione Web, utilizzare il nome del file di dati del database interessato.
10. Fare clic sulla colonna Attach as (Associa come) per immettere il nome del database (ad esempio, "WSS_Content_Backup") e fare clic su OK.

    Nota: Prima di ripristinare un database del contenuto, assicurarsi che il relativo nome non esista in nessuna delle altre applicazioni Web.

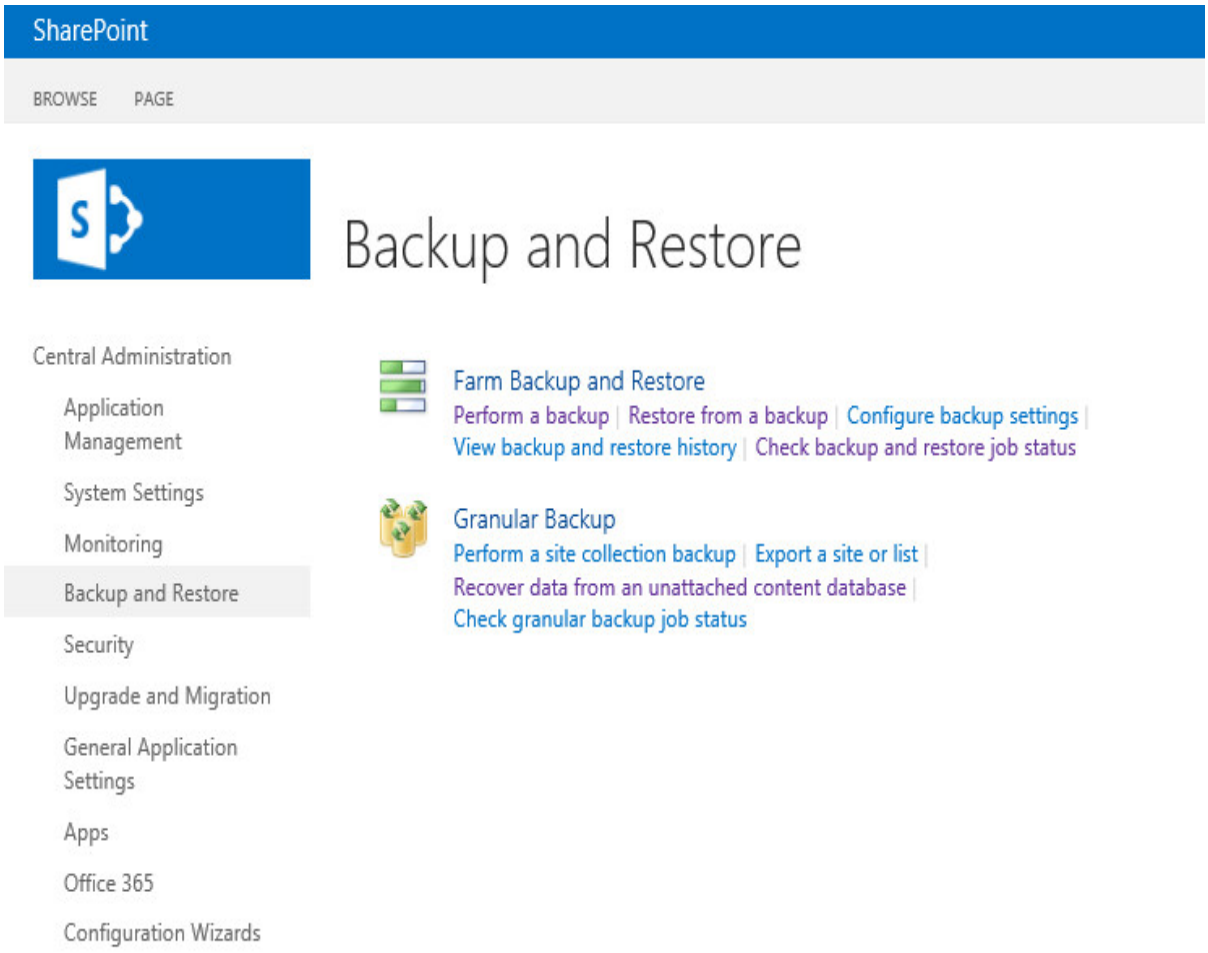


Il nuovo database è associato alla cartella Database.

Nota: Il nuovo database non è associato ad alcuna applicazione Web.

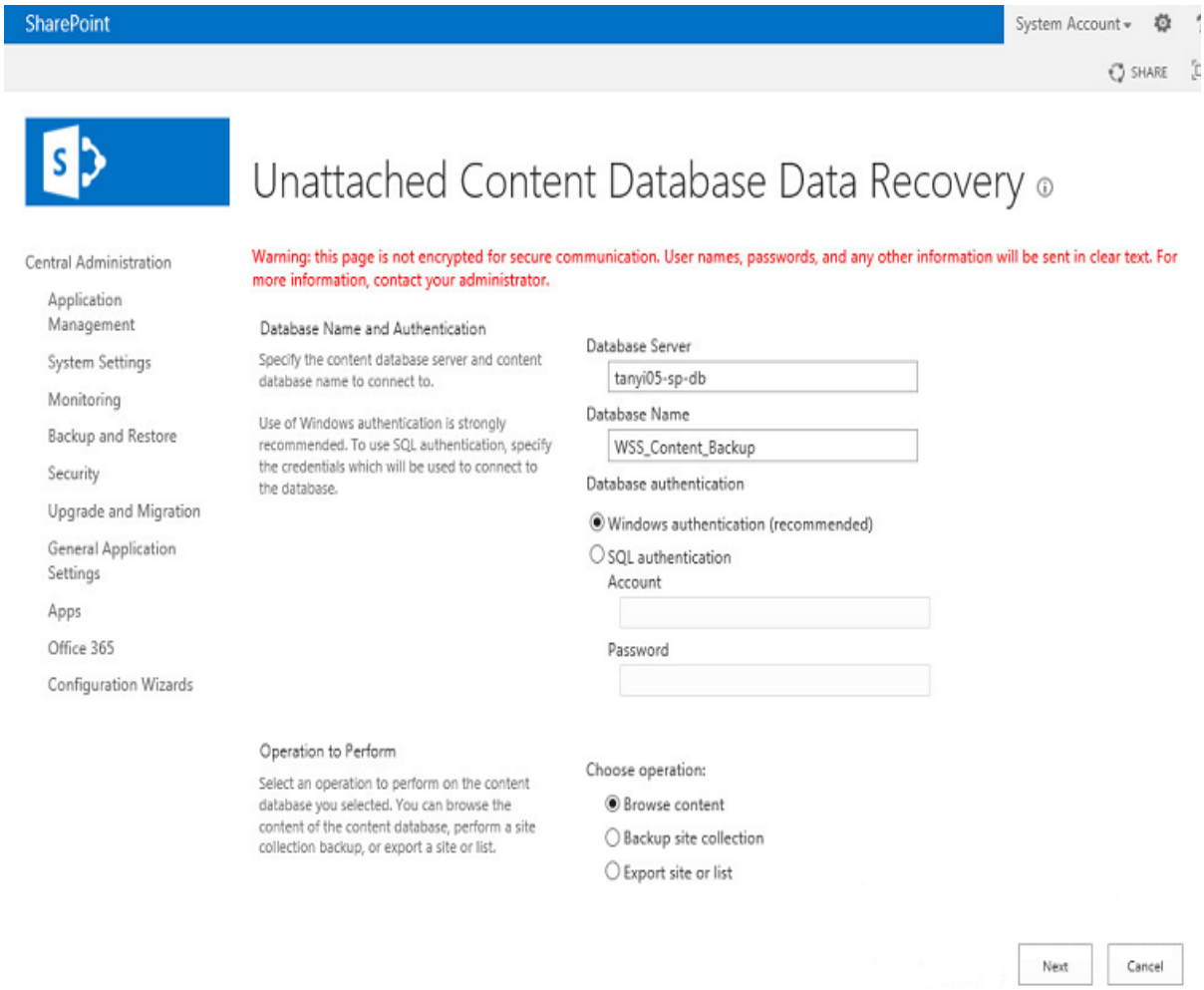


11. Accedere al computer che funge da server Web front-end nella farm del server SharePoint.
12. Aprire Amministrazione centrale e fare clic sull'intestazione Backup e ripristino.



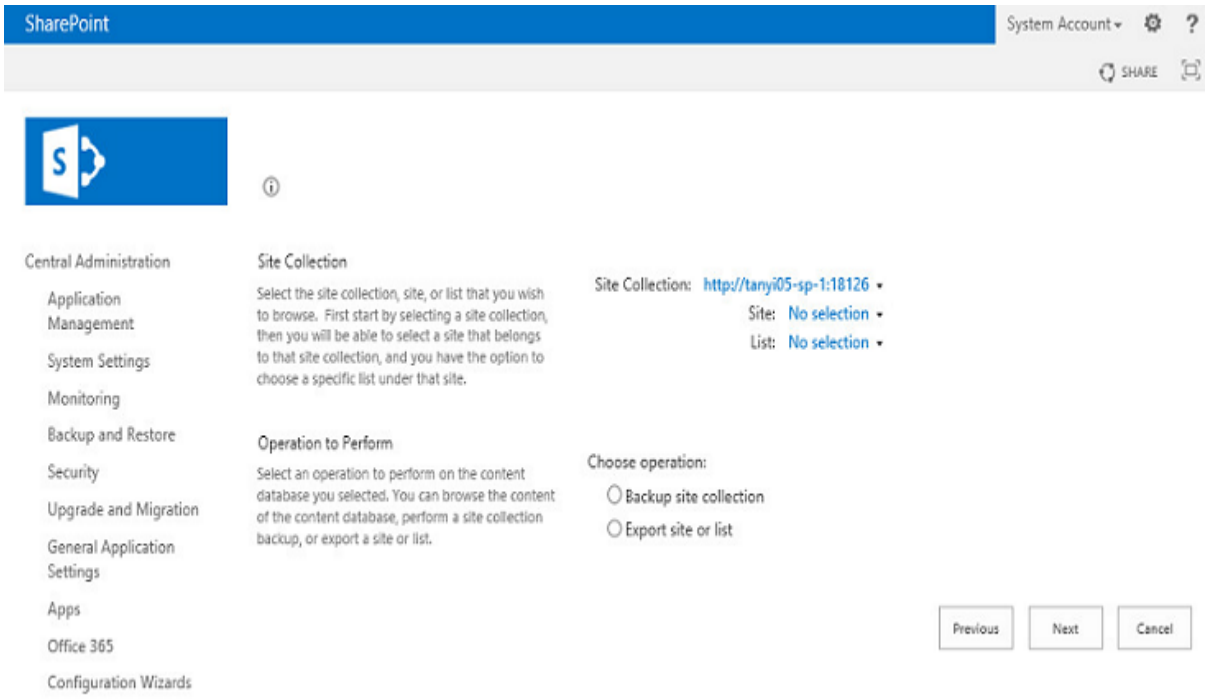
13. Fare clic sul collegamento Recover Data from an Unattached Content Database (Recupera dati da un database del contenuto non collegato), fornire il nome del server SQL e il nome del database non collegato e utilizzare l'autenticazione di Windows.
14. Selezionare l'opzione Esplora contenuto e fare clic sul pulsante **Avanti**.

    Nota: Il nome del server SQL è il nome dei server di database utilizzati dalla farm del server SharePoint; il nome del database è il nome del nuovo database collegato.



15. Scegliere se si desidera eseguire il backup della raccolta di siti o esportare il sito e l'elenco selezionato.

    Nota: Per impostazione predefinita, se il database è un database del contenuto non collegato, l'URL della raccolta siti ancora include il numero di porta dell'applicazione Web Amministrazione centrale.



È stato eseguito il ripristino mediante montaggio del database da un punto di ripristino.

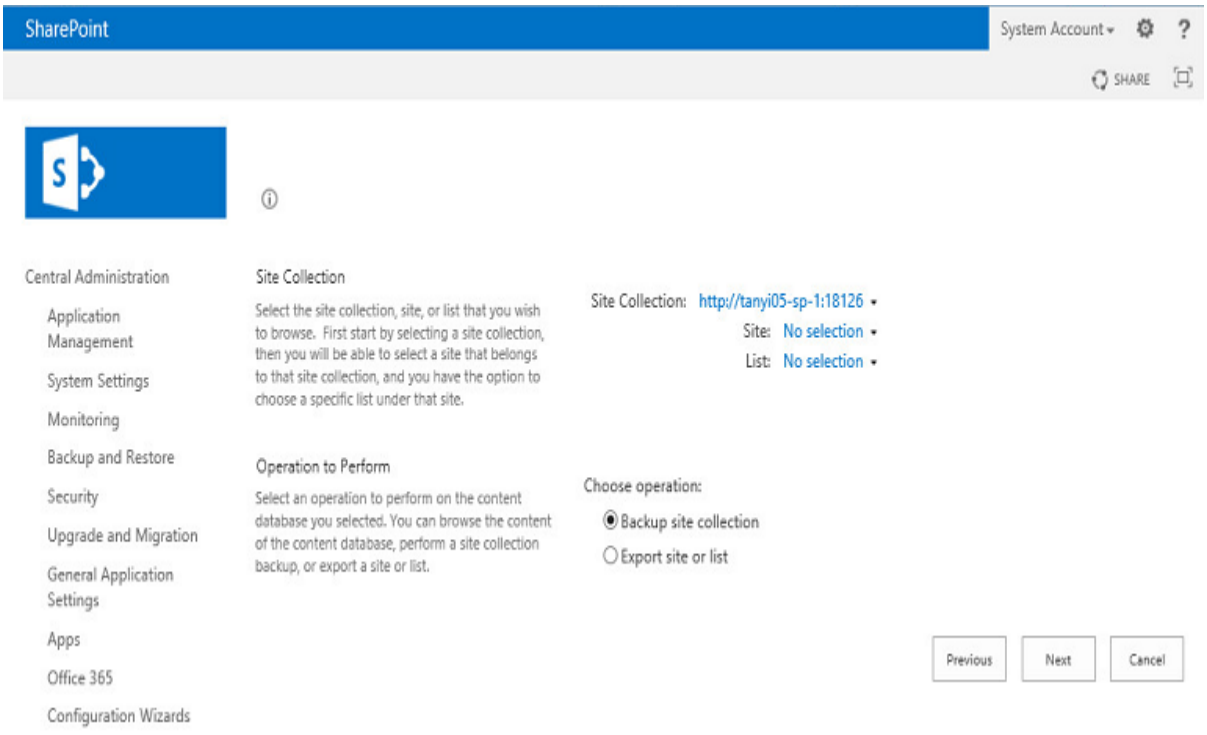
Ripristino di una raccolta siti

Effettuare le operazioni seguenti:

1. Ripristinare il contenuto della raccolta siti da un database del contenuto non collegato.

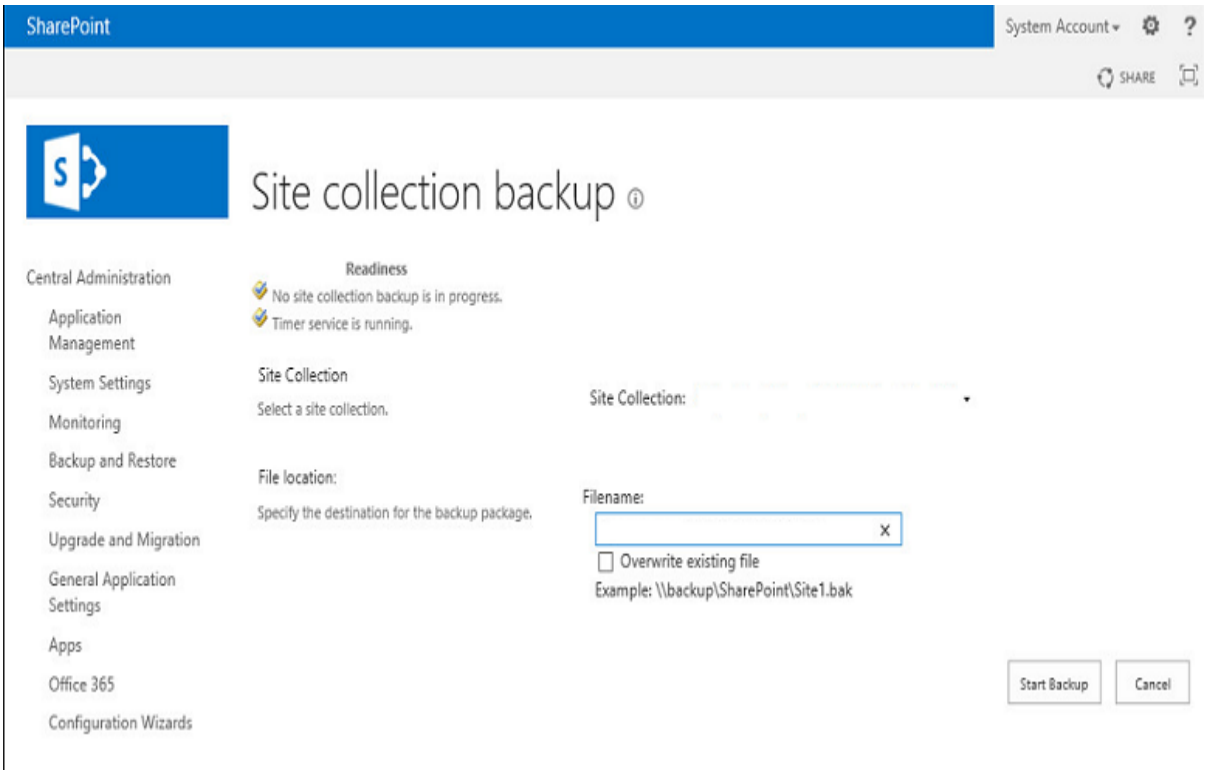
   Da Amministrazione centrale

   a. Selezionare l'opzione Backup raccolta siti e fare clic sul pulsante Avanti.



   b. Selezionare la raccolta di siti e fornire la posizione del file per il pacchetto di backup.

   c. Selezionare Sovrascrivi file esistenti



d. Fare clic sul pulsante Avvia backup per avviare il backup.

   Viene eseguito il backup della raccolta di siti in un file.

Utilizzare i comandi PowerShell

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

   ConnectAsUnattachedDatabase: specifica che vengono restituiti solo i database non collegati nella farm.

   DatabaseName: specifica il nome del database del contenuto.

   DatabaseServer: indica il nome del server host per il database del contenuto specificato nel parametro DatabaseName.

   Per ulteriori informazioni, consultare l'articolo di Microsoft.

b. Backup-SPSite -Identity xxxx -Path xxxx

   Identity: specifica l'URL o il GUID della raccolta siti di cui eseguire il backup.

   Path: specifica il percorso completo del file di backup (ad esempio, C:\-backup\sitecollection.bak).

   Per ulteriori informazioni, consultare l'articolo di Microsoft.

2. Fare clic su SharePoint Management Shell per avviare la console.
3. Utilizzare i comandi PowerShell per ripristinare la raccolta siti.

```
Restore-SPSite -Identity xxxx -Path xxxx
```

Identity: specifica il percorso URL in cui viene ripristinata la raccolta siti (ad esempio, http://www.contoso.com).

Path: specifica un percorso valido della posizione di backup(ad esempio, C:\-backup\sitecollection.bak).

Per ulteriori informazioni, consultare l'articolo di Microsoft.

Nota: non è possibile eseguire il ripristino di una raccolta siti nella posizione originale. È possibile procedere come segue:

a. New-SPContentDatabase -Name xxxx -DatabaseServer xxxx -WebApplication xxxx

   Name: specifica il nuovo database del contenuto da creare all'interno della farm.

   DatabaseServer: indica il nome del server host per il database del contenuto specificato nel parametro Name.

   WebApplication: collega il database del contenuto all'applicazione Web SharePoint specificata.

b. Restore-SPSite -Identity xxxx -Path xxxx -GradualDelete -DatabaseServer xxxx -DatabaseName xxxx

   Identity: specifica il percorso URL in cui viene ripristinata la raccolta siti (ad esempio, http://www.contoso.com).

   Path: specifica un percorso valido della posizione di backup(ad esempio, C:\-backup\sitecollection.bak).

   GradualDelete: specifica che la raccolta di siti sovrascritta con il parametro Force dovrebbe essere eliminata progressivamente nel corso del tempo tramite un processo timer, invece di essere eliminata completamente in una sola operazione. Ciò consente di ridurre l'impatto sulle prestazioni dei prodotti SharePoint 2010 e sul server SQL.

   DatabaseName: specifica il database del contenuto del server SQL in cui verranno archiviati i dati della raccolta siti.

   DatabaseServer: specifica il nome del server SQL in cui si trova il database del contenuto specificato nel parametro DatabaseName.

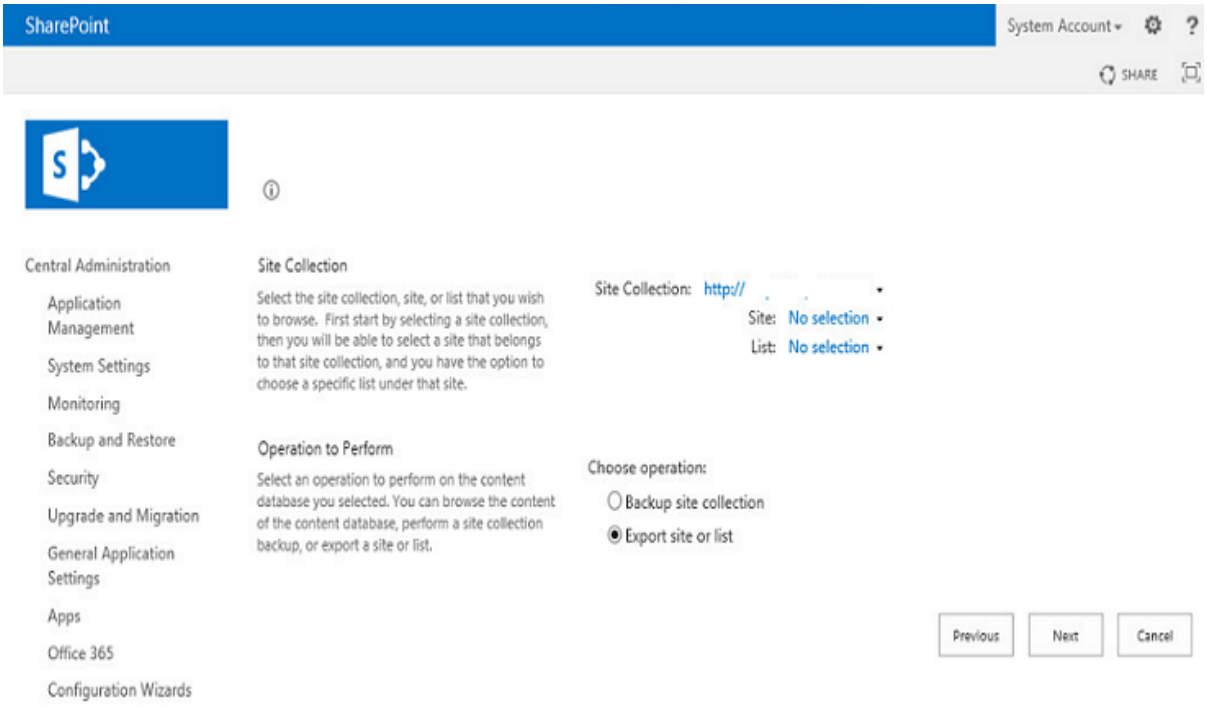
Ripristino di un sito

Effettuare le operazioni seguenti:

1. Ripristinare il contenuto del sito da un database del contenuto non collegato.

   Da Amministrazione centrale

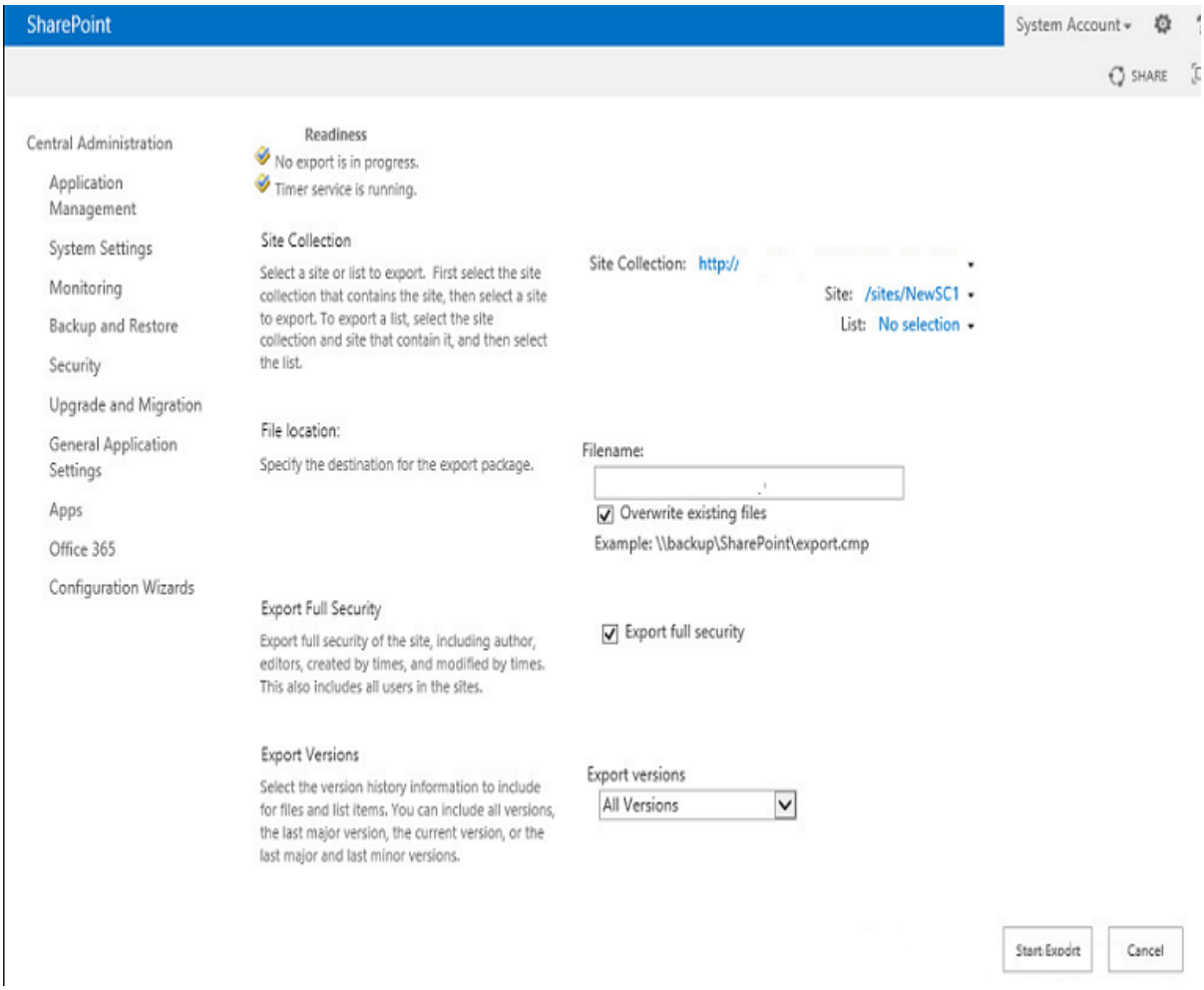
   a. Selezionare l'opzione Esporta sito o elenco e fare clic sul pulsante Avanti.



   b. Selezionare il sito e fornire la posizione dei file del pacchetto di esportazione.

      Esempio: Il nome del sito da ripristinare è TestSite1 e l'URL è /TestSite1/.

   c. Selezionare le opzioni per la protezione e le versioni (per impostazione sono incluse tutte le versioni).



d. Fare clic sul pulsante Avvia esportazione per avviare il processo. Il sito viene quindi esportato in un file.

Utilizzare i comandi PowerShell

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

ConnectAsUnattachedDatabase: specifica che vengono restituiti solo i database non collegati nella farm.

DatabaseName: specifica il nome del database del contenuto.

DatabaseServer: indica il nome del server host per il database del contenuto specificato nel parametro DatabaseName.

Per ulteriori informazioni, consultare l'articolo di Microsoft.

b. Impostazione dell'oggetto da esportare

$ExportObject = New-Object Microsoft.SharePoint.Deployment.SPExportObject

$ExportObject.Type = [Microsoft.SharePoint.Deployment.SPDeploymentObjectType]::Web

$ExportObject.Url = $SiteUrl

$SiteUrl: specifica il percorso URL in cui verrà eseguito il backup del sito.

c. Configurazione delle impostazioni di esportazione

$ExportSettings = New-Object Microsoft.SharePoint.Deployment.SPExportSettings

$ExportSettings.UnattachedContentDatabase = $database

$ExportSettings.SiteUrl = $CAUrl

$CAUrl: specifica l'URL del sito di amministrazione centrale.

$ExportSettings.FileLocation = $ExportPath

$ExportSettings.LogFilePath = $ExportPath

$ExportPath: specifica il percorso in cui salvare il file di backup (ad esempio, C:\backup).

$ExportSettings.BaseFileName = $ExportFile

$ExportFile: specifica il nome del file di backup (ad esempio, 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)

Backup del sito in un file.

$ExportJob.Run()

Per ulteriori informazioni, consultare l'articolo di Microsoft.

2. Fare clic su SharePoint Management Shell per avviare la console.
3. Utilizzare i comandi PowerShell per ripristinare il sito nella posizione di origine o nella nuova posizione.

```
Import-SPWeb -Identity xxxx -Path xxxx -Inclu-
deUserSecurity:$true -UpdateVersions:xxxx
```

Identity: specifica l'URL o il GUID Web in cui eseguire l'importazione, ad esempio, http://www.contoso.com.

Path: specifica il nome del file di importazione, ad esempio, C:\backup\list.cmp.

IncludeUserSecurity: consente di mantenere le impostazioni di protezione utente, ad eccezione degli elenchi SharePoint che non rispettano i set di autorizzazioni a livello di elemento ed ereditarietà.

UpdateVersions: indica le modalità di risoluzione dei casi in cui è presente una versione del file da importare già esistente sul sito interessato. È possibile selezionare una delle opzioni seguenti:

Aggiungi: consente di aggiungere il file come nuova versione.

Sovrascrivi: sovrascrive il file corrente e tutte le relative versioni (eseguendo prima l'eliminazione e poi l'inserimento).

Ignora: ignora il file se già presente nella destinazione. Il nuovo file non viene aggiunto.

Il valore predefinito è Aggiungi.

Per ulteriori informazioni, consultare l'articolo di Microsoft.

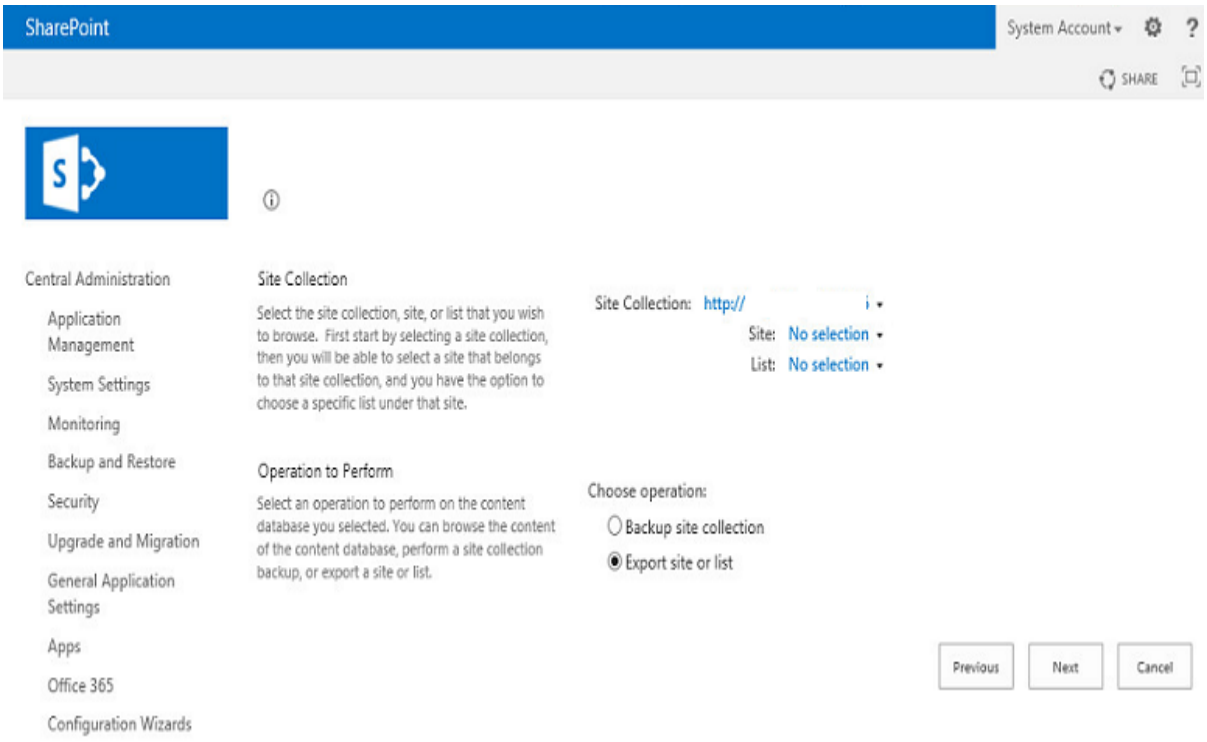
Ripristino di un elenco o una libreria

Effettuare le operazioni seguenti:

1. Ripristinare il contenuto dell'elenco o della libreria dal database del contenuto non collegato.

   Da Amministrazione centrale

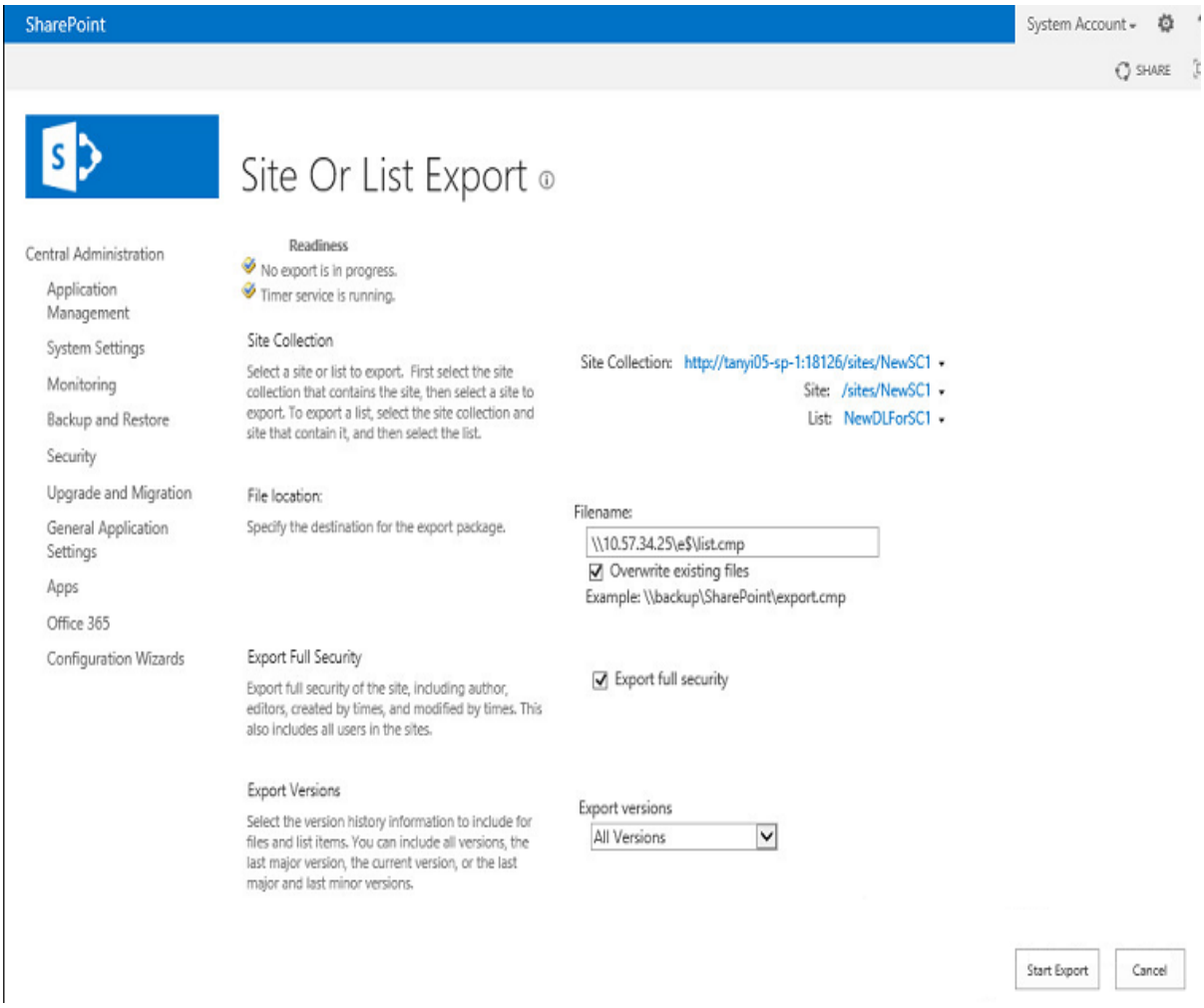
   a. Selezionare l'opzione Esporta sito o elenco e fare clic su **Avanti**.



   b. Selezionare il sito e l'elenco e fornire la posizione dei file del pacchetto di esportazione.

      Esempio: Il nome dell'elenco o della libreria da ripristinare è NewList1 e l'URL è /TestSite1/NewList1.

   c. Selezionare le opzioni per la protezione e le versioni (per impostazione sono incluse tutte le versioni).



d. Fare clic su **Avvia esportazione** per avviare il processo

   L'elenco o la libreria vengono esportati in un file.

Utilizzare i comandi PowerShell

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

   ConnectAsUnattachedDatabase: specifica che vengono restituiti solo i database non collegati nella farm.

   DatabaseName: specifica il nome del database del contenuto.

   DatabaseServer: indica il nome del server host per il database del contenuto specificato nel parametro DatabaseName.

   Per ulteriori informazioni, consultare l'articolo di Microsoft.

b. Impostazione dell'oggetto da esportare

   $ExportObject = New-Object Microsoft.SharePoint.Deployment.SPExportObject

$ExportObject.Type = [Microsoft.SharePoint.Deployment.SPDeploymentObjectType]::List

$ExportObject.Url = $ListUrl

$ListUrl: specifica il percorso URL in cui verrà eseguito il backup dell'elenco o della libreria. Se si tratta di un elenco, è possibile utilizzare il parametro "/Lists/{ListName}". Se si tratta di una libreria, utilizzare il parametro "/{LibraryName}".

c. Configurazione delle impostazioni di esportazione

$ExportSettings = New-Object Microsoft.SharePoint.Deployment.SPExportSettings

$ExportSettings.UnattachedContentDatabase = $database

$ExportSettings.SiteUrl = $CAUrl

$CAUrl: specifica l'URL del sito di amministrazione centrale.

$ExportSettings.FileLocation = $ExportPath

$ExportSettings.LogFilePath = $ExportPath

$ExportPath: specifica il percorso in cui salvare il file di backup (ad esempio, C:\backup).

$ExportSettings.BaseFileName = $ExportFile

$ExportFile: specifica il nome del file di backup (ad esempio, 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. Backup dell'elenco o della libreria in un file.

$ExportJob.Run()

Per ulteriori informazioni, consultare l'articolo di Microsoft.

2. Fare clic su SharePoint Management Shell per avviare la console.

3. Utilizzare i comandi PowerShell per ripristinare l'elenco o la libreria nella posizione di origine o nella nuova posizione.

```
Import-SPWeb -Identity xxxx -Path xxxx -Inclu-
deUserSecurity:$true -UpdateVersions:xxxx
```

Identity: specifica l'URL o il GUID Web in cui eseguire l'importazione (ad esempio, http://www.contoso.com).

Path: specifica il nome del file di importazione (ad esempio, C:\backup\list.cmp)

IncludeUserSecurity: consente di mantenere le impostazioni di protezione utente, ad eccezione degli elenchi SharePoint che non rispettano i set di autorizzazioni a livello di elemento ed ereditarietà.

UpdateVersions: indica le modalità di risoluzione dei casi in cui è presente una versione del file da importare già esistente sul sito interessato. È possibile selezionare una delle opzioni seguenti:

Aggiungi: consente di aggiungere il file come nuova versione.

Sovrascrivi: sovrascrive il file corrente e tutte le relative versioni (eseguendo prima l'eliminazione e poi l'inserimento).

Ignora: ignora il file se già presente nella destinazione. Il nuovo file non verrà aggiunto.

Il valore predefinito è Aggiungi.

Per ulteriori informazioni, consultare l'articolo di Microsoft.

Ripristino di un file

Effettuare le operazioni seguenti:

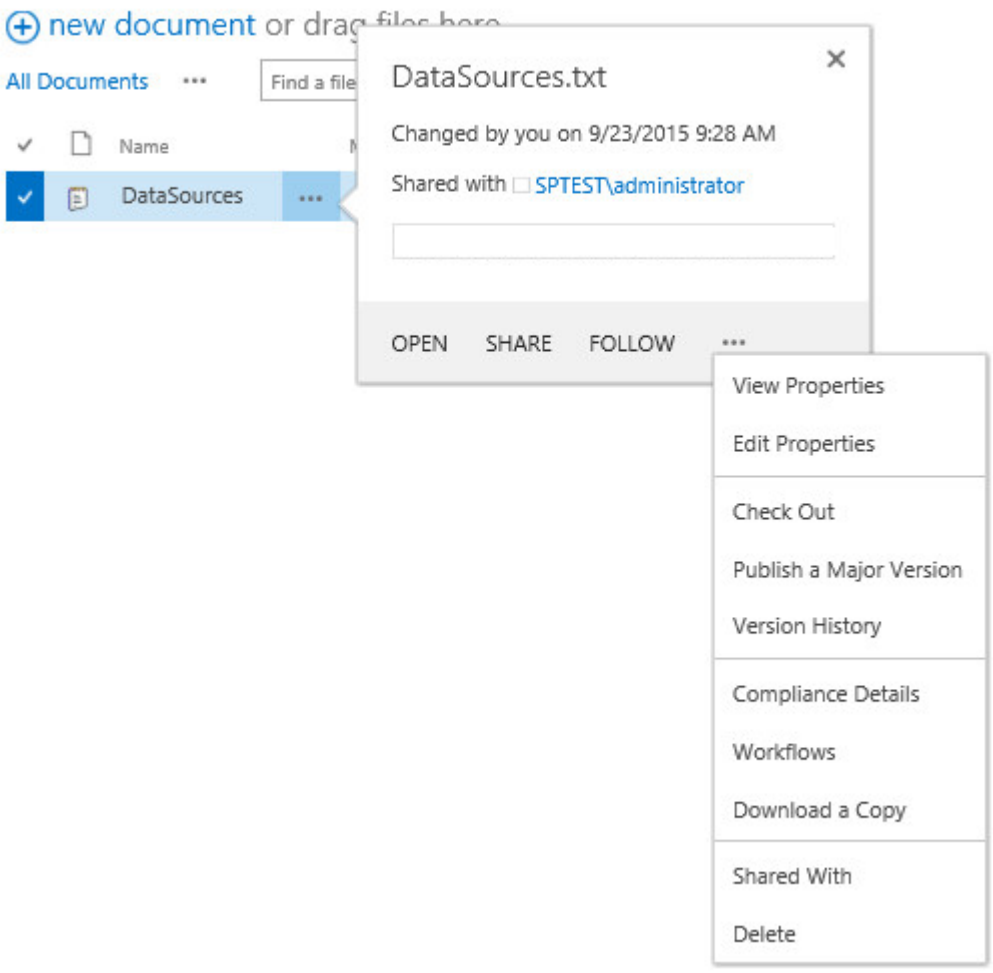
1. Ripristinare l'elenco o la libreria in una nuova posizione. Per ulteriori informazioni, consultare la sezione Ripristino di un elenco o di una libreria.

   Esempio: L'elenco o la libreria di origine vengono nominati NewList1 e l'URL è http://contoso.com /TestSite1/NewList1

   - Usare i comandi PowerShell per ripristinare l'elenco o la libreria alla nuova posizione. Ad esempio, http://contoso.com/TestSite2

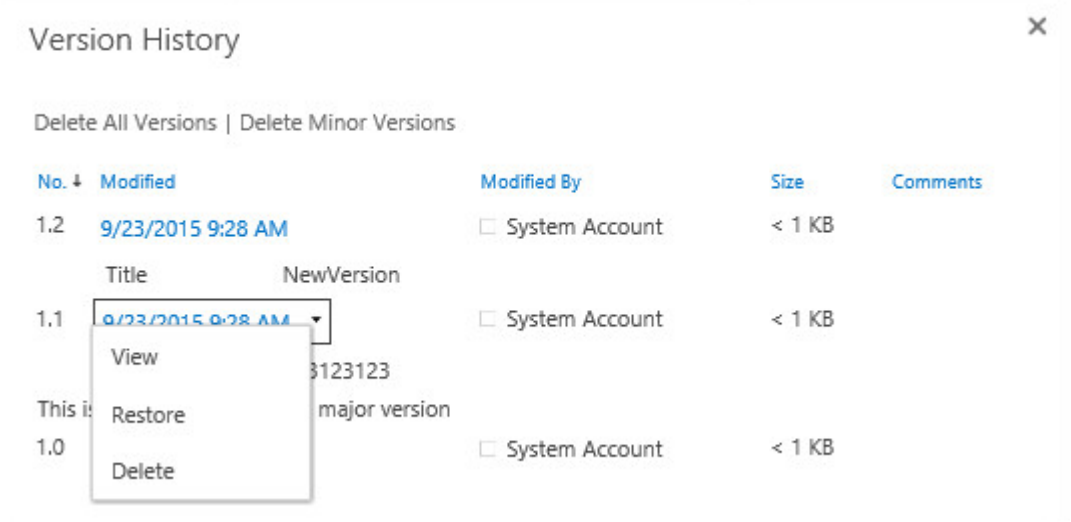
     Import-SPWeb -Identity http://contoso.com/TestSite2 -Path C:\-backup\list.cmp -IncludeUserSecurity:$true -UpdateVersions:Overwrite

   - Accedere al nuovo URL dell'elenco o della libreria. Vengono ripristinati tutti gli elementi in http://contoso.com/TestSite2/NewList1.
2. Accedere al nuovo URL della posizione dell'elenco o della libreria.
3. Verificare la cronologia di versione del file nell'elenco o nella libreria.



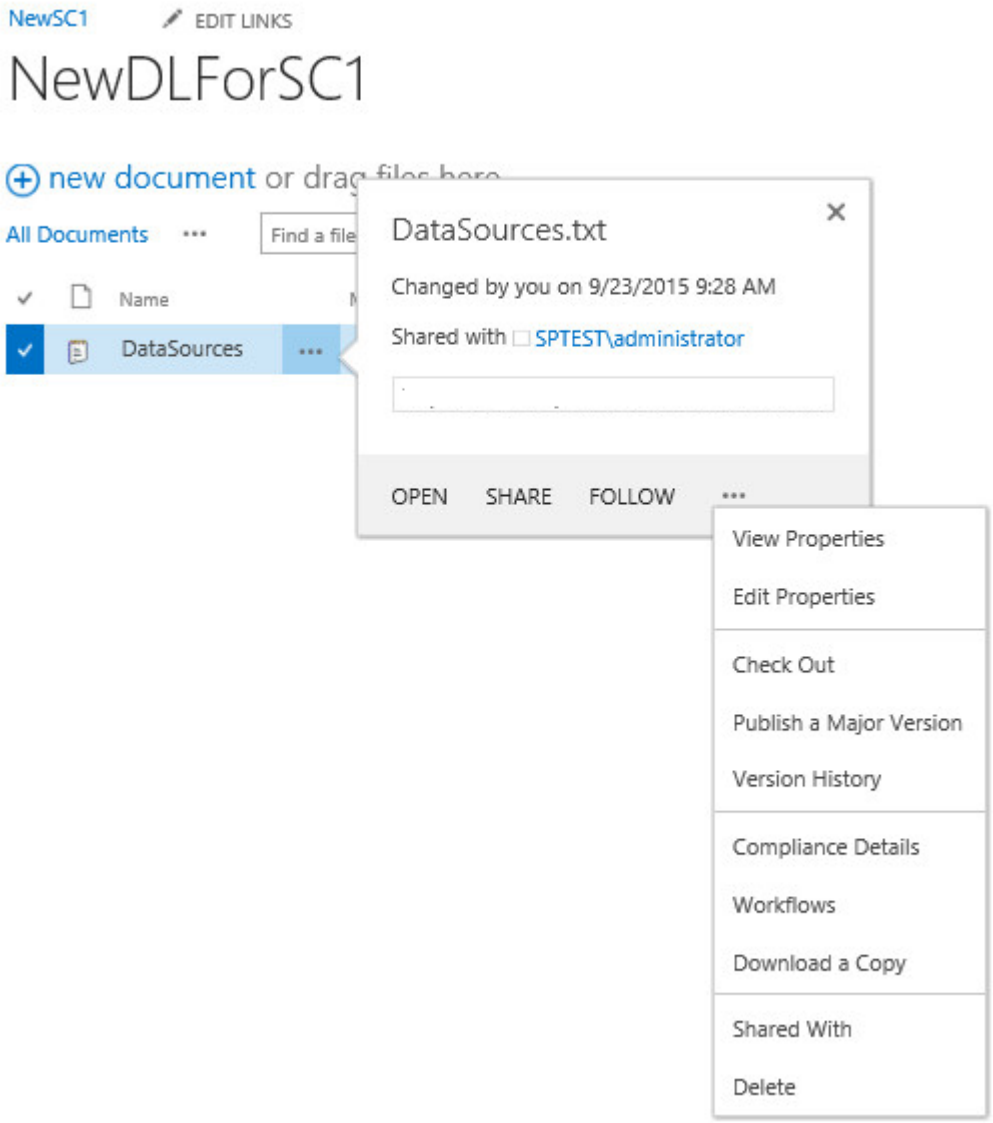
4. Selezionare la versione specifica del file e fare clic su Ripristina.

   Ad esempio, ripristinare la versione specifica 1.1 del file.



   La versione 1.1 del file viene ripristinata.

5. Fare clic su Scarica una copia per salvare il file con la versione 1.1 specifica in una posizione.



Il file salvato viene ripristinato nell'elenco o nella libreria di origine.

Creazione di una rete isolata per il ripristino SharePoint

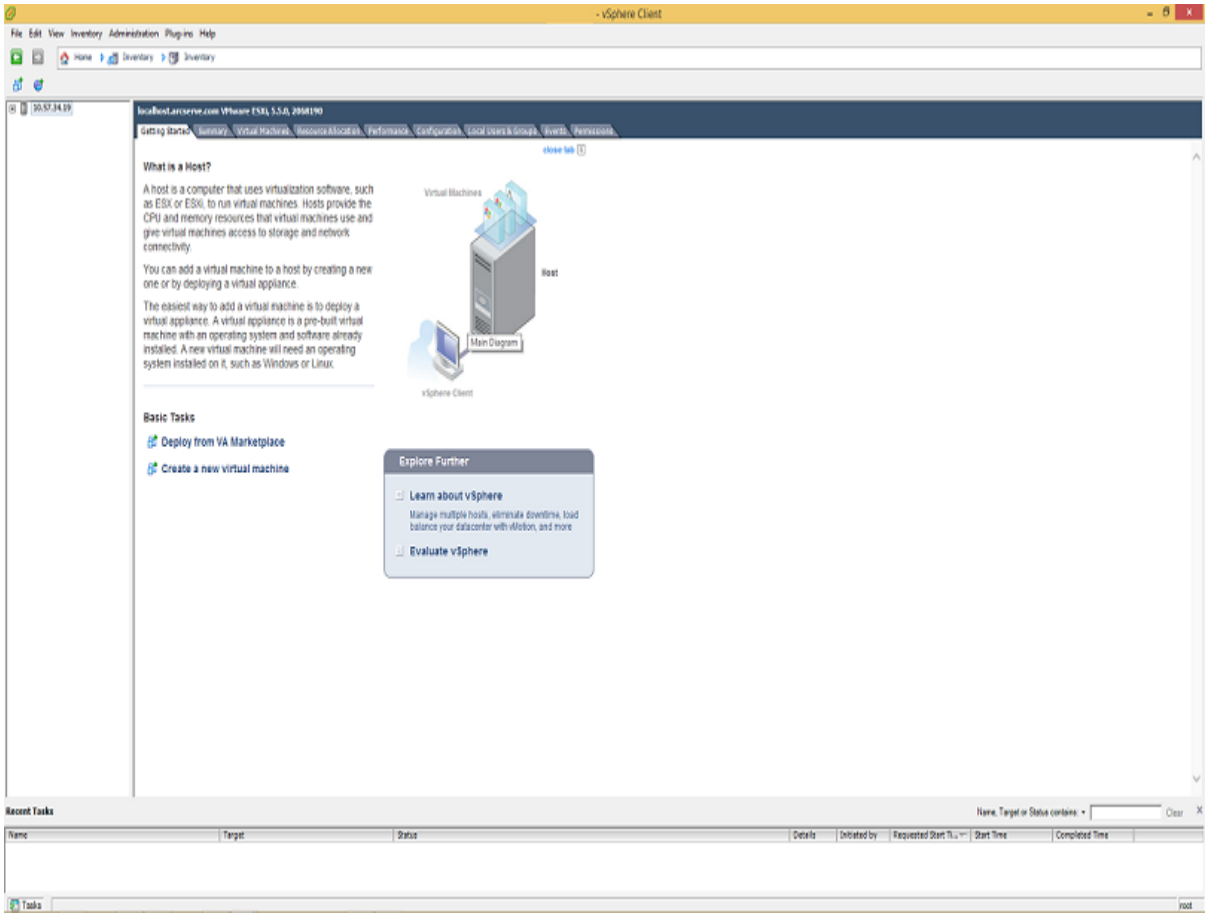
È possibile creare una rete isolata per il ripristino di SharePoint nei computer VMware e Hyper-V.

- Creazione di una rete isolata per il ripristino SharePoint per il computer virtuale VMware
- Creazione di una rete isolata per il ripristino SharePoint per il computer virtuale Hyper-V

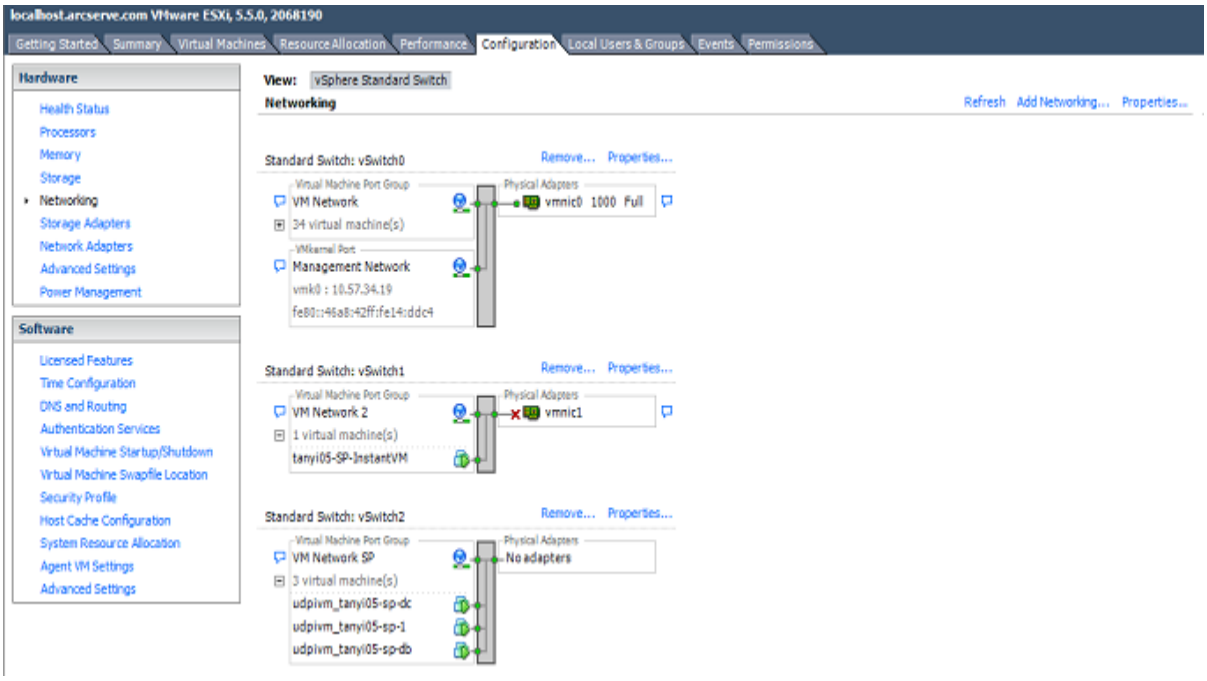
Creazione di una rete isolata per il ripristino SharePoint per il computer virtuale VMware

Effettuare le operazioni seguenti:

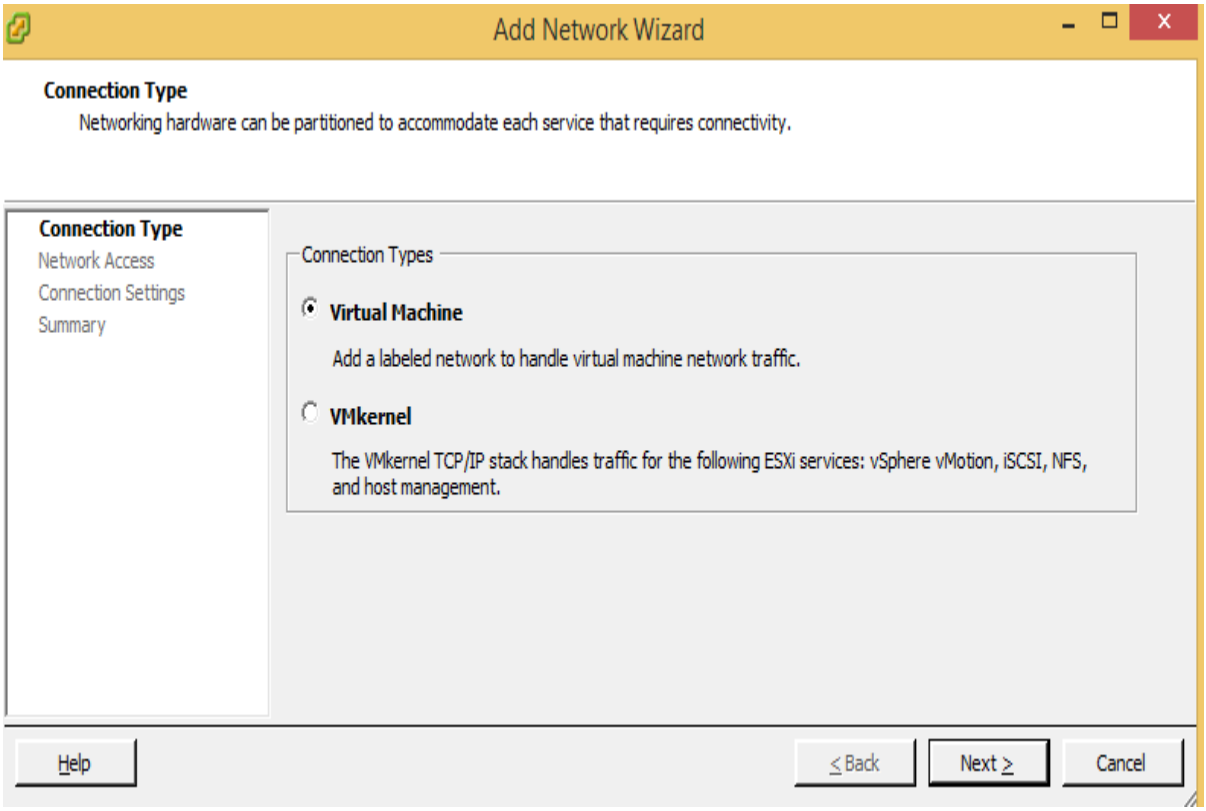
1. Accedere al server VMware ESXi mediante il client vSphere.



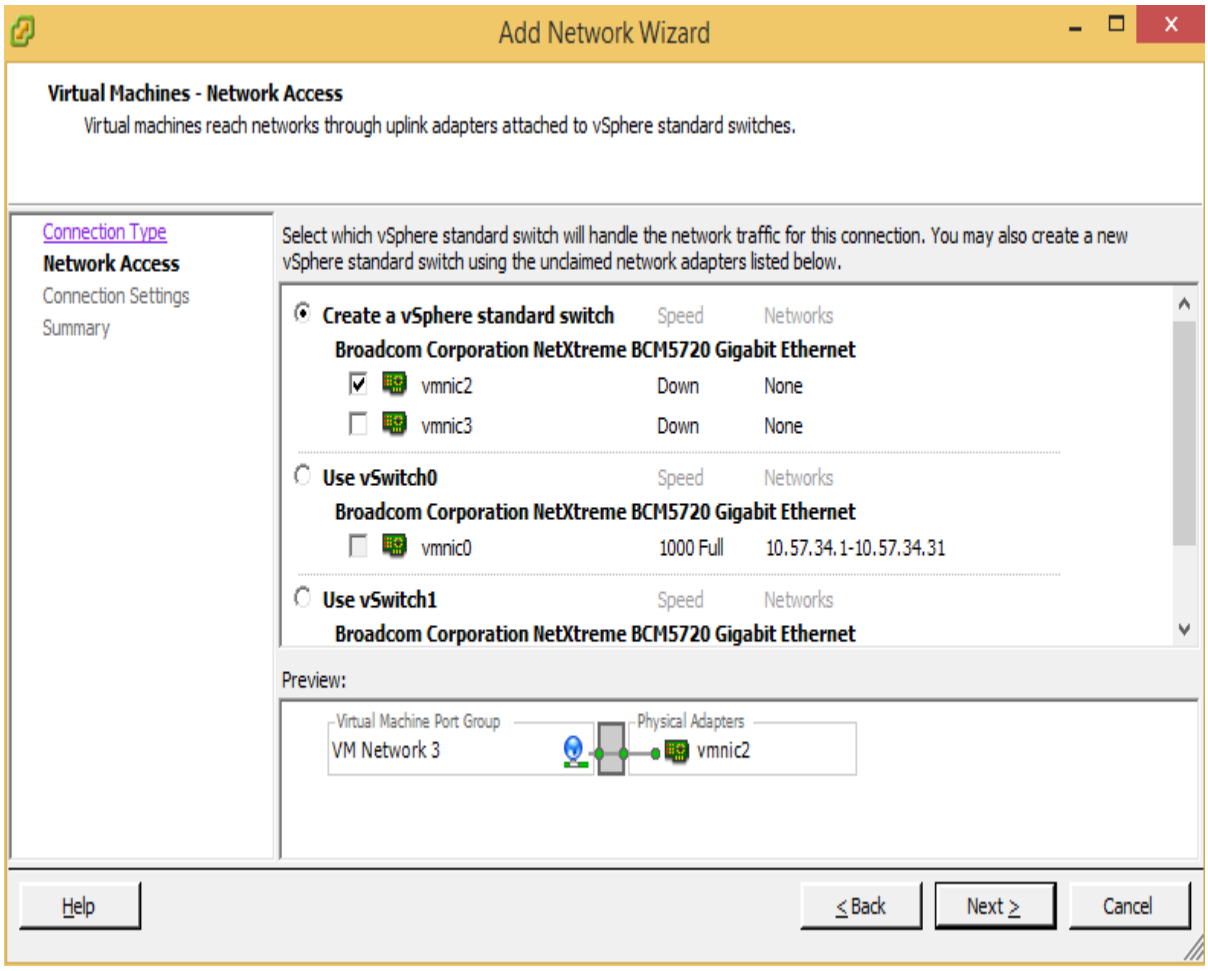
2. Fare clic sulla scheda Configurazione.
3. Selezionare la rete nel riquadro Hardware e fare clic su Aggiungi rete.



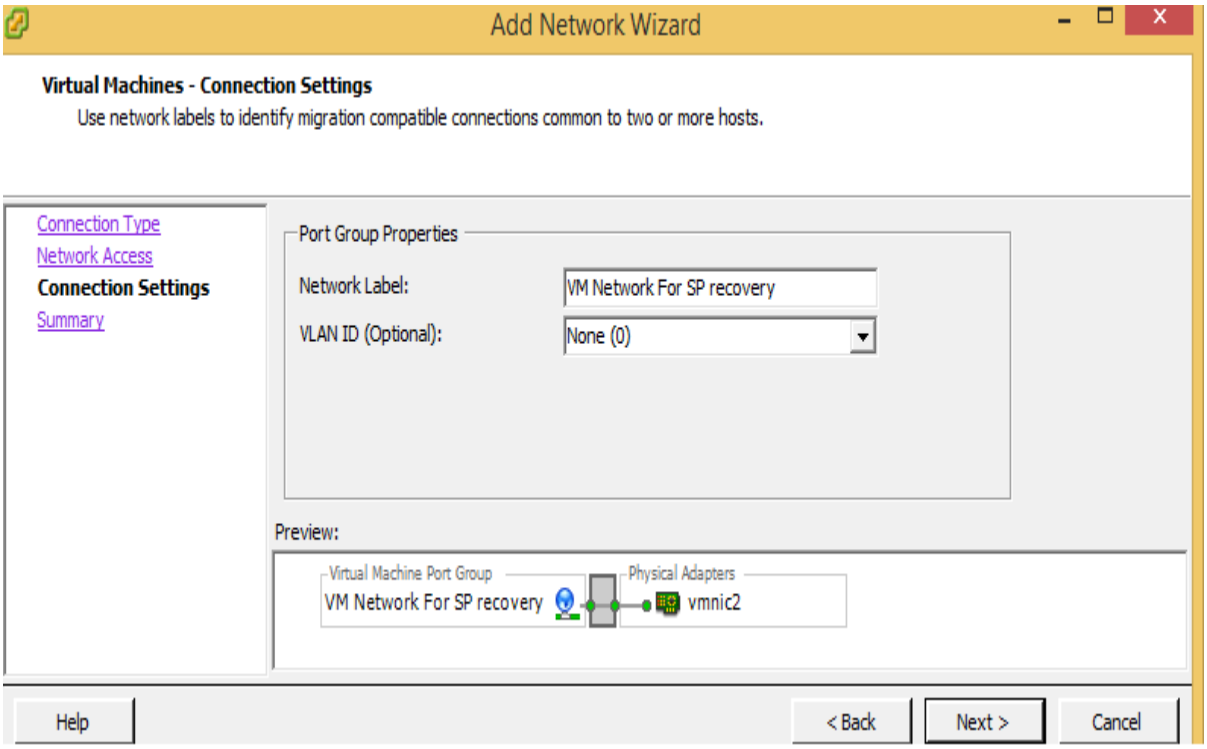
4. Assicurarsi che sia selezionato il pulsante di opzione del computer virtuale e fare clic su Avanti.



5. Selezionare la scheda NIC fisica che si desidera utilizzare per la connessione dello switch virtuale ad altre risorse fisiche sulla rete e fare clic su Avanti.

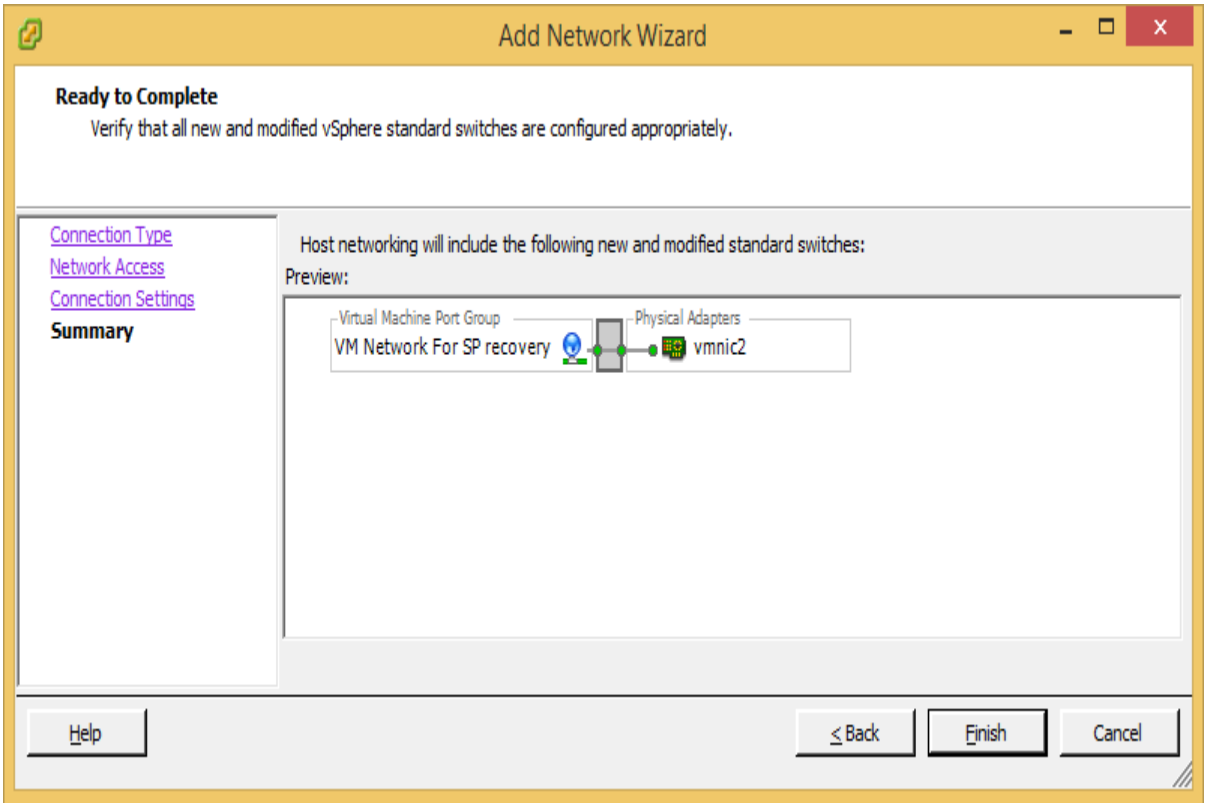


6. Assegnare un'etichetta di rete allo switch virtuale e un ID VLAN (se necessario), quindi fare clic su **Avanti**.



7. Verificare che le impostazioni di switch virtuale siano corrette, quindi fare clic su **Fine**.

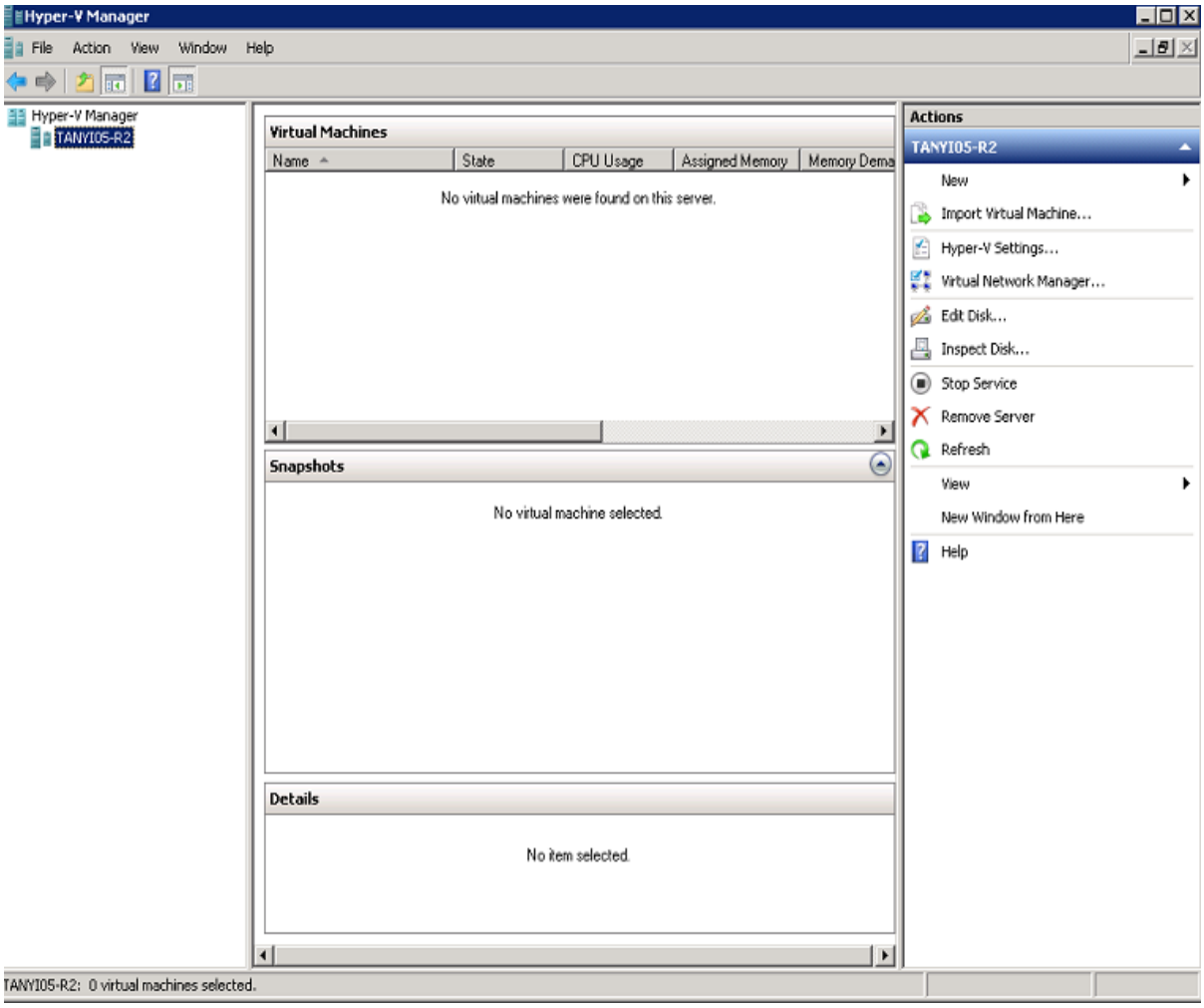
   Tornando alla scheda Configurazione di rete, sarà possibile visualizzare il nuovo switch virtuale aggiunto.


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

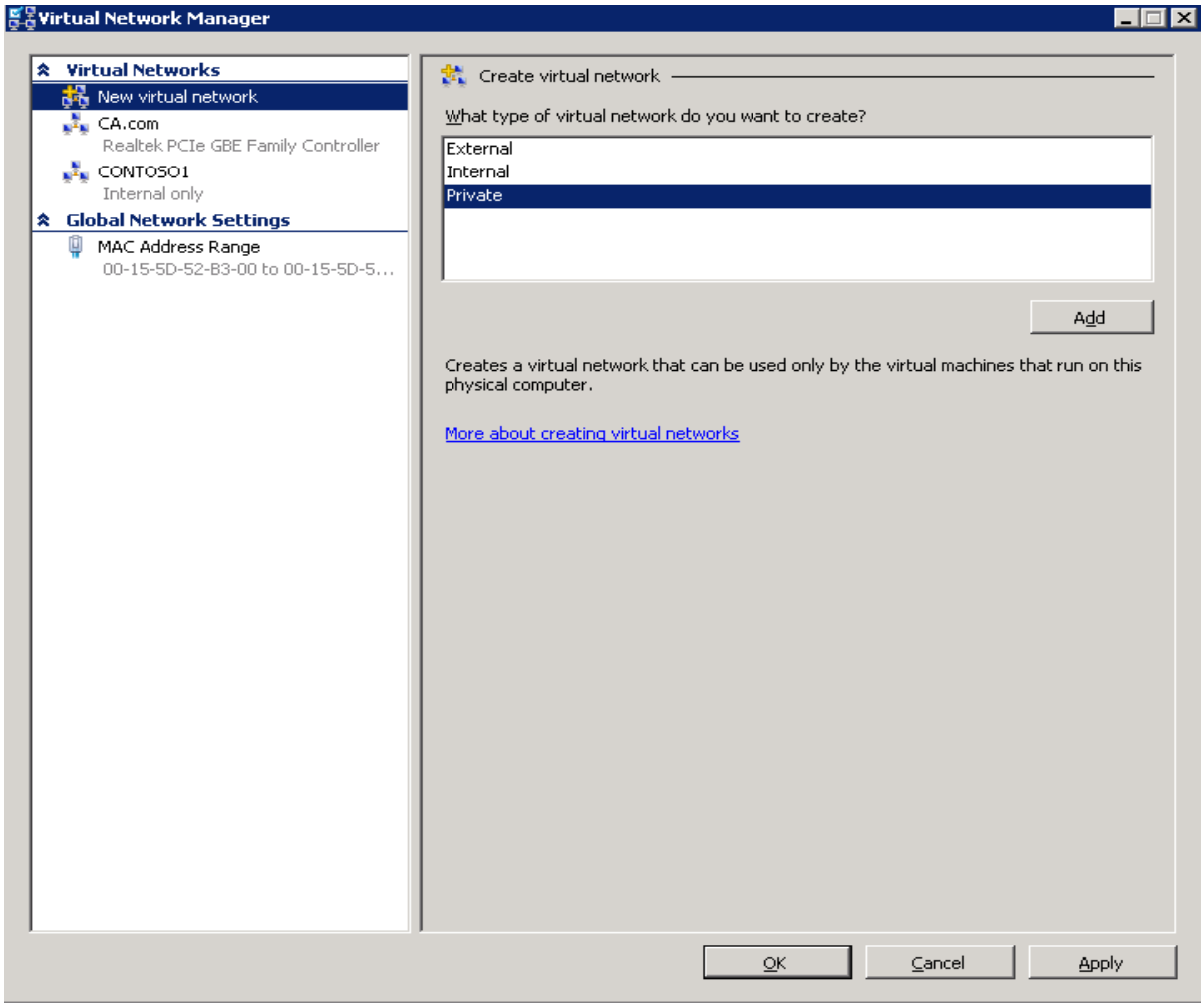
Creazione di una rete isolata per il ripristino SharePoint per il computer virtuale Hyper-V

Effettuare le operazioni seguenti:

1. Accedere alla console di gestione di Hyper-V.
2. Fare clic su Gestione rete virtuale.

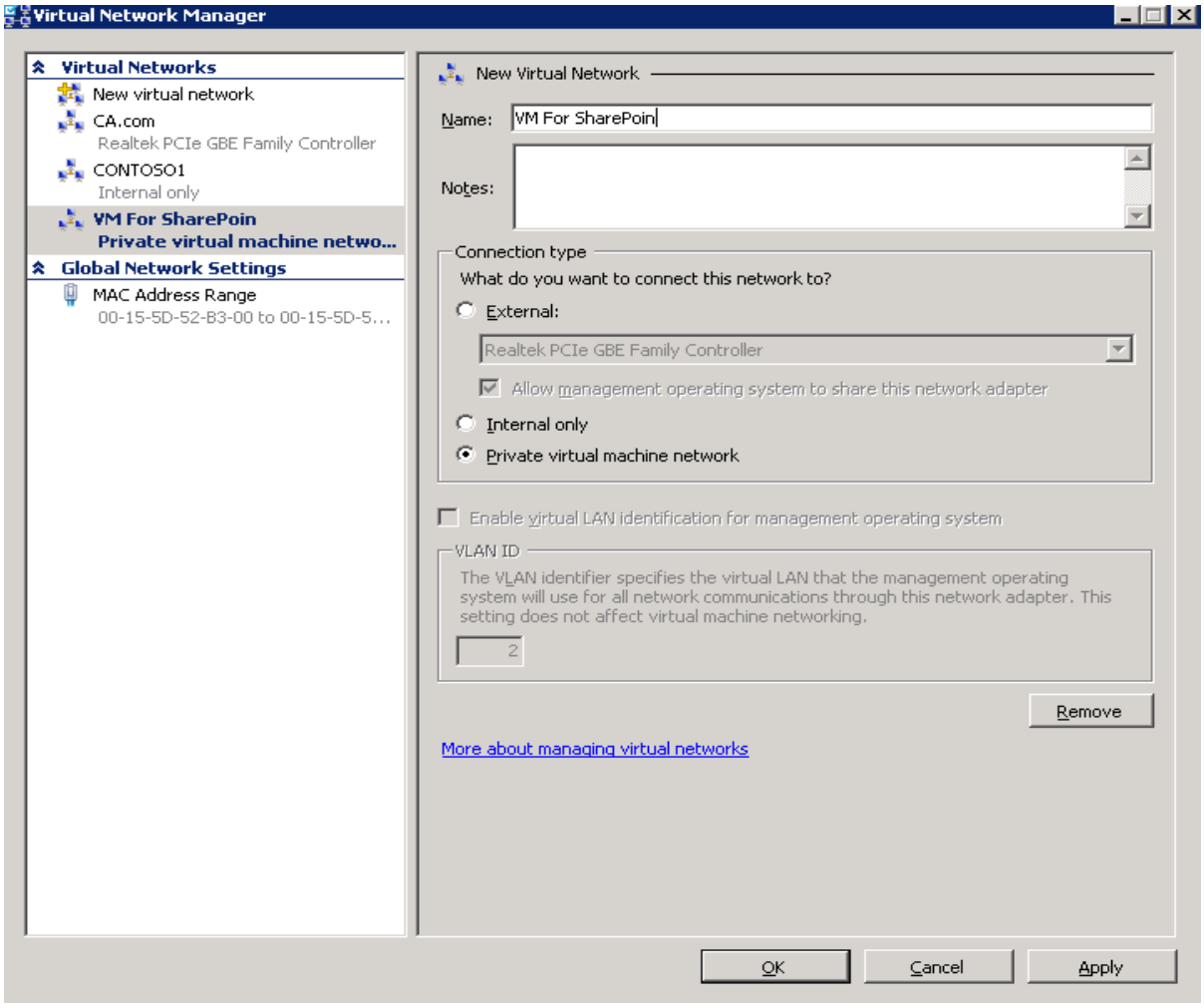


3. Fare clic sulla nuova rete virtuale, selezionare il tipo Privato e fare clic su **Aggiungi**.



4. Digitare il nome delle rete virtuale privata e fare clic su OK.

   La nuova rete virtuale viene aggiunta.


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

Chapter 6: Generazione di rapporti Arcserve UDP

La presente sezione descrive i seguenti argomenti:

Introduzione ai rapporti Arcserve UDP

La scheda **Rapporti** fornisce l'accesso a vari tipi di rapporti, tra cui Avvisi, Tendenza dati, Stato di backup, Distribuzione dati e SLA. Il riquadro sinistro include un elenco di rapporti che è possibile generare. Il riquadro centrale mostra i dettagli del rapporto selezionato e consente di configurare varie impostazioni di rapporto. Il rapporto viene generato per un gruppo di nodi o di server. È anche possibile filtrare il rapporto in modo che visualizzi informazioni dettagliate per un singolo nodo.

Per ulteriori informazioni su questi rapporti, consultare la sezione Rapporti di Arcserve UDP.

Il drill-down di questo rapporto include i seguenti elementi:

Nodi del processo

Visualizza il nome del nodo in cui vengono eseguiti i processi degli agenti Arcserve UDP, di Host-Based VM o di Virtual Standby.

Nodi protetti

Visualizza il nome del nodo dell'agente e il nodo protetto dall'agente Arcserve Unified Data Protection o dal backup del computer virtuale basato su host, di Virtual Standby o Arcserve Backup.

Prodotto

Visualizza il prodotto installato sul nodo. Il nome del prodotto può corrispondere a Agente Arcserve Unified Data Protection, Recovery Point Server di Arcserve Unified Data Protection, Computer virtuale basato su host o Arcserve Backup.

Filtri/Azioni

Mostra le opzioni globali e locali di filtro e le azioni corrispondenti ai rapporti. Per ulteriori informazioni, consultare la sezione Utilizzo di filtri e azioni.

Rapporti Arcserve UDP

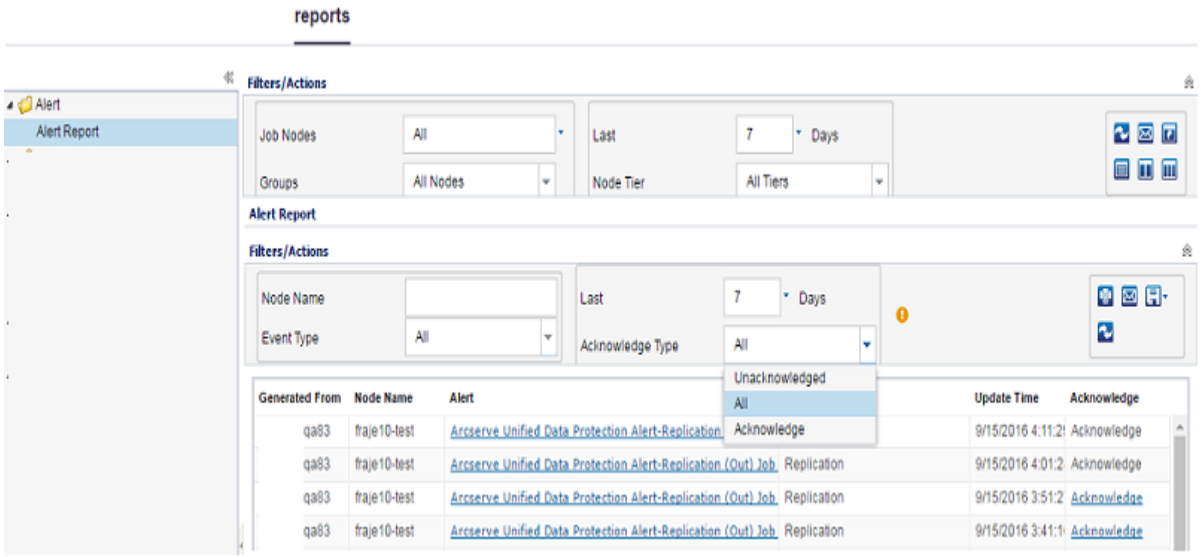
Arcserve UDP fornisce i seguenti tipi di rapporti:

- Rapporto di avviso
- Rapporto Tendenza delle dimensioni di backup
- **Rapporto relativo al backup** Arcserve UDP offre tre tipi di rapporti relativi al backup:
  - Rapporto Stato di backup dei nodi
  - Rapporto Stato di protezione della virtualizzazione
  - Rapporto capacità gestita
- Rapporto Distribuzione dati sui supporti
- **Rapporto SLA:** Il rapporto Service Level Agreement (SLA) mostra la conformità dei rapporti relativi a Recovery Point Objective (RPO) e Recovery Time Objective (RTO)
  - Rapporto RPO
  - Rapporto RTO
- **Rapporto Stato processo:** Arcserve UDP consente di generare il rapporto Stato processo per recuperare le informazioni su tutti i processi eseguiti in un periodo specificato.

Rapporti di avviso

Arcserve UDP mostra le informazioni di avviso per i nodi. Oltre ai filtri e alle azioni comuni, il rapporto di avviso offre la possibilità di ordinamento out delle dashboard di avviso tramite la ricezione di messaggi. Per impostazione predefinita, il dashboard del rapporto di avviso mostra soltanto gli avvisi non ricevuti. È possibile fare clic sul collegamento **Conferma** contenuto in ogni avviso per rimuoverlo dalla visualizzazione del dashboard. Se si desidera visualizzare il rapporto ricevuto, selezionare **Conferma** nell'opzione **Tipo di conferma** del filtro locale.

Rapporto di avviso

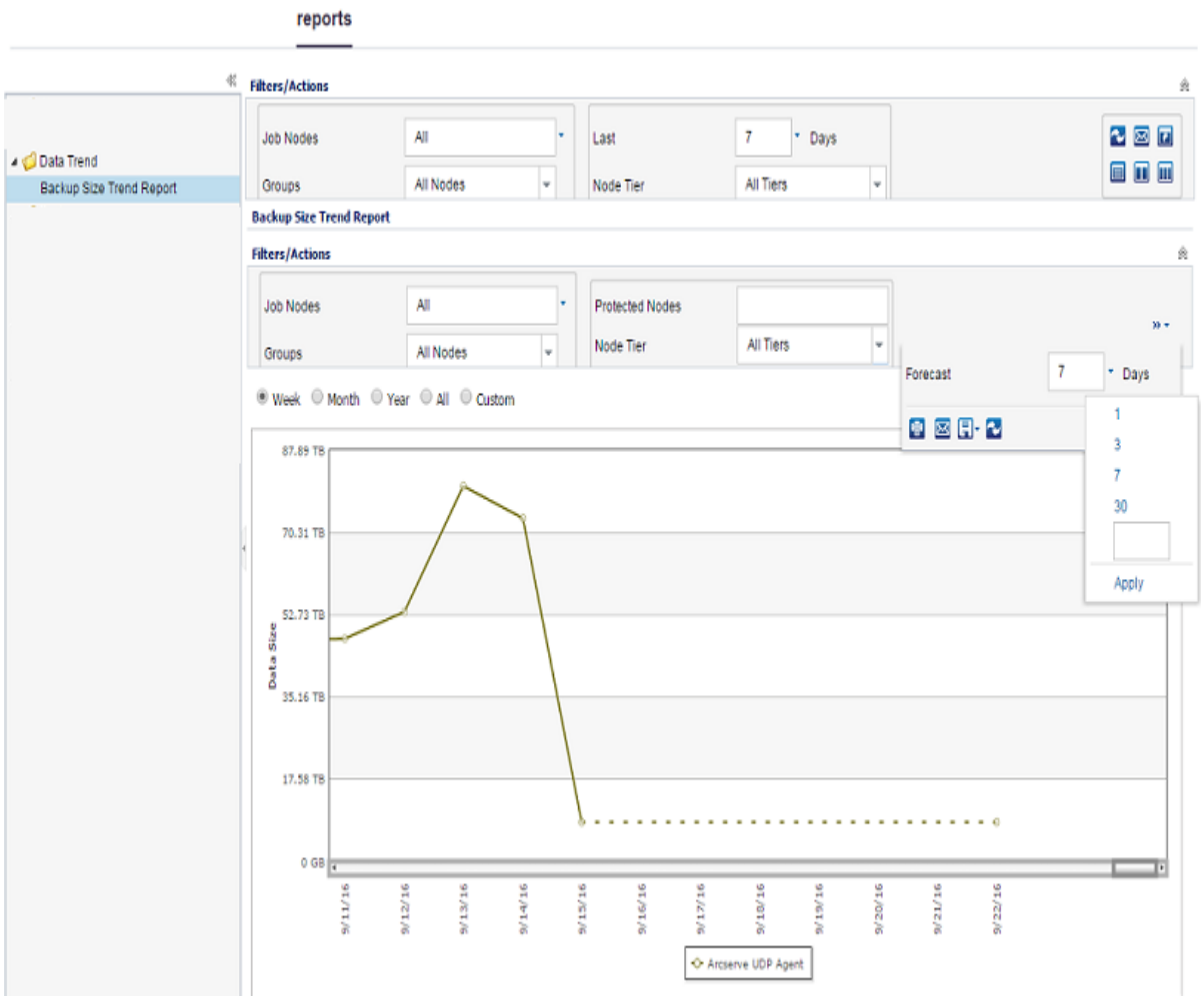


Rapporti Tendenza delle dimensioni di backup

Il rapporto Tendenza delle dimensioni di backup di Arcserve UDP mostra le dimensioni dei dati di backup di Arcserve Backup e Arcserve Unified Data Protection in una visualizzazione cronologica, illustrandone la tendenza di crescita in modo da consentire di prevedere le esigenze future relative allo spazio di archiviazione. Il rapporto contiene informazioni sui nodi in esecuzione su sistemi operativi Windows e Linux supportati e consente di eseguire il drill-down per visualizzare informazioni più dettagliate relative ai singoli nodi.

Oltre a filtri e azioni comuni, il rapporto di tendenza delle dimensioni di backup offre la possibilità di visualizzare i risultati in base al numero di **giorni**. Per impostazione predefinita, il filtro per gli **ultimi** giorni non è applicabile. In alternativa, è possibile utilizzare il filtro della modalità **Visualizzazione** (settimana, mese, anno, personalizzato).

Rapporto Tendenza delle dimensioni di backup



Rapporti Stato di backup del nodo

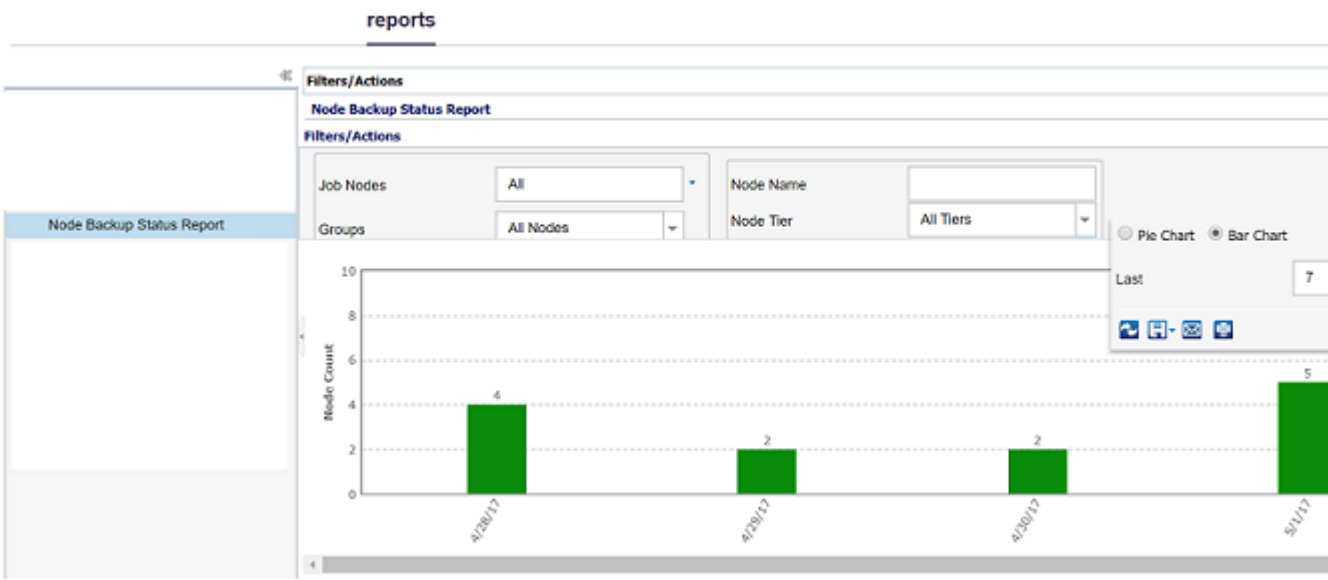
Arcserve UDP visualizza lo stato di backup più recente di tutti i nodi per un periodo di tempo specifico. Questo rapporto consente di visualizzare informazioni dettagliate sui nodi sulla base delle categorie quali tipo selezionato di gruppi e livello del nodo.

Oltre a filtri e azioni comuni, il rapporto Stato di backup del nodo consente di visualizzare i risultati in base al numero di **giorni**. Nel grafico a barre, il numero del nodo è visibile nella parte superiore di ogni barra.

Il rapporto visualizza lo stato di processo seguente:

- **Completato correttamente:** fornisce un elenco dei processi che sono stati completati correttamente.
- **Non riuscito:** fornisce un elenco dei processi che non sono riusciti.
- **Incompleto:** fornisce un elenco dei processi terminati con lo stato incompleto.
- **Annullato:** fornisce un elenco dei processi che sono stati annullati.
- **Non eseguito:** fornisce un elenco dei processi che non sono stati eseguiti.
- **Nessun backup:** fornisce l'elenco dei nodi senza un piano assegnato o dei nodi con un piano assegnato ma ancora in attesa di essere sottoposti a backup.

Rapporto Stato di backup del nodo:

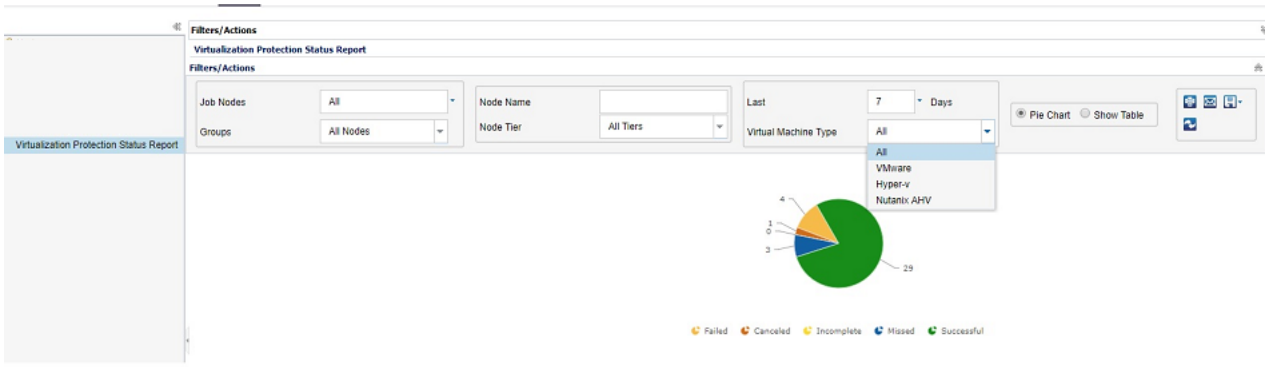


Rapporti Stato di protezione della virtualizzazione

Visualizza lo stato di backup più recente dei computer virtuali protetti da Host-Based VM Backup, da Virtual Standby o da Arcserve Backup. Questo rapporto consente di visualizzare informazioni per un periodo di tempo specificato e di eseguire il drill-down per visualizzare informazioni più dettagliate su ogni categoria selezionata.

Oltre ai filtri e alle azioni comuni, il rapporto Stato di protezione della virtualizzazione consente di visualizzare i risultati in base al numero di **giorni** e visualizzare i rapporti come grafico a torta o come tabella.

Rapporto Stato di protezione della virtualizzazione



Rapporti Capacità gestita

Visualizza le dimensioni dei dati non elaborati dell'ultimo backup completo eseguito correttamente per ciascun nodo protetto da Arcserve Backup, dall'agente Arcserve Unified Data Protection e da Host-based VM Backup.

Per ulteriori informazioni su filtri e azioni, consultare la sezione Filtri e azioni comuni.

Note:

- L'immissione di un valore nel filtro **Ultimi giorni** non modifica il risultato per il filtro globale. Indipendentemente dal numero di giorni specificato, l'applicazione del filtro mostra i valori più recenti.
- I dati relativi al backup del nodo nell'archivio dati eliminato potrebbero essere visualizzati se il rapporto sulla capacità gestita non viene aggiornato, salvo se il backup viene eseguito sulla destinazione di backup più recente. Ad esempio, se il piano è stato modificato per l'esecuzione dei backup nell'archivio dati DS2 e l'archivio dati è stato eliminato da DS1, i dati eliminati da DS1 potrebbero essere ancora visualizzati nel rapporto, a meno che non viene eseguito il backup su DS2.
- Nell'area della griglia del rapporto, le tre colonne seguenti sono valide soltanto per i nodi di computer virtuali protetti da backup senza agente basato su host:

  Spazio volumi utilizzato (VM)

  Indica la somma dello spazio utilizzato di volumi nel sistema operativo guest del computer virtuale.

  Per Windows: fa riferimento alla somma dello spazio utilizzato di tutti i volumi NTFS.

  Per computer virtuali Linux: fa riferimento alla somma dello spazio utilizzato di tutti i volumi.

  Per il computer virtuale Linux, è supportato solo il computer virtuale VMware per questa colonna. In questo caso, è necessario aggiornare il nodo del computer virtuale con le credenziali utente root. Sia che si tratti di un computer virtuale Linux VMware senza credenziali o Linux Hyper-V, questa colonna è vuota.

  Per il supporto del computer virtuale Linux, i computer VMware Red Hat o CentOS e i computer virtuali Hyper-V Linux prevedono delle limitazioni. Per ulteriori informazioni, consultare la sezione Problemi noti delle Note di rilascio di Arcserve UDP v6 Aggiornamento 1.

  Dimensioni di lettura sintetica

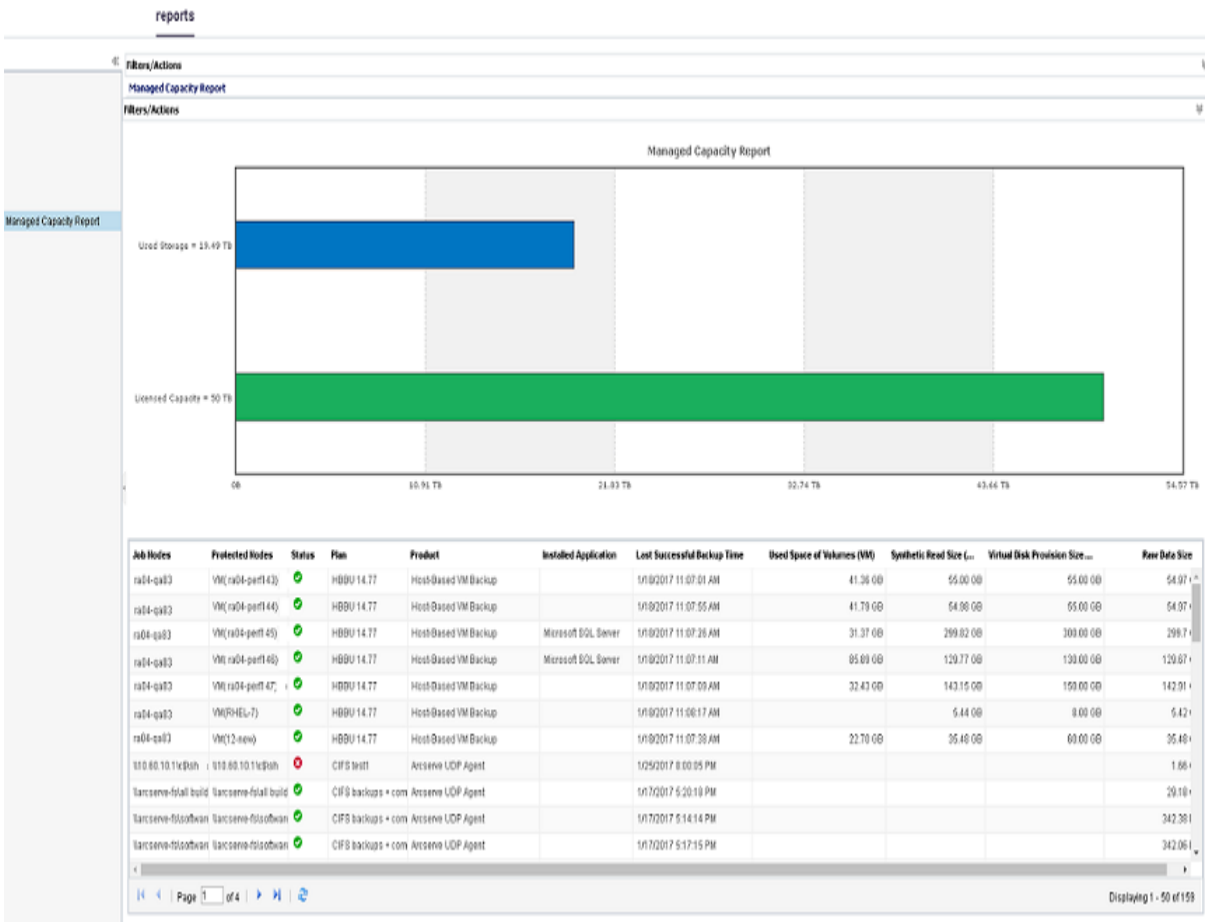
Indica le dimensioni totali di lettura durante il backup.

Dimensioni di provisioning disco virtuale

Indica la somma delle dimensioni di provisioning di tutti i dischi virtuali del computer virtuale.

- In genere, le dimensioni dei dati non elaborati corrispondono alle dimensioni dei dati scritti nella destinazione di backup. Per il backup senza agente basato su host, potrebbe coincidere con le dimensioni di lettura sintetica poiché Arcserve UDP non scrive i blocchi di dati composti da tutti zero nella destinazione di backup. In altre parole, i blocchi di dati composti da tutti zero vengono ignorati durante il backup. Inoltre, per i nodi di computer virtuale protetti da backup senza agente basato su host, è possibile personalizzare i dati mostrati per Dimensioni dati non elaborati configurando alcuni valori del Registro di sistema. Per ulteriori informazioni sulla configurazione dei valori del Registro di sistema e sui comportamenti associati, consultare la sezione Dimensioni dei dati non elaborati nel rapporto sulla capacità gestita per il backup senza agente basato su host del computer virtuale.

  Rapporto capacità gestita

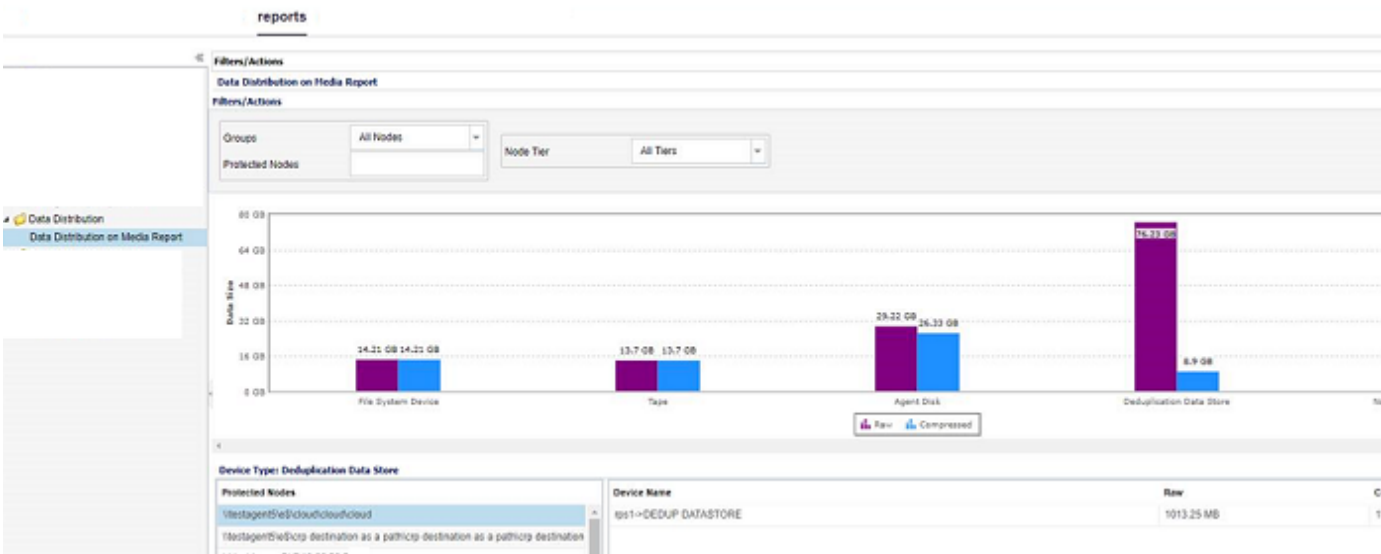

reports
Filters/Actions
Managed Capacity Report
Filters/Actions
Managed Capacity Report
Managed Capacity Report
Used Storage = 19.49 TB
Licensed Capacity = 50 TB
0B
10.91 TB
21.83 TB
32.74 TB
43.66 TB
54.57 TB
Job Nodes
Protected Nodes
Status
Plan
Product
Installed Application
Last Successful Backup Time
Used Space of Volumes (VM)
Synthetic Read Size (...
Virtual Disk Provision Size ...
Raw Data Size
ra04-ga03
VM(ra04-perf143)
HBBU 14.77
Host-Based VM Backup
1/1/0/2017 11:07:01 AM
41.36 GB
55.00 GB
55.00 GB
54.97
ra04-ga03
VM(ra04-perf144)
HBBU 14.77
Host-Based VM Backup
1/1/0/2017 11:07:55 AM
41.70 GB
54.98 GB
55.00 GB
54.97
ra04-ga03
VM(ra04-perf145)
HBBU 14.77
Host-Based VM Backup
Microsoft SQL Server
1/1/0/2017 11:07:26 AM
31.37 GB
299.82 GB
300.00 GB
299.7
ra04-ga03
VM(ra04-perf146)
HBBU 14.77
Host-Based VM Backup
Microsoft SQL Server
1/1/0/2017 11:07:11 AM
95.69 GB
129.77 GB
130.00 GB
120.67
ra04-ga03
VM(ra04-perf147)
HBBU 14.77
Host-Based VM Backup
1/1/0/2017 11:07:09 AM
32.43 GB
143.15 GB
150.00 GB
142.91
ra04-ga03
VM(RHEL-7)
HBBU 14.77
Host-Based VM Backup
1/1/0/2017 11:06:17 AM
5.44 GB
8.00 GB
5.42
ra04-ga03
VM(12-new)
HBBU 14.77
Host-Based VM Backup
1/1/0/2017 11:07:38 AM
22.70 GB
35.48 GB
60.00 GB
35.48
\\10.60.10.1\c$\sh
\\10.60.10.1\c$\sh
CIFS test1
Arcserve UDP Agent
1/25/2017 8:00:05 PM
1.66
tiarcserve-fs\all build
tiarcserve-fs\all build
CIFS backups + com
Arcserve UDP Agent
1/17/2017 5:20:19 PM
29.10
tiarcserve-fs\softwar
tiarcserve-fs\softwar
CIFS backups + com
Arcserve UDP Agent
1/17/2017 5:14:14 PM
342.39
tiarcserve-fs\softwar
tiarcserve-fs\softwar
CIFS backups + com
Arcserve UDP Agent
1/17/2017 5:17:15 PM
342.06
Page 1 of 4
Displaying 1 - 50 of 159

Rapporti Distribuzione dati sui supporti

Visualizza la dimensione compressa ed effettiva dei dati di backup (raw) per tipi di destinazione diversi (deduplicazione o non deduplicazione e destinazione locale). Il presente rapporto consente di visualizzare tutti i nodi, compresi i nodi di Arcserve Backup e l'agente Arcserve UDP. Per visualizzare le informazioni sui dati Arcserve Backup, abilitare la **Pianificazione della sincronizzazione dati di Arcserve Backup** nella scheda **Impostazioni**. Per visualizzare le informazioni più recenti, fare clic su **Esegui ora** nella scheda Impostazioni.

Per ulteriori informazioni su filtri e azioni, consultare la sezione Filtri e azioni comuni.

del Rapporto Distribuzione dati sui supporti



Nota: Il rapporto Distribuzione dati sui supporti dipende dai dati sul punto di ripristino disponibili nella destinazione di backup. È possibile utilizzare l'opzione **Aggiornamento** per avviare la sincronizzazione su richiesta e ottenere lo stato più recente nei rapporti.

Rapporti RPO

Il rapporto sull'obiettivo del punto di ripristino (Recovery Point Objective, RPO) è un rapporto di conformità che mostra come vengono distribuiti i punti di ripristino nell'ambiente di backup. Il rapporto consente di valutare l'intervallo di tempo minimo e massimo di restituzione del nodo in caso di ripristino di emergenza. Poiché il rapporto RPO riguarda la destinazione di backup, i dati vengono compilati quando è disponibile un backup. È possibile compilare questo rapporto tramite aggiornamento su richiesta oppure in base a una pianificazione.

Nota: Il rapporto viene compilato direttamente anche da Arcserve UDP Dashboard. Facendo clic nel grafico a barre RPO di un mese nel Dashboard viene visualizzata la schermata del rapporto RPO per il mese specifico nella pagina RPO.

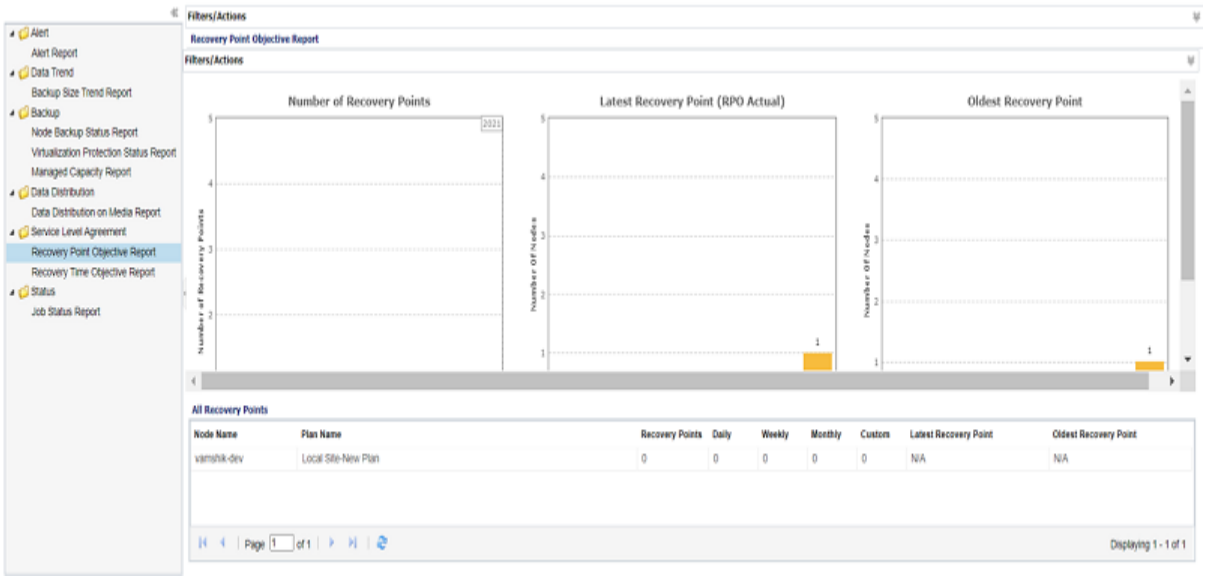
Il grafico a barre RPO fornisce le seguenti informazioni:

- Distribuzione mensile dei punti di ripristino nella destinazione di backup.
- Durata del punto di ripristino più recente disponibile per ciascun nodo.
- Durata del punto di ripristino meno recente disponibile per ciascun nodo.
- Numeri forniti nella parte superiore di ogni barra.
- *Tipo di destinazione*: consente di selezionare il tipo di destinazione. Ad esempio, Destinazione cloud, Recovery Point Server e Condivisione locale.
- *Nome di destinazione* consente di selezionare una destinazione dall'elenco di destinazioni che viene visualizzato come risultato dell'opzione selezionata come tipo di destinazione.
- Facendo clic su barra specifica all'interno di uno dei seguenti tre grafici è possibile visualizzare risultati specifici: *Numero di punti di ripristino* per ogni mese, *Data punto di ripristino più recente* e *Data punto di ripristino meno recente*.

Nel grafico a barre RPO, la sezione Tutti i punti di ripristino visualizza le informazioni quali Nome nodo, Nome piano, Punti di ripristino, Giornaliero, Settimanale, Mensile, Personalizzato, Ultimo punto di ripristino e Punto di ripristino precedente.

Oltre ai filtri e alle azioni comuni , i rapporti RPO forniscono un'opzione univoca di **aggiornamento** nel filtro locale.

Rapporto RPO



Nota: Il rapporto dipende dai dati sul punto di ripristino disponibili nella destinazione di backup. È possibile utilizzare l'opzione **Aggiornamento** per avviare la sincronizzazione su richiesta e ottenere lo stato più recente nei rapporti.

Rapporti RTO

Il rapporto sull'obiettivo del momento di ripristino (Recovery Time Objective, RTO) è un rapporto di conformità che mostra se la durata prefissata di ripristino è stata raggiunta per tutti i tipi di processo di ripristino eseguiti. Il rapporto RTO mostra i seguenti tipi di stato:

- **RTO Met (RTO raggiunto):** il processo di ripristino ha raggiunto l'obiettivo definito.
- **RTO Not Met (RTO non raggiunto):** il processo di ripristino non ha raggiunto l'obiettivo definito.
- **RTO Not defined (RTO non definito)**: l'obiettivo per il processo di ripristino non è stato definito.
- **RTO Not Tested (RTO non verificato):** l'obiettivo del momento di ripristino è stato definito, ma il processo non è stato ancora verificato.

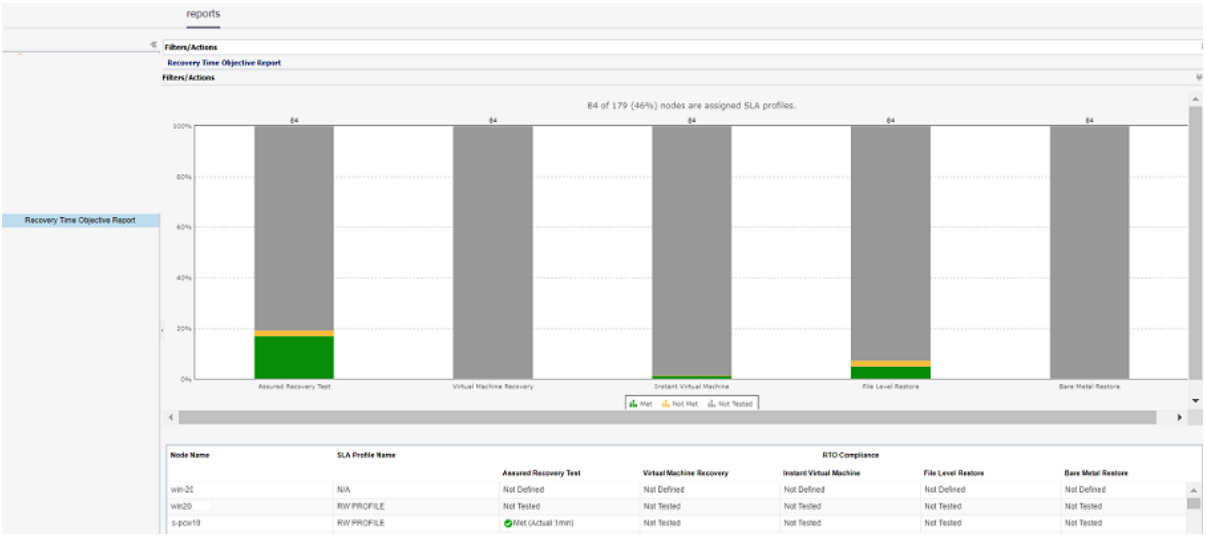
È possibile definire gli obiettivi del momento di ripristino per tutti i processi di ripristino. Per ulteriori informazioni, consultare la sezione per Creazione del profilo SLA.

Oltre ai filtri e alle azioni comuni, i rapporti RTO forniscono un'opzione unica del **Profilo SLA** e lo stato RTO nel filtro locale.

Nota: Il rapporto RTO non è supportato per i processi di ripristino bare metal eseguiti per i processi di backup configurati su una destinazione locale.

Dashboard Rapporto RTO

Considerazioni sul rapporto RTO	Descrizione
Parametri considerati per la generazione del grafico RTO	• Raggiunto • Non raggiunto • Non verificato
Formula per definire la percentuale di stato RTO (%)	Profilo SLA assegnato ai nodi/Nodi totali*100
Codifica a colori utilizzata per il grafico	• Raggiunto = verde • Non raggiunto = rosso • Non verificato = grigio

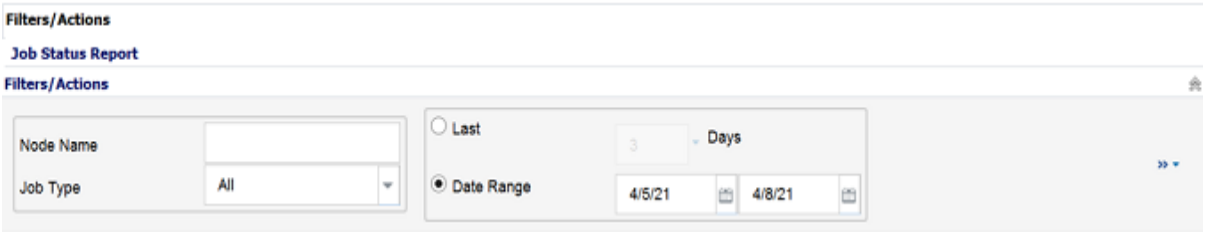

reports
Filters/Actions
Recovery Time Objective Report
Filters/Actions
84 of 179 (46%) nodes are assigned SLA profiles.
Recovery Time Objective Report
Assured Recovery Test
Virtual Machine Recovery
Instant Virtual Machine
File Level Restore
Bare Metal Restore
Met
Not Met
Not Tested
Node Name
SLA Profile Name
RTO Compliance
win-2(
N/A
Not Defined
win20
RW PROFILE
Not Tested
s-pcw10
RW PROFILE
Met (Actual 1min)

Rapporti Stato processo

Il rapporto Stato processo consente di conoscere lo stato complessivo di tutti i tipi di processi eseguiti nella console. Questo rapporto può rivelarsi utile per soddisfare i requisiti di controllo. Oltre ai filtri e alle azioni comuni, il rapporto Stato processo consente di visualizzare i risultati in base al tipo di processo, ID processo, allo stato del processo e al nome del piano (attivo o eliminato che sia). Inoltre, il formato visualizzato della durata corrisponde a Ore:Minuti:Secondi.

È possibile visualizzare il Rapporto stato processo utilizzando i filtri locali. L'opzione Filtri/Azioni contiene quanto segue:

- **Nome nodo**: filtra il rapporto Stato processo in base al nome del nodo.
- **Tipo di processo**: filtra il rapporto Stato processo in base al tipo di processo.
- **Ultimo**: consente di visualizzare il rapporto Stato processo relativo all'ultimo numero di giorni.
- **Intervallo date**: consente di visualizzare il rapporto Stato processo nell'intervallo di date specificato.



Nota: è possibile scegliere tra il filtro Ultimo o Intervallo date. Per impostazione predefinita, il filtro Ultimo è selezionato e viene visualizzato il rapporto Stato processo relativo agli ultimi 7 giorni.

Dal registro, è possibile fare clic sull'ID del processo per visualizzare i dettagli. È inoltre possibile visualizzare lo stato del processo di ogni processo.

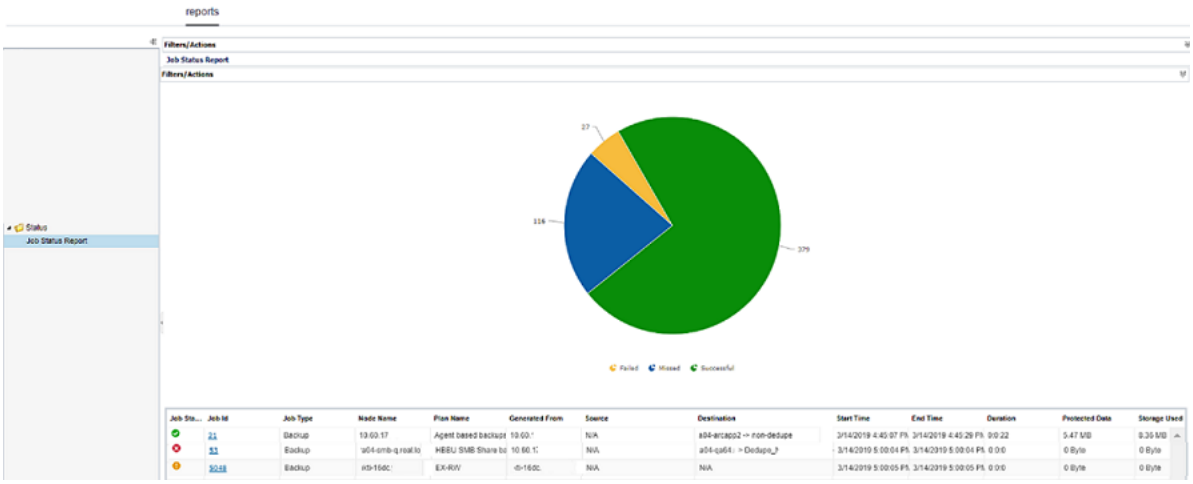
È possibile visualizzare i valori effettivi di origine e di destinazione per i tipi di processi. Il rapporto visualizza lo stato di processo seguente:

- **Completato correttamente:** fornisce un elenco dei processi che sono stati completati correttamente.
- **Non riuscito:** fornisce un elenco dei processi che non sono riusciti.
- **Incompleto**: fornisce un elenco dei processi terminati con lo stato incompleto.

- **Annullato:** fornisce un elenco dei processi che sono stati annullati.
- **Non eseguito:** fornisce un elenco dei processi che non sono stati eseguiti.

Nota: Il valore predefinito per la durata di conservazione per recuperare lo stato del processo è 180 giorni. È possibile modificare la configurazione per personalizzare i giorni di conservazione predefiniti per l'eliminazione.

Rapporto Stato processo



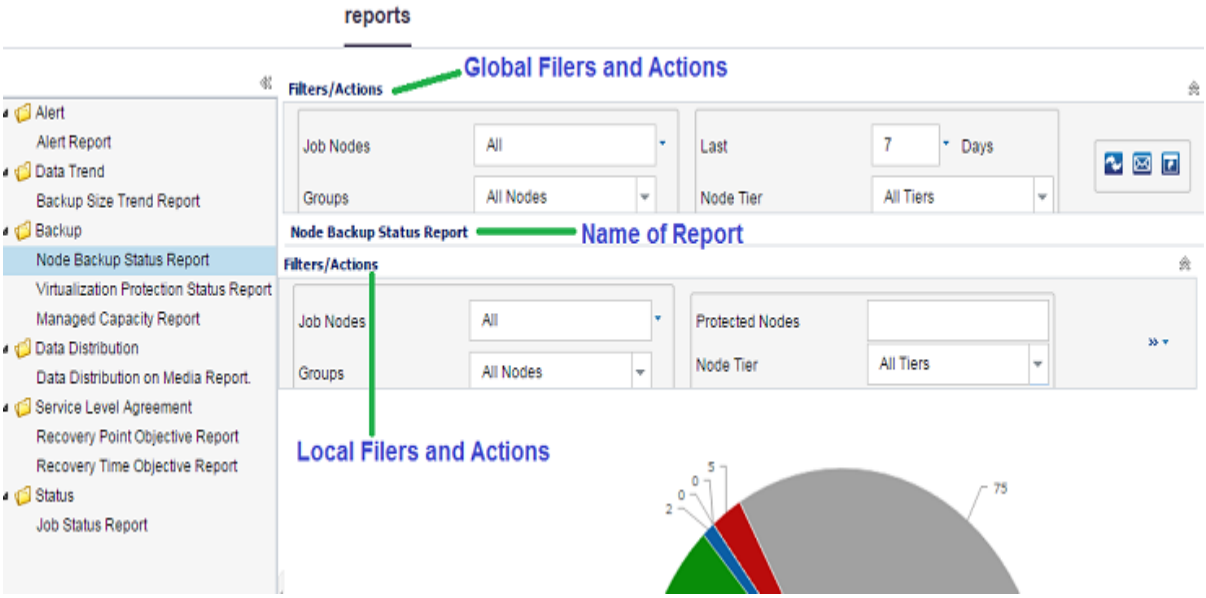
Nota: quando sono in esecuzione più processi, viene generato il rapporto di stato del processo. Tuttavia, quando si fa clic sul grafico a torta, i dati di drill-down visualizzati potrebbero essere incoerenti. Per risolvere questo problema, aggiornare il rapporto.

Utilizzo di filtri e azioni

Ciascuna pagina dei rapporti contiene due opzioni di Filtri/Azioni. La prima opzione è l'opzione globale visualizzata nella parte superiore della pagina del rapporto. La seconda opzione è l'opzione locale visualizzata al di sotto del nome del rapporto nella pagina corrispondente e fornisce soluzioni relative a un determinato rapporto.

Come prerequisito, installare Microsoft .NET Framework (versione 3.5) nel computer in cui è installata la console per consentire la corretta esportazione delle immagini contenute nei rapporti tramite la funzionalità di esportazione per i grafici dei rapporti.

Nota: Adobe Flash non è più necessario e l'installazione di .NET Framework come prerequisito consente di visualizzare i grafici.



Filtri

Le opzioni globali e locali contengono filtri per l'immissione di dati e la definizione delle opzioni di visualizzazione dei rapporti. Le opzioni disponibili per i filtri globali sono simili per tutti i rapporti. Le opzioni disponibili per i filtri locali variano in base al tipo di rapporto.

Azioni

Per rapporti che utilizzano l'opzione Globale:

- **Aggiorna:** consente di aggiornare le informazioni relative alla pagina.
- **Pianificare rapporti da inviare per posta elettronica:** consente di creare una pianificazione per i rapporti da inviare mediante Posta elettronica. Per ulteriori informazioni, consultare la sezione Pianificazione di messaggi di posta elettronica.

  Nota: un messaggio di posta elettronica pianificato esegue l'esportazione di un massimo di 5000 record.
- **Reimposta:** consente di modificare tutti i parametri di filtro sui valori predefiniti.
- **La visualizzazione rapporti mostra un solo rapporto:** consente di visualizzare un rapporto per riquadro.
- **La visualizzazione rapporti mostra vari rapporti suddivisi in due colonne:** consente di suddividere il riquadro di visualizzazione del rapporto in due colonne per la visualizzazione di più rapporti.
- **La visualizzazione rapporti mostra vari rapporti suddivisi in tre colonne:** consente di suddividere il riquadro di visualizzazione del rapporto in tre colonne per la visualizzazione di più rapporti.

  Per rapporti che utilizzano l'opzione Locale:
- **Stampa:** fare clic sull'icona corrispondente per stampare il rapporto.

  Nota: tramite l'opzione Stampa, è possibile accedere solo ai primi 50 nodi o ai primi 50 avvisi dell'elenco completo dei dati.
- **Aggiorna:** fare clic per aggiornare le informazioni sul rapporto corrispondenti.
- **Posta elettronica:** consente di inviare il rapporto mediante posta elettronica. Per ulteriori informazioni, consultare la sezione Invia rapporto per posta elettronica.

  Nota: un messaggio di posta elettronica esegue l'esportazione di un massimo di 10000 record.
- **Salva:** l'opzione consente di esportare un rapporto. Selezionare uno dei seguenti formati tra **CSV**, **PDF** e **HTML**, quindi fare clic su **Apri** o su una delle opzioni di **salvataggio** della finestra di dialogo visualizzata nella parte inferiore della pagina per esportarne il rapporto.

  Nota: tramite l'opzione Salva, è possibile accedere solo ai primi 10000 nodi o avvisi dell'elenco completo dei dati.

Utilizzo dei rapporti Arcserve UDP

La presente sezione descrive i seguenti argomenti:

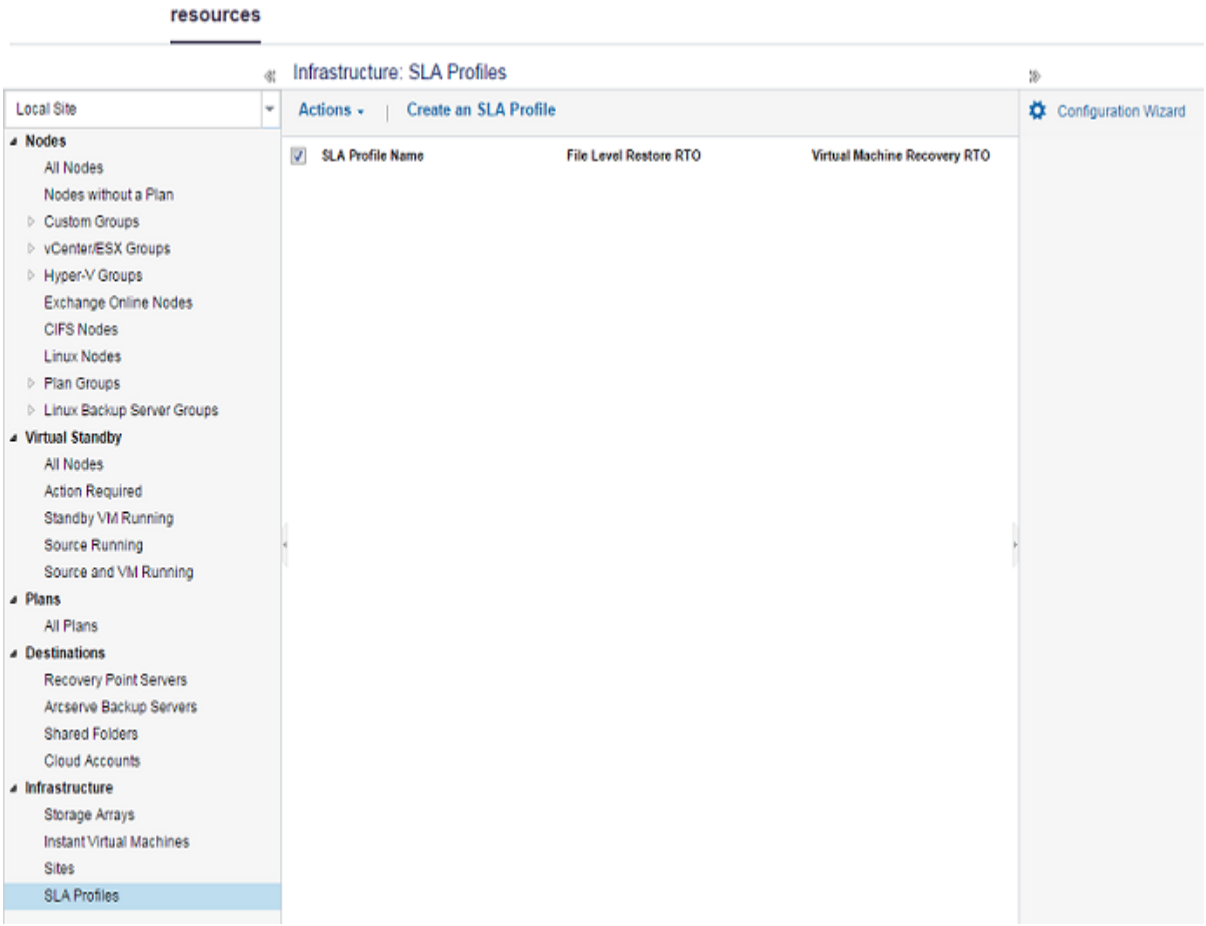
1. Creazione di un profilo SLA
2. Pianificazione dei messaggi di posta elettronica
3. Invio di rapporti tramite posta elettronica
4. Generazione di un rapporto
5. Personalizzazione dei giorni di conservazione per un rapporto sullo stato del processo
6. Dimensioni dei dati non elaborati nel rapporto sulla capacità gestita per il backup senza agente basato su host del computer virtuale
7. Visualizzazione dei valori effettivi di origine e di destinazione per i tipi di processi

Creazione di un profilo SLA

Per generare rapporti RTO, è necessario creare un profilo SLA.

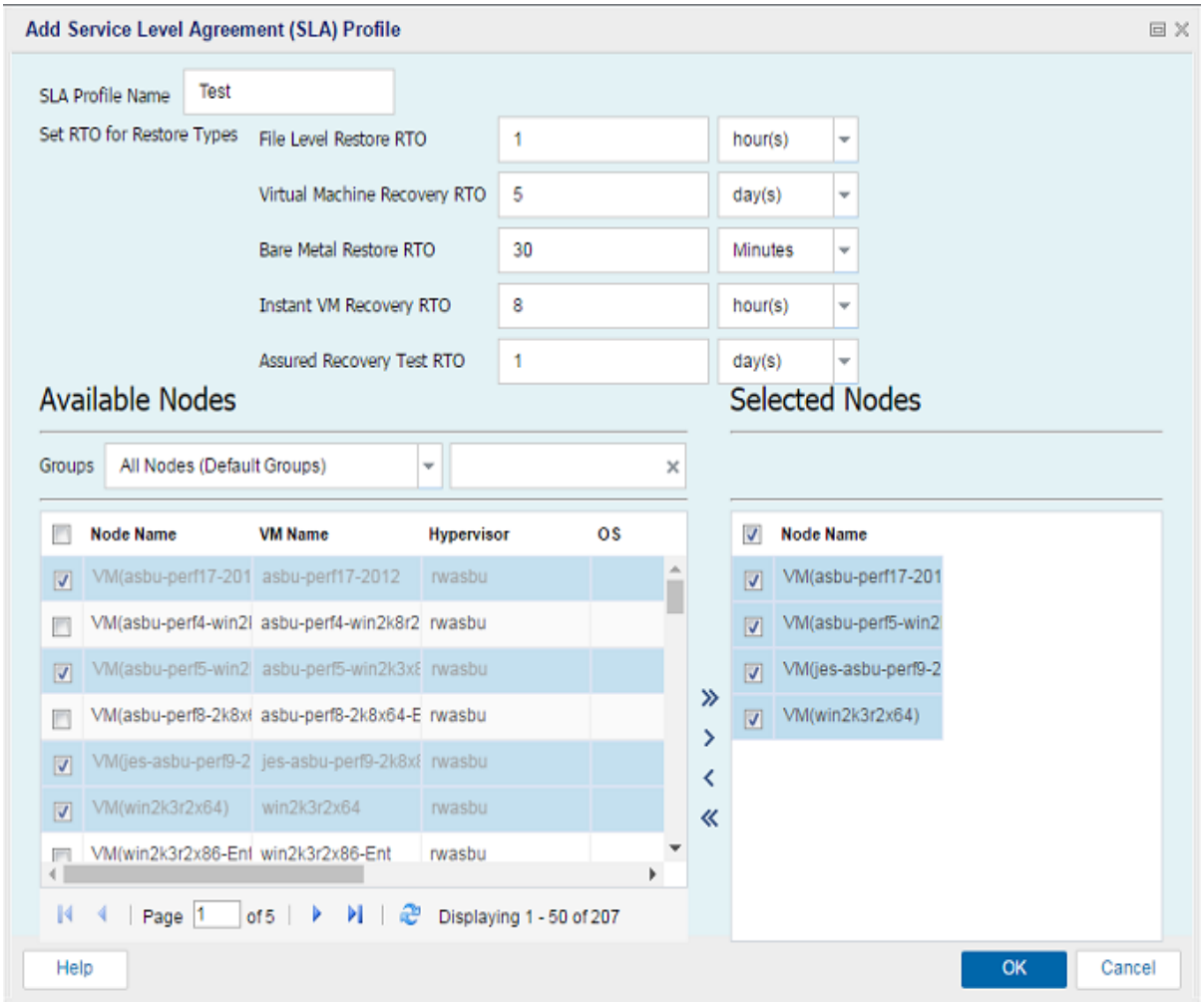
Effettuare le operazioni seguenti:

1. Accedere al riquadro sinistro della scheda **Risorse** e fare clic su **Infrastruttura**>**Profilo SLA**.



2. Fare clic su **Crea profilo SLA** dal riquadro centrale.

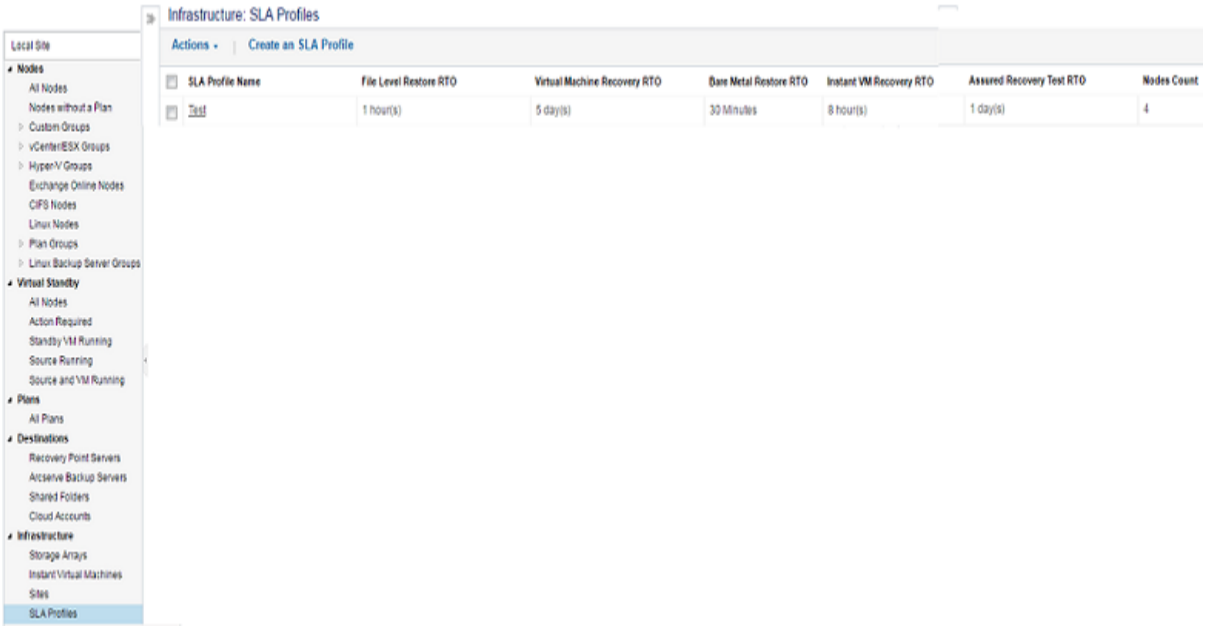
   Viene visualizzata la finestra di dialogo **Aggiungi profilo SLA**.



3. Dal riquadro Aggiungi SLA, eseguire le seguenti operazioni:
   a. Immettere un **nome per il profilo SLA**
   b. Immettere il tempo e la durata per le opzioni desiderate nel campo **Imposta RTO per il tipo di ripristino**.

      Nota: Per tutte le opzioni, è possibile selezionare il tempo in giorni, ore e minuti.
   c. Dalla sezione **Nodi disponibili**, selezionare le caselle di controllo dei nodi per cui si desidera generare rapporti, quindi spostarli nella sezione **Nodi selezionati**.
   d. Selezionare uno o più nodi in **Nodi selezionati** e fare clic su **OK**.

Il profilo SLA viene creato e aggiunto nel campo Nome profilo SLA.



4. Per modificare o eliminare il profilo SLA esistente, selezionare la casella di controllo del profilo desiderato e fare clic su **Azioni**.



È possibile visualizzare il rapporto **RTO** tramite la scheda **Rapporti** per conoscere lo stato del processo per tutti i profili SLA definiti.

Pianificazione dei messaggi di posta elettronica

Arcserve Unified Data Protection consente di creare una pianificazione per l'invio dei rapporti tramite posta elettronica ai destinatari specificati.

Nota: Prima di creare una pianificazione per l'invio di messaggi di posta elettronica, configurare le impostazioni di posta elettronica. Per ulteriori informazioni sulla configurazione, consultare la sezione Configurazione di posta elettronica e avvisi.

È possibile creare una pianificazione e modificare la pianificazione.

Creazione della pianificazione

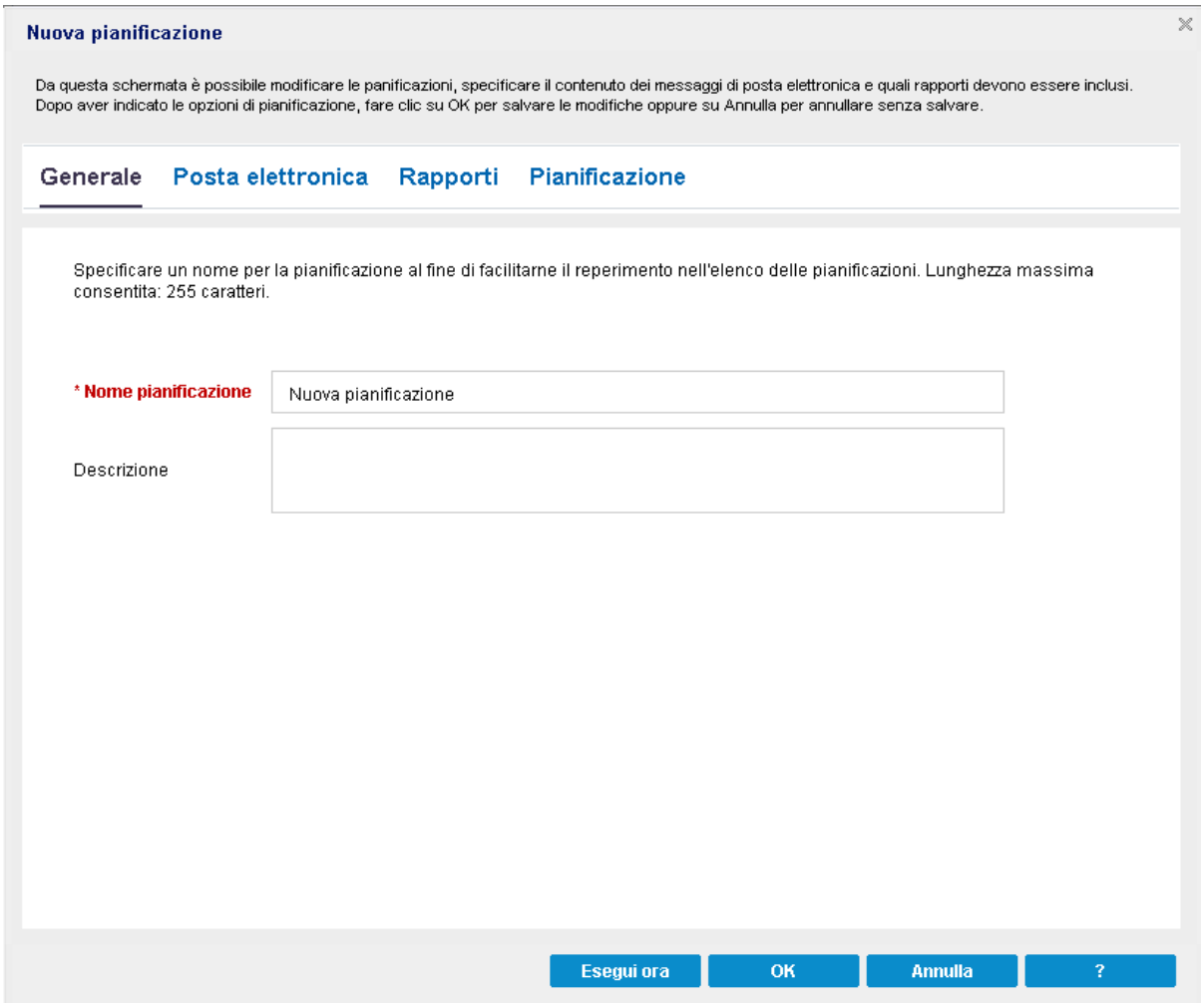
È possibile aggiungere una nuova pianificazione per l'invio dei rapporti tramite posta elettronica. I messaggi di rapporto vengono automaticamente aggiornati, generati e inviati secondo la pianificazione. È possibile personalizzare la pianificazione dei messaggi di posta elettronica di rapporto. L'applicazione consente di definire il contenuto dei messaggi di posta elettronica, i rapporti da allegare, i destinatari e la data e l'ora di invio del rapporto. I rapporti selezionati mostrano informazioni dettagliate in formato tabella all'interno del messaggio di posta elettronica.

Effettuare le operazioni seguenti:

1. Accedere ad Arcserve Unified Data Protection.
2. Dalla barra di navigazione, fare clic su **Rapporti**.
3. In alto a destra di qualsiasi rapporto, fare clic sulla sezione **Filtri/Azioni** globale.
4. Dall'elenco espanso, selezionare l'icona di posta elettronica per aprire la finestra di dialogo **Pianificare rapporti da inviare per posta elettronica.**

   Viene visualizzata la finestra di dialogo **Pianifica posta**.
5. Fare clic su **Nuovo** nella finestra di dialogo **Pianifica posta**.

   Viene visualizzata la finestra di dialogo **Nuova pianificazione**.



Sono disponibili le schede seguenti:

- **Generale**: specificare un nome e una descrizione (facoltativo) per la nuova pianificazione.
- **Posta elettronica**: specificare le impostazioni di posta elettronica, il contenuto e gli allegati per la pianificazione della posta elettronica.
- **Rapporti**: selezionare i rapporti che si desiderano includere nel messaggio di posta elettronica.
- **Pianificazione**: specificare una pianificazione per la posta elettronica.

6. Completare i campi obbligatori in ciascuna scheda.
7. Fare clic su **OK** per salvare la pianificazione.

   La nuova pianificazione viene aggiunta alla finestra di dialogo **Pianifica posta**.

   Nota: Non fare clic su **OK** se si desidera visualizzare immediatamente il rapporto.

8. (Facoltativo) Per visualizzare immediatamente il rapporto, fare clic su **Esegui ora**.

   Il rapporto viene inviato ai destinatari.

Modifica della pianificazione

Arcserve UDP consente di aggiornare una pianificazione aggiunta mediante l'operazione di creazione della pianificazione.

Effettuare le operazioni seguenti:

1. Accedere ad Arcserve Unified Data Protection.
2. Fare clic sulla scheda **Rapporti.**
3. Fare clic sulla sezione **Filtri/Azioni** globale.
4. Dall'elenco espanso, selezionare l'icona di posta elettronica per aprire la finestra di dialogo **Pianifica posta**.
5. Fare clic su **Modifica** nella finestra di dialogo **Pianifica posta**.

   Viene visualizzata la finestra di dialogo **Modifica pianificazione**.
6. Aggiornare i dettagli della pianificazione, quindi fare clic su **OK**.

   La pianificazione aggiornata viene visualizzata nella finestra di dialogo **Pianifica posta**.

   Nota: Non fare clic su **OK** se si desidera visualizzare immediatamente il rapporto.
7. (Facoltativo) Per visualizzare immediatamente il rapporto aggiornato, fare clic su **Esegui ora**.

   Il rapporto viene inviato ai destinatari.

Invia rapporto per posta elettronica

Arcserve Unified Data Protection consente di inviare singoli rapporti a destinatari specifici. Quando si invia un rapporto tramite posta elettronica, il contenuto sarà lo stesso di quello stampato e tutti i grafici verranno inviati come immagini incorporate.

Nota: prima di utilizzare l'opzione **Invia rapporto per posta elettronica**, configurare le **impostazioni di posta elettronica**. Per ulteriori informazioni sulla configurazione, consultare la sezione Configurazione di posta elettronica e avvisi.

Effettuare le operazioni seguenti:

1. Accedere ad Arcserve Unified Data Protection.
2. Dalla barra di navigazione, fare clic su **Rapporti**, quindi selezionare un rapporto.
3. Fare clic sulla sezione **Filtri/Azioni** locale, disponibile sotto il nome del rapporto selezionato.
4. Dall'elenco espanso, selezionare l'icona di posta elettronica per aprire la finestra di dialogo **Invia rapporto per posta elettronica**.

   Nota: Se la configurazione della posta elettronica non è completa, nella finestra di dialogo **Avviso** viene indicato che le impostazioni di posta elettronica non sono state specificate. Per ulteriori informazioni sulla configurazione, consultare la sezione Configurazione di posta elettronica e avvisi.



5. Completare i seguenti campi:
   - **A** : specificare il destinatario a cui viene inviato il messaggio di posta elettronica.

     Nota: il valore predefinito per questo campo è l'indirizzo di posta elettronica specificato nel modulo di configurazione.
   - **CC** : specificare ulteriori destinatari, separati da punto e virgola, a cui inviare il rapporto.
   - **Priorità** : specificare la priorità del messaggio di posta elettronica. Il valore predefinito per questo campo è Normale.
   - **Oggetto:** specificare l'oggetto del messaggio di posta elettronica. Per impostazione predefinita, nel campo viene inserito il rapporto selezionato.
   - **Commento**: (facoltativo) immettere qualsiasi informazione che si desidera condividere.
   - **Allegato** : selezionare i formati da associare ai dati del rapporto.
6. Fare clic su **OK**.

   Il messaggio di posta elettronica viene inviato.

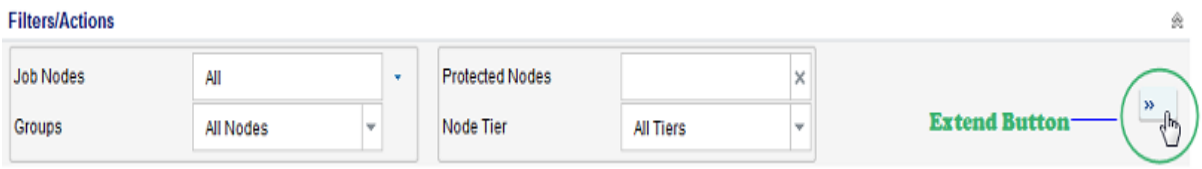
Generazione di un rapporto

È possibile generare rapporti predefiniti dalla scheda **Rapporti**. È possibile generare i rapporti nei formati PDF, CSV e HTML.

Effettuare le operazioni seguenti:

1. Accedere alla scheda **Rapporti** e selezionare un rapporto dal riquadro sinistro.
2. Fare clic sull'elenco a discesa locale **Filtri/Azioni.**
3. Immettere o selezionare i dettagli nelle opzioni dell'elenco a discesa di **Filtri/Azioni**.
4. Dall'elenco a discesa del pulsante **Salva**, fare clic su **CSV**, **PDF** o **HTML**.

   Nota: Le immagini di grandi dimensioni o più dati in una pagina del rapporto possono nascondere alcune opzioni, tra cui il pulsante Salva. Per visualizzare queste opzioni, fare clic sul pulsante Extend (Estendi).



Il rapporto viene generato nel formato selezionato.

Personalizzazione dei giorni di conservazione per un rapporto sullo stato del processo

Il valore predefinito per i giorni di conservazione per il recupero del rapporto sullo stato del processo è 180 giorni. È possibile modificare il numero di giorni di conservazione disponibile nella configurazione indicata nel file ConsoleConfiguration.xml dal percorso seguente:

Programmi\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml

In base alle proprie esigenze, è possibile modificare il numero di giorni di conservazione nella configurazione.

```
<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>
```

Dimensioni dei dati non elaborati nel rapporto sulla capacità gestita per il backup senza agente basato su host del computer virtuale

È possibile configurare i seguenti Registri di sistema a livello di proxy o di computer virtuale:

A livello di proxy per tutti i computer virtuali protetti dal proxy corrente:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

"CountNtfsVolumeSize"=dword:00000001

“ReportZeroIfHavingNonNtfsVolume”=dword:00000001

"BackupZeroBlock"=dword:00000001

A livello di computer virtuale per un computer virtuale specifico:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\{VM UUID}]

“CountNtfsVolumeSize”=dword:00000001

“ReportZeroIfHavingNonNtfsVolume”=dword:00000001

"BackupZeroBlock"=dword:00000001

Nota: Il Registro di sistema a livello di computer virtuale prevale su quello a livello di proxy.

Si osservano i seguenti comportamenti:

Chiave di registro	Impostazione predefinita	Valori possibili	Scopo	Informazioni supplementari
GetVMGuestVolumeUsedSize	0	0 o 1	Specifica se contare lo spazio utilizzato di tutti i volumi di un computer virtuale.	

			0: conta la dimensione del file VMDK del computer virtuale come dimensione dei dati non elaborati del computer virtuale. 1: conta soltanto lo spazio utilizzato dei volumi. **Nota:** Per gli utenti guest di Windows vengono considerati solo i volumi NTFS. Per gli utenti guest di Linux vengono considerati tutti i volumi.	
ReportZeroIfHavingNonNtfsVolume	0	0 o 1	Specifica il comportamento per la colonna relativa alla dimensione dei dati non	1. Ignorato se GetVMGuestVolumeUsedSize=0 2. Applicabile solo al computer virtuale Windows

			elaborati nel rapporto sulla capacità gestita quando sono presenti volumi non NTFS nei computer virtuali. 0: la dimensione dei volumi non NTFS non viene considerata nella colonna della dimensione dei dati non elaborati. 1: la dimensione globale dei dati non elaborati mostrata è 0 quando sono presenti volumi non NTFS nel computer virtuale	
BackupZeroBlock	0	0 o 1	Specifica se scrivere i blocchi di dati composti da tutti zero nella destinazione di backup. 1 - Scrive zero blocchi di dati nella destinazione	1. Ignorato se GetVMGuestVolumeUsedSize=1 2. Se è stato modificato, il valore avrà effetto solo in seguito a un backup completo

			di backup. 0- I blocchi di dati composti da zero vengono ignorati nel backup.	

Esempio

Un computer virtuale dispone di un disco virtuale thin provisioning con dimensioni di provisioning pari a 1000 GB. Le dimensioni del file VMDK del disco virtuale è di 800 GB, di cui 200 GB di blocchi di dati composti da tutti zero. Nel sistema operativo guest del computer virtuale sono disponibili 2 volumi NTFS il cui spazio utilizzato è rispettivamente 100 GB e 200 GB e 1 volume FAT32 il cui spazio utilizzato è di 1 GB.

Nomi delle chiavi	Valori predefiniti	Valori personalizzati	Impostazioni personalizzate	Valori personalizzati
GetVMGuestVolumeUsedSize	0	0	1	1
ReportZeroIfHavingNonNtfsVolume	N/D	N/D	1	1
BackupZero Block	0	1	N/D	N/D
Expected Raw DataSize	600 GB (esclusi i blocchi di dati composti da zero)	800 GB (compresi i blocchi di dati composti da zero)	300 GB	0

Visualizzazione dei valori effettivi di origine e di destinazione per i tipi di processi

La tabella seguente descrive i valori effettivi di origine e di destinazione visualizzati per tutti i tipi di processo che consentono di comprendere il rapporto Stato del processo:

Tipo di processo	Valore effettivo di origine	Valore effettivo di destinazione	Commenti
Backup FS sull'Archivio dati (di deduplicazione / non di deduplicazione) - Nodi Windows, Linux	Non disponibile (N\D)	Visualizzato come previsto	
Backup FS su condivisione di rete	N/D	Visualizzato come previsto	
Ripristino FS da condivisione di rete	N/D	N/D	
Processi di backup CIFS - Archivio dati non di deduplicazione	N/D	Visualizzato come previsto	
Processi di ripristino CIFS - Archivio dati non di deduplicazione	Visualizzato come previsto	N/D	
Ripristino FS da archivio dati (di deduplicazione / non di deduplicazione)	Visualizzato come previsto	N/D	
Copia file da archivio dati (di deduplicazione / non di deduplicazione), Copia file da DS di replica	Visualizzato come previsto	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Archiviazione di file da archivio dati (di deduplicazione / non di deduplicazione), Archiviazione di file da DS di replica	Visualizzato come previsto	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Copia file / Archiviazione file su condivisione N\W	N/D	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D

Ripristino di Copia file / Archiviazione file	N/D	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Eliminazione Archiviazione file	N/D		**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Processo di catalogo FS (basato sull'agente/senza agente)	Visualizzato come previsto	N/D	
Copia dei punti di ripristino dall'archivio dati (di deduplicazione, non di deduplicazione)	Visualizzato come previsto	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Copia di punti di ripristino da condivisione N\W, locale	N/D	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Ripristino della copia dei punti di ripristino su condivisione N\W, locale	N/D	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Processi del computer virtuale istantaneo	Visualizzato come previsto	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Processi Assured Recovery	Visualizzato come previsto	N/D	
Ripristino bare metal da Archivio dati (di deduplicazione / Non di deduplicazione)	Visualizzato come previsto	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Processi Virtual Standby	Visualizzato	N/D	**Nota:** Le colonne Dati

	come previsto		protetti e Archiviazione utilizzata sono visualizzate come N/D
Processi Copia su nastro	Visualizzato come previsto	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Processi di replica, Processi di replica tra siti	Visualizzato come previsto	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Processi di replica MSP	Visualizzato come previsto	Visualizzato come previsto	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Jumpstart RPS da Condivisione N\W	Visualizzato come previsto	N/D	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D
Jumpstart RPS (Archivio dati di deduplicazione / Non di deduplicazione)	Visualizzato come previsto	Visualizzato come previsto	**Nota:** Le colonne Dati protetti e Archiviazione utilizzata sono visualizzate come N/D

Chapter 7: Gestione di High Availability

La presente sezione descrive i seguenti argomenti:

Funzionamento di High Availability

Unified Data Protection consente di monitorare e gestire le funzioni di Arcserve High Availability dalla scheda **high availability**. Per gestire queste funzioni, occorre accedere innanzitutto al Servizio di controllo. La prima volta che si seleziona la scheda **High Availability**, viene aperta la finestra di dialogo **Aggiungi un Servizio di controllo.** Questa finestra di dialogo non verrà visualizzata in seguito.

Gestione dei servizi di controllo High Availability

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **High Availability.**

   Viene aperta la finestra di dialogo **Aggiungi un Servizio di controllo**.

2. Immettere i dettagli del servizio di controllo come l'indirizzo IP, il nome account, la password, il protocollo e il numero di porta.

3. Fare clic su **OK**.

   Il servizio di controllo specificato viene aggiunto sotto l'intestazione Servizi e scenari di controllo nel riquadro sinistro. Per modificare o eliminare un servizio di controllo, selezionarlo e fare clic con il pulsante destro del mouse per visualizzare le opzioni. È inoltre possibile selezionare il servizio di controllo nel riquadro centrale e fare clic sul menu **Azioni** per modificare o eliminare un servizio di controllo. Oppure fare clic con il pulsante destro del mouse sul servizio di controllo nel pannello di navigazione.

   Nota: Espandere il servizio di controllo per visualizzare gli scenari, i gruppi e gli altri dettagli.

Gestione delle licenze High Availability

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **High Availability.**
2. Nel riquadro sinistro, fare clic su **Servizi e scenari di controllo**.

   Viene visualizzata la pagina **Servizi e scenari di controllo**.
3. Selezionare il servizio di controllo e fare clic su **Registra**.

   Viene visualizzata la finestra di dialogo **Registra**.
4. Immettere la chiave di registrazione
5. Fare clic su **OK**.

   La licenza è registrata.

Gestione di scenari

Arcserve Unified Data Protection consente di gestire gli scenari HA esistenti e di creare scenari di sistema completo. È inoltre possibile creare gruppi di scenari per l'organizzazione degli scenari. Le sezioni seguenti descrivono le modalità di gestione degli scenario HA:

- Gestione del gruppo di scenari
- Creazione di scenari Sistema completo
- Gestione di scenari
- Modifica degli scenari
- Gestione degli host scenario
- Operazioni sugli scenari
- Ripristino bare metal e Replica inversa
- Monitoraggio degli scenari

Gestione del gruppo di scenari

Arcserve Unified Data Protection consente di gestire gruppi in un servizio di controllo. È possibile aggiungere, rinominare, eliminare, assegnare un flag e pubblicare commenti per un gruppo.

Effettuare le operazioni seguenti:

1. Selezionare un Servizio di controllo gestito dal riquadro sinistro.

   Nel riquadro centrale vengono elencati tutti i gruppi del Servizio di controllo.

2. Fare clic sul menu a discesa **Azioni**, quindi fare clic su una delle opzioni seguenti:

   Aggiungi gruppo di scenari

   Crea un gruppo.

   Selezionare un gruppo per eseguire le azioni seguenti:

   Rinomina il gruppo di scenari

   Rinomina il gruppo.

   Rimuovi il gruppo di scenari

   Elimina il gruppo. Non è possibile rimuovere un gruppo se esso contiene degli scenari.

   Assegna un flag e commenta

   Assegna un flag di diversi colori al gruppo e consente di aggiungere dei commenti per il flag. Utilizzare i flag per personalizzare e identificare con facilità il proprio gruppo.

3. Facoltativamente, fare clic con il pulsante destro del mouse su un gruppo nel riquadro sinistro per aggiungere, eliminare o rinominare un gruppo del servizio di controllo selezionato.

   Il gruppo viene aggiunto o aggiornato in base alla propria selezione.

Creazione di scenari Sistema completo

Effettuare le operazioni seguenti:

1. Dal riquadro sinistro, fare clic su **Servizi e scenari di controllo**, quindi fare clic su un servizio di controllo gestito.

   Tutti i gruppi di scenari nel servizio di controllo sono elencati.

2. Fare clic su un gruppo di scenari.

   Nel riquadro centrale viene visualizzata la pagina **Scenari**.

3. Nel riquadro centrale, fare clic su **Crea scenario**.

   Nota: Facoltativamente, nel riquadro sinistro, è possibile fare clic con il pulsante destro del mouse, quindi fare clic su **Crea scenario**.

   Vengono visualizzate la procedura guidata di **creazione sistemi completi** e la finestra di dialogo **Selezione del server e del tipo di prodotto**.

4. Immettere il nome dello scenario, selezionare il tipo di prodotto e specificare se si desidera la verifica Assured Recovery.

5. Fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo **Host master e di replica**.

6. Immettere i dettagli per Host master e di replica.

7. Fare clic su **Avanti**.

   I moduli vengono verificati sugli host se l'opzione di **verifica del modulo su host** è stata selezionata. È anche possibile installare dei moduli sugli host o disinstallare dei moduli dagli host.

8. Fare clic su **Avanti** dopo aver verificato i moduli.

   Viene visualizzata la finestra di dialogo **Impostazioni volume**.

9. Selezionare i volumi che si desidera proteggere.

   Nota: Quando si seleziona l'opzione **Abilita l'esclusione di directory e file**, pagefile.sys, hyberfil.sys, le informazioni sul volume di sistema, il file di riciclo, i file riciclati e le cartelle vengono filtrati per impostazione predefinita.

10. Fare clic su **Avanti**.

    Viene visualizzata la finestra di dialogo **Selezione del pool di risorse**. È possibile selezionare il pool di risorse in cui si trova il computer virtuale dopo l'avanzamento o durante la verifica Assured Recovery.

11. Fare clic su **Avanti**.

    Viene visualizzata la finestra di dialogo **Selezione archiviazione**.

12. Selezionare l'archivio dati per archiviare il computer virtuale. Facoltativamente, selezionare **Allocare e confermare lo spazio su richiesta (mediante disco dinamico)**. Il computer virtuale generato utilizza il thin provisioning per il disco virtuale se si seleziona questa opzione.
13. Fare clic su **Avanti**.

    Viene visualizzata la finestra di dialogo **Proprietà scenario**.
14. Espandere le proprietà e apportare le modifiche desiderate, quindi fare clic su **Avanti**. Per ulteriori informazioni, consultare la Guida per l'amministratore di Arcserve RHA.

    Viene visualizzata la finestra di dialogo **Proprietà di master e replica**.
15. Verificare le proprietà degli host master e di replica, quindi fare clic su **Fare clic per modificare i mapping di rete fisica**.

    Viene visualizzata la finestra di dialogo **Mapping scheda di rete High Availability**.

    Nota: Se è presente un'unica scheda di rete virtuale nei server master e di replica, questi ultimi vengono mappati automaticamente.
16. Procedere come segue:
    a. In **Scheda di rete replica,** fare clic per selezionare la scheda di cui si desidera eseguire il mapping sulla scheda elencata nella colonna Scheda di rete master.
    b. In **Applica informazioni sulla scheda master** (impostazione predefinita), selezionare se la scheda master è in modalità DHCP.
    c. Selezionare **Personalizza informazioni scheda** per abilitare l'indirizzo IP, il gateway, i server DNS e l'impostazione Server WINS. Aggiungere o rimuovere l'indirizzo IP, i gateway, i server DNS e i server WINS se necessario.
17. Fare clic su OK per chiudere la finestra di dialogo **Mapping scheda di rete**, quindi fare clic su **Avanti** per continuare.

    Viene visualizzata la finestra di dialogo **Proprietà avanzamento**.
18. Espandere **Reindirizzamento traffico di rete** e le altre proprietà per verificare i valori, quindi fare clic su **Avanti**.

    Viene visualizzata la finestra di dialogo **Avvio replica inversa e di avanzamento**
19. Specificare il tipo di avanzamento. Per gli scenari Sistema completo, la replica inversa è manuale.
20. Fare clic su **Avanti**.

    Attendere mentre viene completato il processo Verifica scenario e viene visualizzata la finestra di dialogo **Verifica scenario**.

Per continuare, è necessario risolvere gli eventuali errori rilevati dal processo Verifica scenario. Risolvere anche gli eventuali avvisi elencati. Dopo aver apportato le modifica, fare clic su **Riprova** per ripetere la verifica.

21. Fare clic su **Avanti**.

    Viene visualizzata la finestra di dialogo **Esecuzione scenario**.

22. Fare clic su **Fine** per salvare le impostazioni correnti ed eseguire lo scenario in un secondo momento.

    Facoltativamente, per eseguire lo scenario istantaneamente, selezionare **Esegui ora** dopo aver fatto clic sul pulsante Fine, quindi fare clic su **Fine**.

    Per gli scenari di sistema completo, selezionare **Sincronizzazione volume**.

    Verrà, quindi, creato lo scenario.

Gestione di scenari

Quando si seleziona un Servizio di controllo gestito dal riquadro sinistro, tutti gli scenari nel Servizio di controllo vengono mostrati nel riquadro centrale. Gli scenari vengono elencati con il relativo tipo, stato, prodotto e modalità. Le statistiche di RPO/RTO, dell'utilizzo dello spool master e dell'avanzamento della sincronizzazione sono inoltre elencate qui. Selezionando uno scenario è possibile eseguire varie operazioni come ad esempio eliminare, rinominare, assegnare un flag o commentare.

Effettuare le operazioni seguenti:

1. Dal riquadro sinistro, fare clic su **Servizi e scenari di controllo**, quindi fare clic su un servizio di controllo gestito.

   Tutti i gruppi di scenari nel servizio di controllo sono elencati nel riquadro centrale.

2. Dal riquadro sinistro, fare clic su un gruppo di scenari.

   Nel riquadro centrale vengono elencati gli scenari nel gruppo di scenari.

3. Selezionare uno scenario.

4. Fare clic sul menu a discesa **Azioni**, quindi fare clic su una delle opzioni seguenti:

   Rinomina scenario

   Rinomina lo scenario.

   Rimuovi scenario

   Elimina lo scenario.

   Non è possibile rimuovere un gruppo se esso contiene degli scenari.

5. Facoltativamente, dal riquadro sinistro, fare clic con il pulsante destro del mouse su uno scenario per eliminarlo o rinominarlo.

   Il scenario viene aggiornato.

Modifica degli scenari

Arcserve Unified Data Protection consente di modificare le proprietà dello scenario quando lo scenario è in stato Interrotto. È possibile inserire, rinominare o eliminare host o modificare la topologia di uno scenario.

Effettuare le operazioni seguenti:

1. Dal riquadro sinistro, fare clic su **Servizi e scenari di controllo**, quindi fare clic su un servizio di controllo gestito.

   Tutti i gruppi di scenari nel servizio di controllo sono elencati nel riquadro centrale.

2. Dal riquadro sinistro, fare clic su un gruppo di scenari, quindi fare clic su uno scenario.

   Viene visualizzata la pagina <scenario group>:<scenario>.

3. Selezionare un host dallo scenario.

4. Fare clic sulla scheda **Proprietà** e selezionare una delle opzioni seguenti dall'elenco a discesa.

   Proprietà scenario

   Aggiorna le proprietà degli scenari.

   Proprietà HA

   Aggiorna le proprietà High Availability.

   Proprietà host

   Aggiorna le proprietà dell'host.

   Directory principali

   Aggiorna le directory principali.

   Nota: Ciò si applica solo agli scenari di sistema completi.

5. Fare clic su **Salva** dal menu a discesa **Azione**.

   Le proprietà dello scenario vengono aggiornate.

   Modificare le impostazioni della piattaforma virtuale per uno scenario di sistema completo interrotto.

   Effettuare le operazioni seguenti:

1. Selezionare un host di replica dallo scenario.

2. Fare clic sulla scheda **Proprietà** e **Proprietà host** dall'elenco a discesa.

3. Espandere **Computer virtuale** e selezionare **Fare clic qui per modificare le impostazioni della piattaforma virtuale**.

Viene visualizzata la procedura guidata **Impostazioni della piattaforma virtuale**.

4. Selezionare **Tipo di piattaforma virtuale** e il relativo indirizzo IP o nome host.
5. Selezionare il pool di risorse per il server ESX e vCenter o il server host per Citrix Xen.
6. Selezionare l'archiviazione. Per Hyper-V, accedere alle directory e selezionare la posizione del computer virtuale sul server Hyper-V.
7. Fare clic su **Fine**.

Modificare il mapping della scheda di rete per High Availability o Assured Recovery, eseguire i passaggi seguenti.

Effettuare le operazioni seguenti:

1. Selezionare l'host di replica dallo scenario.
2. Fare clic sulla scheda **Proprietà** e selezionare **Proprietà host** dall'elenco a discesa.
3. Espandere **Computer virtuale** e fare clic su **Impostazioni computer virtuale**.
4. Selezionare **Fare clic per modificare i mapping di rete fisica** per la proprietà **Mapping scheda di rete High Availability** o **Mapping scheda di rete Assured Recovery**.

   Viene visualizzata la finestra di dialogo **Mapping scheda di rete High Availability**.
5. Selezionare le schede di rete della replica per eseguire il mapping della scheda di rete master.

   È possibile personalizzare le informazioni sulla scheda di replica includendo l'indirizzo IP, il gateway, i server DNS e i server WINS.
6. Fare clic su **OK**.

   I mapping vengono modificati e salvati.

Gestione degli host scenario

È possibile inserire, eliminare e rinominare gli host in uno scenario.

Effettuare le operazioni seguenti:

1. Dal riquadro sinistro, fare clic su **Servizi e scenari di controllo**, quindi fare clic su un servizio di controllo gestito.

   Tutti i gruppi di scenari nel servizio di controllo sono elencati nel riquadro centrale.
2. Dal riquadro sinistro, fare clic su un gruppo di scenari, quindi fare clic su uno scenario.

   Viene visualizzata la pagina <scenario group>:<scenario>.
3. Selezionare un host dallo scenario.
4. Fare clic sul menu a discesa **Modifica**, quindi fare clic su una delle opzioni seguenti:

   Inserisci host

   Inserisce un host figlio all'host selezionato nello scenario.

   Rimuovi host

   Elimina l'host selezionato dallo scenario.

   Rinomina host

   Rinomina l'host selezionato nello scenario.

   Salva

   Salva tutte le modifiche apportate alle proprietà dello scenario.

   Aggiorna

   Aggiorna tutte le modifiche.

   Le proprietà dello scenario vengono modificate.

Operazioni sugli scenari

È possibile eseguire diverse operazioni sugli scenari.

Effettuare le operazioni seguenti:

1. Dal riquadro sinistro, fare clic su **Servizi e scenari di controllo**, quindi fare clic su un servizio di controllo gestito.

   Tutti i gruppi di scenari nel servizio di controllo sono elencati nel riquadro centrale.

2. Dal riquadro sinistro, fare clic su un gruppo di scenari, quindi fare clic su uno scenario.

   Viene visualizzata la pagina <scenario group>:<scenario>.

3. Fare clic sul menu a discesa **Azioni**, quindi fare clic su una delle opzioni seguenti:

   Esegui

   Dopo aver creato uno scenario, è necessario eseguirlo per avviare il processo di replica. Di norma, prima che le modifiche apportate ai dati sul server master possano essere replicate sul server di replica, è necessario sincronizzare i server master e di replica. Di conseguenza, il primo passaggio dell'avvio di una replica consiste nella sincronizzazione dei server master e di replica. Dopo aver sincronizzato i server, verrà avviata automaticamente una replica in linea, che aggiornerà continuamente il server di replica con tutte le modifiche apportate sul server master.

   Esegui (Modalità valutazione)

   La modalità di valutazione consente di valutare accuratamente l'utilizzo della larghezza di banda e i punti di riferimento del rapporto di compressione necessari per la replica, senza la necessità di replicare realmente i dati. Quando si esegue questo comando, non viene eseguita una replica, ma verranno raccolti dati statistici. Al termine del processo di valutazione verrà generato un rapporto.

   Interrompi

   Uno scenario in esecuzione può essere interrotto per impostarne o modificarne le proprietà. È possibile interrompere gli scenari in esecuzione o in modalità di valutazione.

   Sincronizza

   La sincronizzazione è un processo che consente di rendere i dati coerenti nei server master e di replica. L'opzione consente di attivare il processo di sincronizzazione (che la replica sia in esecuzione o meno).

Rapporto delle differenze

Un rapporto delle differenze confronta le differenze fra il master e la replica in un determinato momento. Il confronto viene eseguito mediante gli stessi algoritmi utilizzati nel processo di sincronizzazione, ma senza trasferire alcun dato. Per ogni server di replica verrà generato un rapporto delle differenze, che verrà quindi inviato alla Gestione al termine del processo. Il rapporto può essere generato in qualsiasi momento.

Esecuzione dell'avanzamento

L'avanzamento (o failover) è il processo di modifica dei ruoli tra il master e la replica. In tal modo, il server master diventa il server di standby, mentre il server di replica diventa il server attivo.

Ripristino del server attivo

Se il processo di avanzamento non viene completato correttamente, è possibile selezionare manualmente il server che dovrà fungere da server attivo durante un processo denominato Recupera server attivo.

Interrompi verifica di funzionamento

Consente di sospendere la verifica di funzionamento che controlla se il server attivo è operativo. È possibile sospendere/riprendere manualmente la verifica di funzionamento per uno scenario HA in esecuzione.

Verifica di integrazione della replica

L'opzione Assured Recovery consente di eseguire una verifica trasparente completa della recuperabilità dei dati sul server di replica. Il server di replica che viene testato è quello che subentrerebbe al server di produzione qualora questo non fosse attivo. L'opzione Assured Recovery è una verifica effettiva del server reale, delle applicazioni e delle azioni che saranno necessarie nel caso in cui il server di replica dovesse diventare il server attivo e svolgerne le relative funzioni.

Avvia/Interrompi computer virtuale

Servirsi dell'operazione per avviare o interrompere un computer virtuale a partire dall'ultimo stato di sistema o da un segnalibro. È possibile avviare o interrompere un computer virtuale dopo aver creato uno scenario ed aver sincronizzato il master con la replica. Utilizzare questa funzionalità quando lo scenario non è in esecuzione. Si tratta di una funzionalità disponibile per scenari DR e HA di sistema completo. La funzionalità Avvia/Interrompi è un elemento del menu di attivazione/disattivazione.

Sospendi replica

Consente di sospendere gli aggiornamenti della replica sull'host di replica allo scopo di eseguire la manutenzione del sistema o qualche altra forma di elaborazione che non modifica i dati ivi replicati. La registrazione delle modifiche continuerà a essere eseguita per l'aggiornamento del server di replica sospeso, ma il trasferimento effettivo non verrà eseguito fino alla ripresa della replica. Non è possibile sospendere la replica durante la sincronizzazione.

Elimina tutte le risorse del computer virtuale

Quando viene eseguito uno scenario di sistema completo, vengono create alcune risorse temporanee come ad esempio file di disco, snapshot e altri file. L'operazione consente di eliminare tali risorse ed è disponibile quando lo scenario non è in esecuzione.

Ripristino dei dati

Consente di recuperare dati perduti o danneggiati sul server master da qualsiasi server di replica attivando un processo di sincronizzazione in direzione inversa.

Imposta segnalibro di ripristino

Un segnalibro è un punto di arresto impostato manualmente per marcare uno stato al quale è possibile eseguire il ripristino. Questa impostazione manuale viene chiamata Segnalibro di ripristino. Si consiglia di impostare un segnalibro prima di eseguire qualsiasi attività che potrebbe provocare l'instabilità dei dati. I segnalibri vengono impostati in tempo reale, non per eventi passati.

L'operazione selezionata viene eseguita.

Ripristino bare metal e Replica inversa

Arcserve Unified Data Protection consente di elaborare il ripristino bare metal e la replica inversa per gli scenari di sistema completo.

Effettuare le operazioni seguenti:

1. Preparare un computer bare metal caricando il computer dal CD del ripristino bare metal
2. Selezionare lo scenario Sistema completo e fare clic su **Ripristina** dal menu a discesa di **Azioni**.

   Verrà visualizzato il **Ripristino guidato dei dati**.
3. Seguire le istruzioni riportate nelle schermate della procedura guidata per creare ed eseguire lo scenario di recupero.

   Nota: Nella pagina **Mapping del volume**, se i volumi vengono mappati automaticamente per l'origine e la destinazione, il mapping del volume personalizzato viene disattivato. Per abilitare il mapping di volume personalizzato, fare clic su **Cancella** per rimuovere il mapping precedente. Fare clic con il tasto destro del mouse sul volume selezionato e selezionare **Mapping del volume personalizzato** per aprire la finestra di dialogo **Ridimensiona volume** e modificare le dimensioni come lo si desidera.

Per eseguire la replica inversa, procedere come segue:

1. Preparare un computer bare metal caricando il computer dal CD del ripristino bare metal
2. Selezionare lo scenario Sistema completo che ha eseguito l'avanzamento o il failover e fare clic su **Esegui** nel menu a discesa **Azioni**.

   Verrà visualizzato il **Ripristino guidato dei dati**.
3. Seguire le istruzioni riportate nelle schermate della procedura guidata per creare ed eseguire lo scenario di recupero.

   Viene eseguito il ripristino dei dati sul computer bare metal. Se è stato selezionato l'avanzamento automatico, il processo di avanzamento viene avviato e il computer bare metal è pronto. Se è stato selezionato l'avanzamento manuale, è necessario avviare manualmente il processo di avanzamento.

Monitoraggio degli scenari

Arcserve Unified Data Protection consente di monitorare gli scenari DR o HA fornendo diversi rapporti e statistiche.

Effettuare le operazioni seguenti:

1. Dal riquadro centrale, selezionare uno scenario.

   Viene visualizzato lo stato dello scenario in esecuzione con dettagli quali ad esempio dati inviati, file inviati, dati ricevuti, file ricevuti e così via.

2. Fare clic sulla scheda **Statistiche** per ulteriori dettagli. La scheda contiene le due categorie seguenti:

   Statistiche in esecuzione

   Visualizza i dati statistici dettagliati durante l'esecuzione dello scenario.

   Record cronologia

   Visualizza rapporti di sincronizzazione, rapporti delle differenze e rapporti di verifica Assured Recovery.

3. Fare clic sulla scheda **Eventi** per visualizzare tutti gli eventi di uno scenario selezionato. Per copiare o cancellare gli eventi, selezionare gli eventi e fare clic con il tasto destro del mouse, quindi selezionare **Mostra eventi** per aprire la finestra di dialogo corrispondente per la copia o l'eliminazione di eventi. Utilizzare i tasti Shift+Ctrl per selezionare più eventi.

   Nota: Gli eventi vengono aggiornati automaticamente. I cinque eventi critici recenti vengono visualizzati nel riquadro quando si seleziona uno scenario.

4. Selezionare il gruppo di scenari dal riquadro a sinistra. Nel riquadro centrale vengono elencati gli scenari nel gruppo. L'elenco consente di verificare l'utilizzo dello spool master, RPO/RTO e l'avanzamento della sincronizzazione.

5. I dettagli del riquadro destro forniscono informazioni quali il nome dello scenario, lo stato dello scenario e l'avanzamento della sincronizzazione.

   Nota: nel riquadro destro, la percentuale di spool indica l'utilizzo di spool del server master nello scenario.

Installazione remota

Arcserve Unified Data Protection consente di distribuire il modulo da un servizio di controllo gestito agli host remoti. Si può anche gestire l'installazione e la verifica dall'elenco degli host.

Effettuare le operazioni seguenti:

1. Nel riquadro sinistro, fare clic su **Installazione remota**.

   Nel riquadro centrale viene visualizzata la pagina **Installazione remota**.

2. Dall'elenco a discesa **Servizio di controllo**, selezionare un servizio di controllo che si desidera utilizzare per distribuire il modulo.

   Gli host esistenti in cui il modulo è stato installato o verificato in precedenza vengono elencati nel riquadro centrale.

3. Dal menu a discesa **Azione,** fare clic su **Aggiungi host**.

   Viene visualizzata la finestra di dialogo **Host di installazione modulo**.

4. Immettere il nome host o l'indirizzo IP dell'host e fare clic su **Aggiungi**.

   L'host viene aggiunto all'elenco.

5. Fare clic su **OK**.

   Viene visualizzata la finestra di dialogo **Aggiungi host**.

6. Selezionare una delle seguenti opzioni:

   Modifica host

   Viene visualizzata la finestra di dialogo **Host di installazione modulo** che consente di aggiungere host o di gestire quelli esistenti.

   Modifica impostazioni installazione

   Viene visualizzata la finestra di dialogo **Modifica impostazioni di installazione.** È possibile specificare i seguenti dettagli:

   Account di installazione

   Account servizio

   Porta

   Usa impostazioni precedenti in caso di nuova installazione o aggiornamento

   Consente di aggiornare o reinstallare un modulo RHA esistente.

7. Fare clic su **OK**.

8. L'host viene visualizzato nella pagina **Installazione remota**.

   La colonna **Stato** visualizza lo stato di installazione.

Nota: Passare il puntatore del mouse sullo stato per ottenere i dettagli in caso di installazione non riuscita.

Azioni per l'installazione remota

È possibile eseguire varie operazioni sugli host aggiunti.

Effettuare le operazioni seguenti:

1. Dal riquadro centrale, selezionare un host.
2. Fare clic sul menu a discesa **Azioni**, quindi selezionare una delle opzioni seguenti:

Aggiungi host

Viene visualizzata la finestra di dialogo **Host di installazione modulo**. Per ulteriori informazioni, consultare la sezione Installazione remota.

Installa/aggiorna

Consente di installare o aggiornare il modulo HA sull'host selezionato.

Disinstalla

Consente di disinstallare il modulo HA dall'host selezionato.

Modifica impostazioni

Viene visualizzata la finestra di dialogo **Modifica impostazioni di installazione**.

Check Host Status (Verifica stato host)

Consente di verificare se l'host esiste.

Rimuovi host

Consente di rimuovere l'host dall'elenco.

Visualizzazione registri

Viene visualizzata la finestra di dialogo **Registri di installazione remota** contenente i registri di tutti gli host remoti. Fare clic per aggiornare e visualizzare i registri più recenti.

L'operazione è stata completata correttamente.

Rapporti High Availability

Arcserve Unified Data Protection fornisce vari rapporti per monitorare lo stato di High Availability. È possibile applicare filtri per generare diversi tipi di rapporti, se necessario.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Servizi e scenari di controllo**.
2. Dal riquadro sinistro, fare clic su **Rapporti**.
3. Nel riquadro centrale viene visualizzata la pagina **Rapporti**.
4. Dal riquadro centrale, selezionare un servizio di controllo dall'elenco a discesa **Servizio di controllo**.
5. Immettere i dettagli e applicare i filtri in base alle necessità.

   Il rapporto HA è stato generato.

Chapter 8: Utilizzo dell'utilità VSphereConfig

La presente sezione descrive i seguenti argomenti:

Attivazione o disattivazione del tag VSP-hereBackupNFC mediante il prompt dei comandi

Importante! Abilitare il tag VSphereBackupNFC sulla scheda kernel specifica per il backup (anziché sulla rete di backup specifica) quando un computer virtuale di origine ospita l'hypervisor ESXi e il backup utilizza VDDK7 (o versioni successive).

Arcserve UDP consente di attivare o disattivare il tag *VSphereBackupNFC* utilizzando il prompt dei comandi. Lo strumento della riga di comando (*AFVSphereConfigTool.exe*) consente di attivare o disattivare il tag VSphereBackupNFC su una scheda kernel specifica.

In questa sezione vengono fornite informazioni su come attivare o disattivare il tag *VSphereBackupNFC* utilizzando il prompt dei comandi.

Effettuare le operazioni seguenti:

1. Aprire il prompt dei comandi e accedere a <Engine>\BIN>.

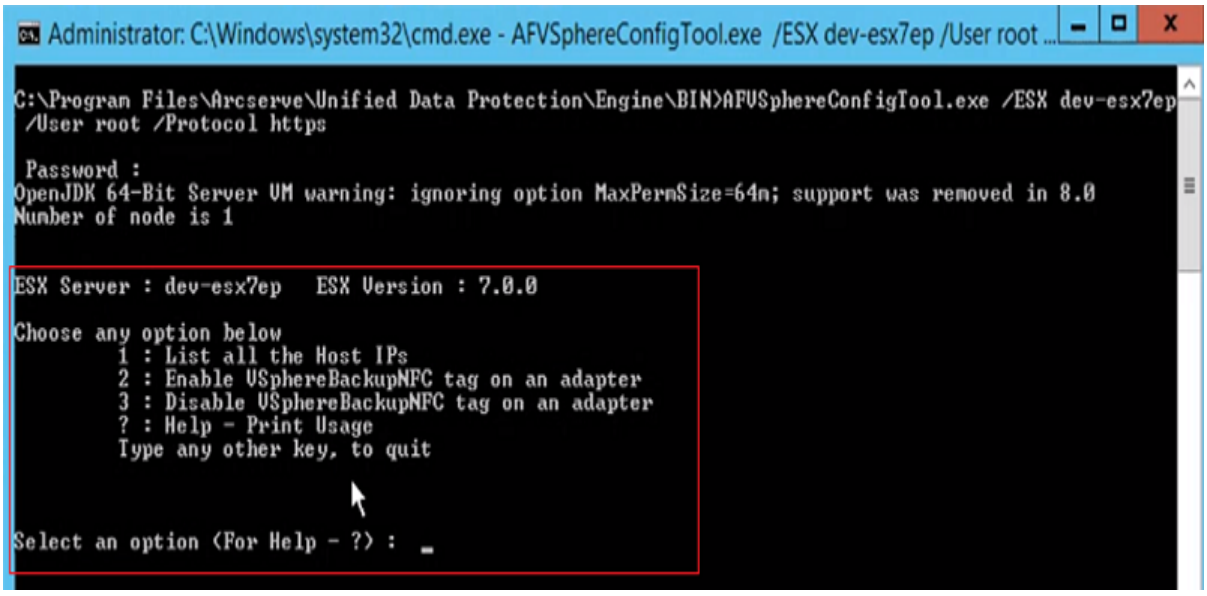
   Esempio: C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN>

2. Connettersi al server ESX utilizzando lo strumento della riga di comando (*AFVSphereConfieffetuatogTool.exe*), quindi digitare una password quando richiesto.

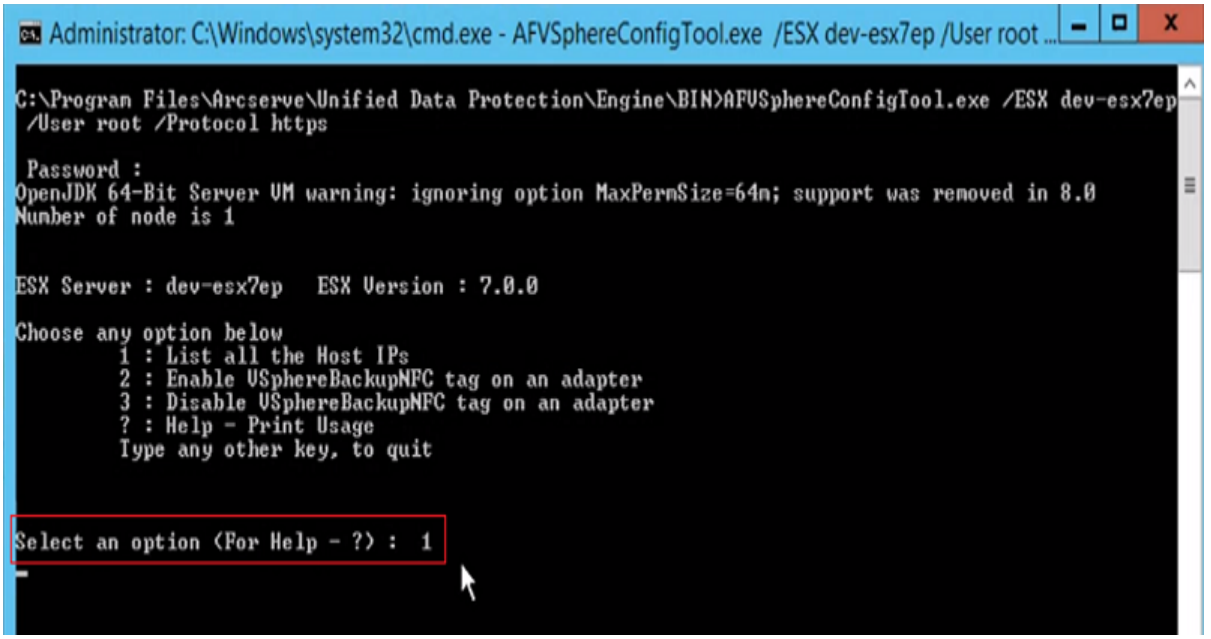
   AFVSphereConfigTool.exe /ESX dev-esx7ep /user root /protocol https

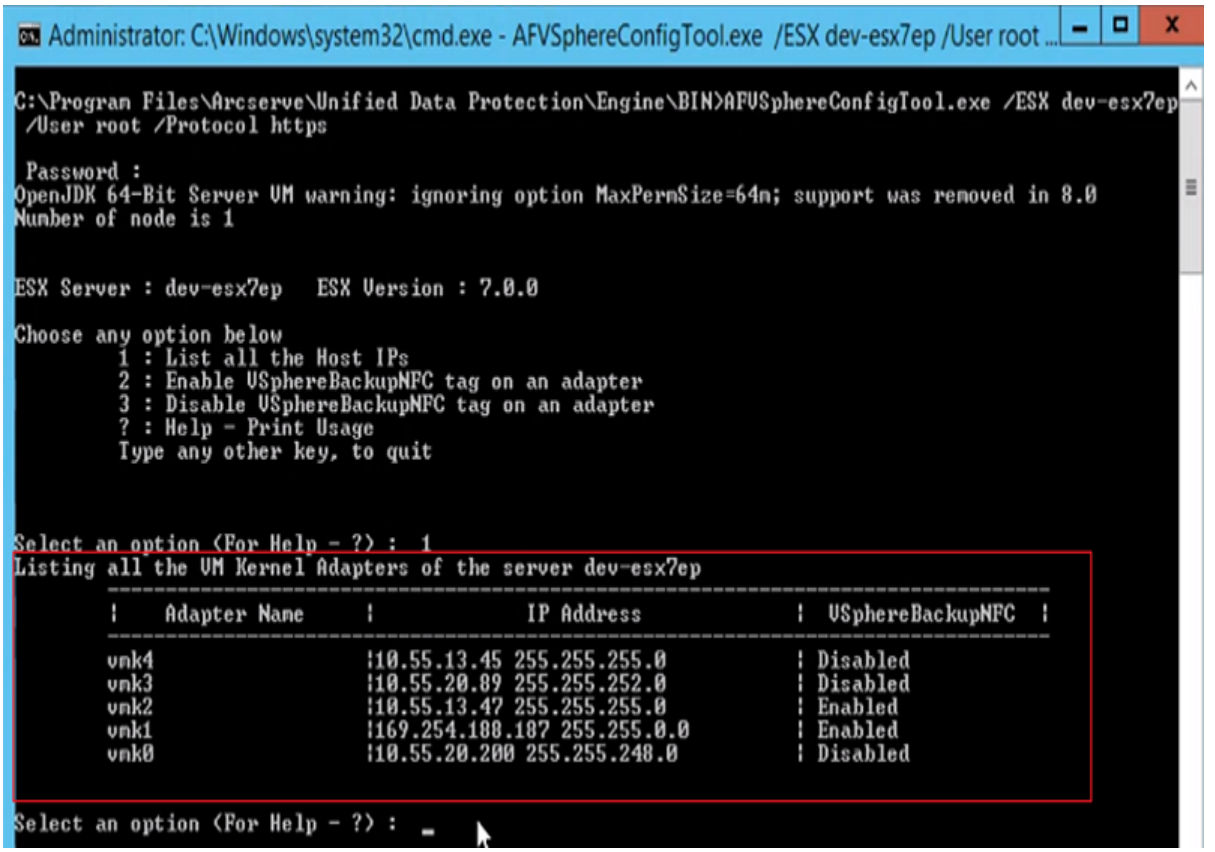
   Il server ESX selezionato (dev-esx7ep) è ora connesso.



3. Dopo aver effettuato la connessione al server ESX, quando viene richiesto di selezionare un'opzione, procedere come segue:
   - Per elencare tutte le schede del kernel del computer virtuale del server ESX, digitare il numero dell'opzione. Ad esempio, digitare 1 per l'opzione.

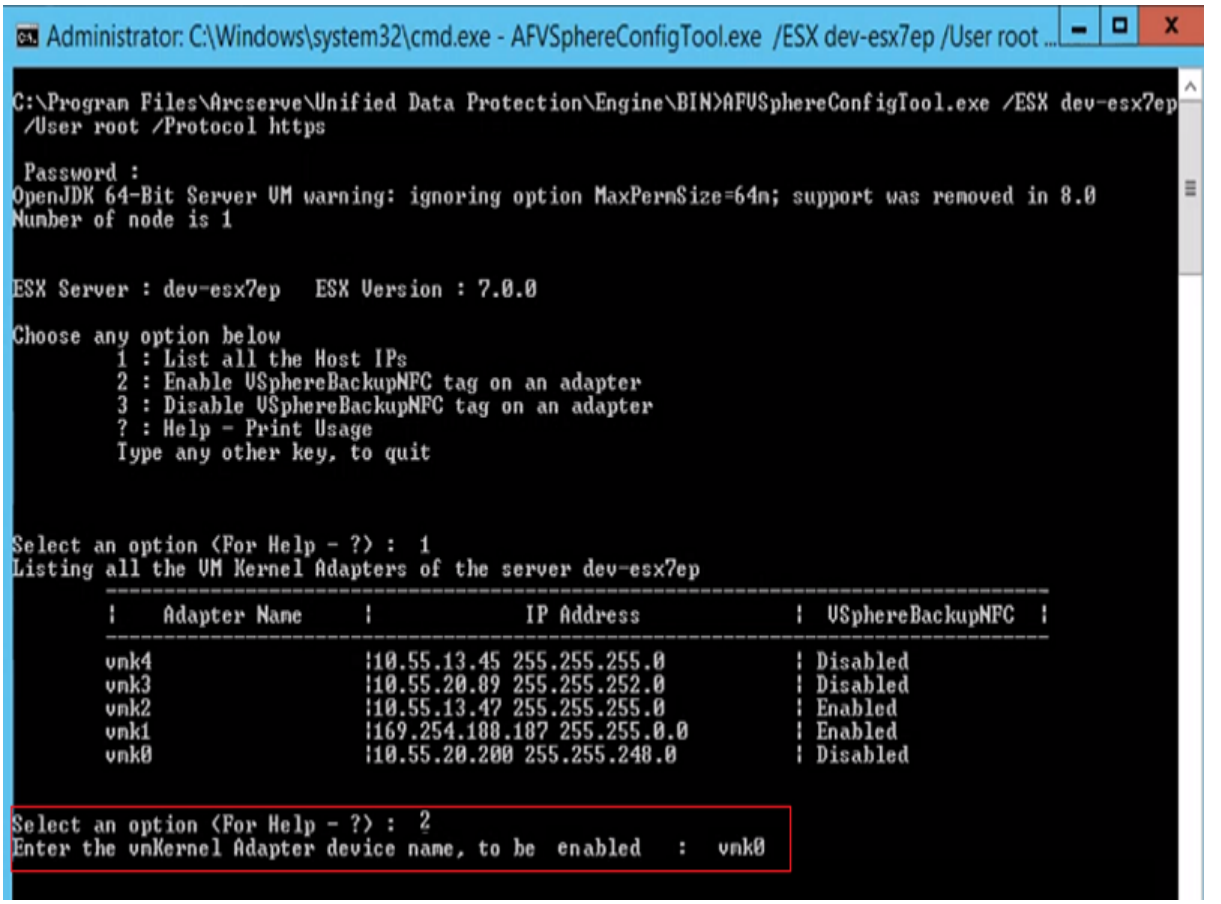


Viene visualizzato un elenco di tutte le schede del kernel del computer virtuale.

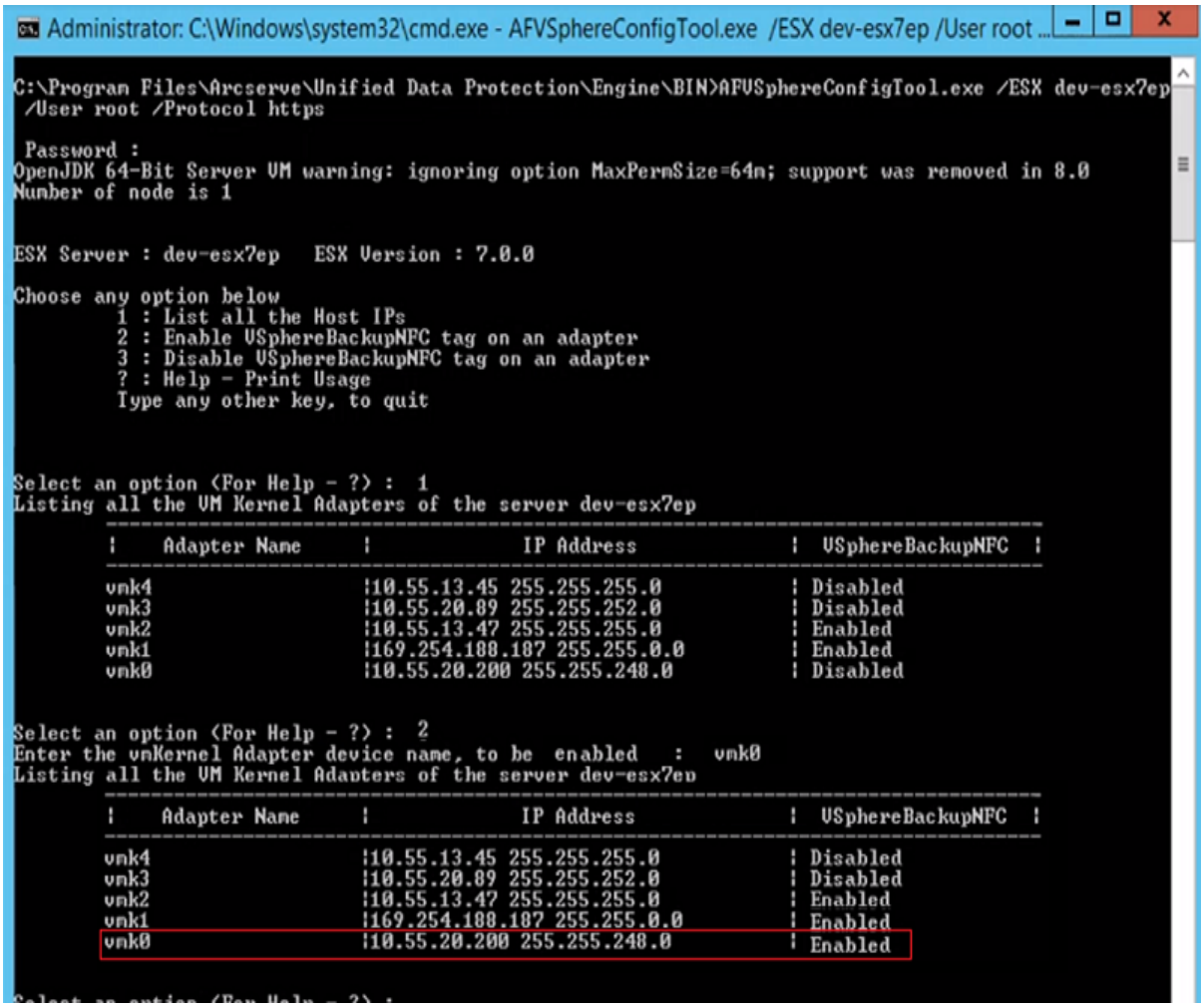


- Per abilitare il tag VSphereBackupNFC su una scheda, digitare il numero dell'opzione. Ad esempio, digitare 2 per l'opzione.

  Quando viene richiesto di immettere il nome del dispositivo della scheda del kernel del computer virtuale, digitare il nome del dispositivo.

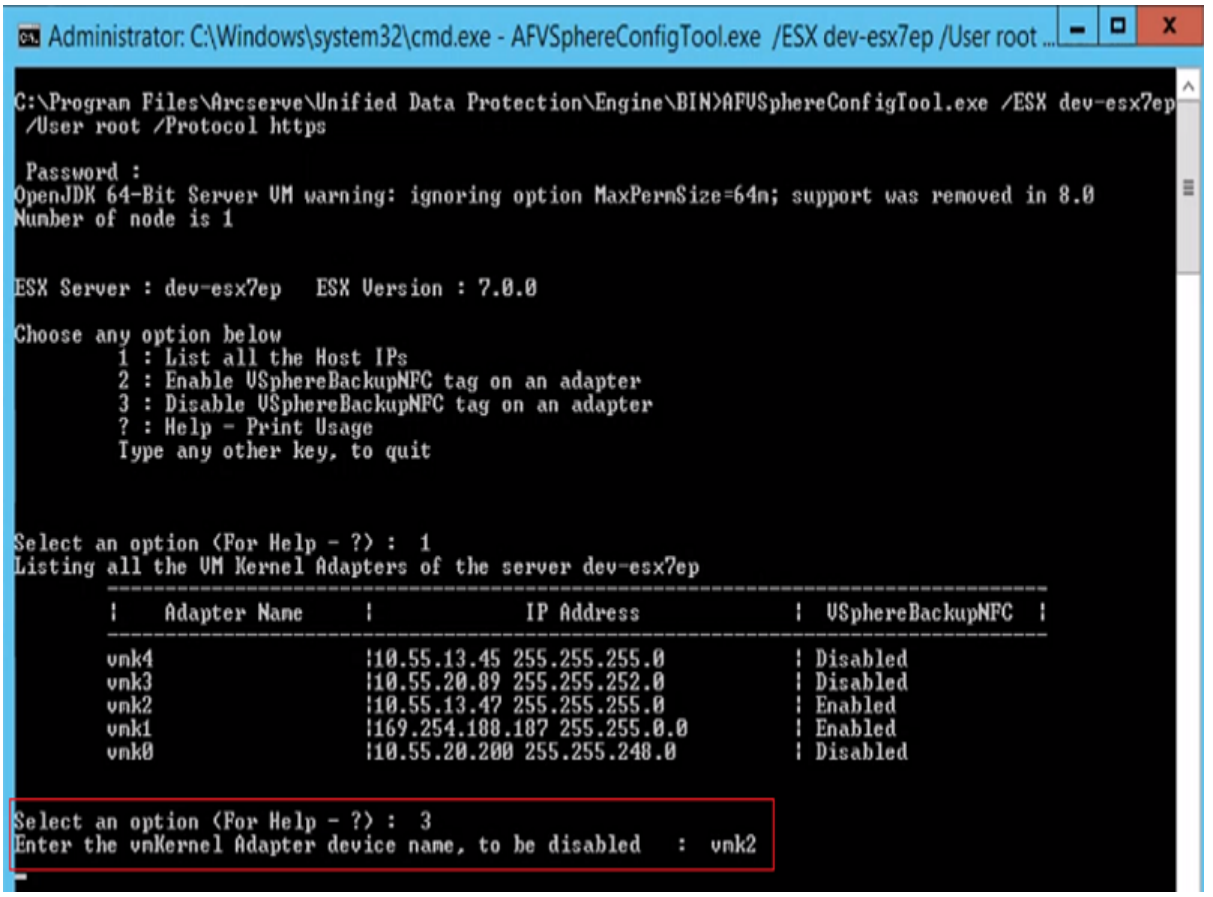


Il tag VSphereBackupNFC viene abilitato sulla scheda selezionata.

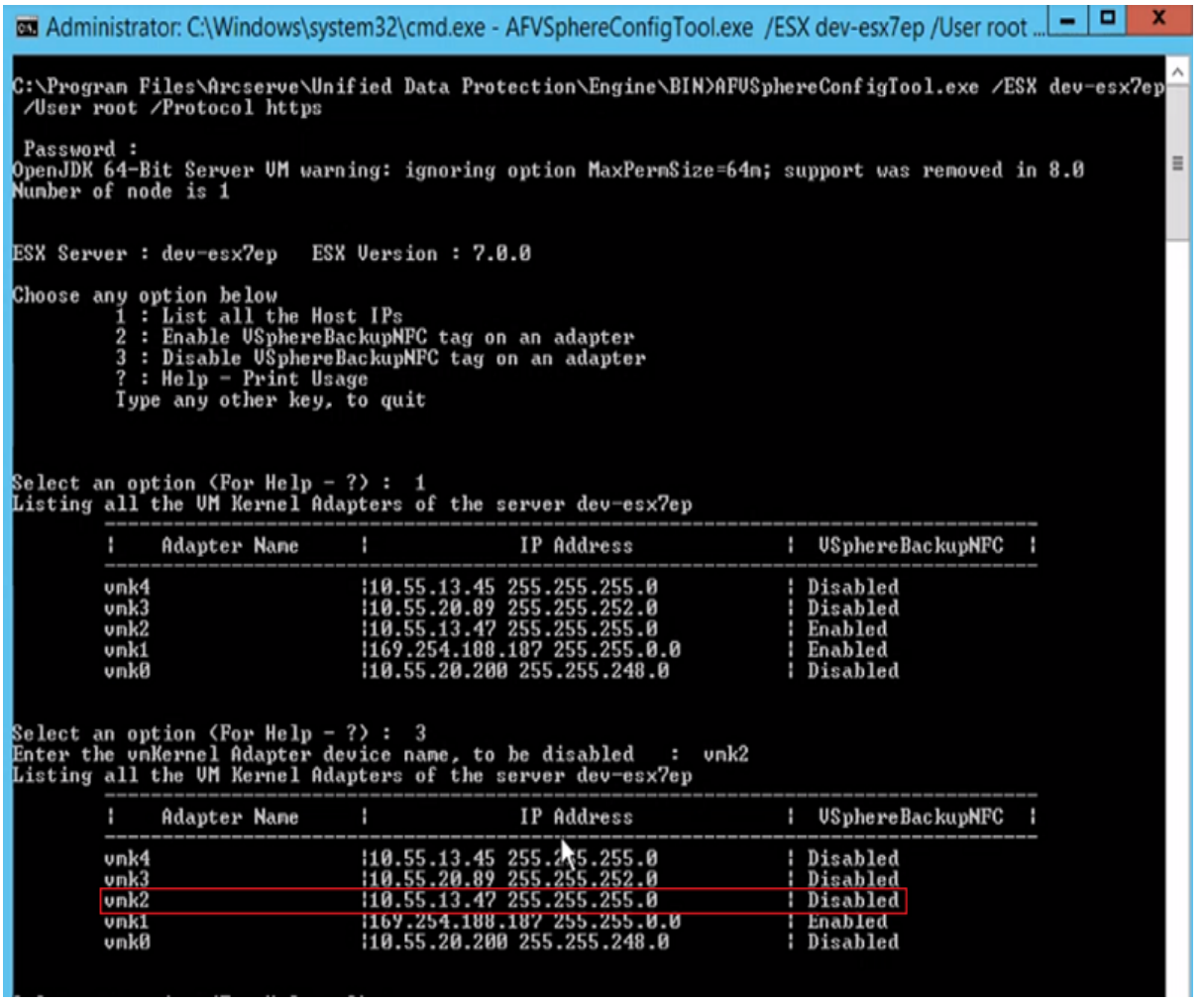


- Per disattivare il tag VSphereBackupNFC su una scheda, digitare il numero dell'opzione. Ad esempio, digitare 3 per l'opzione.

  Quando viene richiesto di immettere il nome del dispositivo della scheda del kernel del computer virtuale, digitare il nome del dispositivo.



Il tag VSphereBackupNFC viene disattivato sulla scheda selezionata.



4. Digitare una chiave qualsiasi (ad eccezione di 1, 2, 3 e?) per chiudere il prompt dei comandi.

Chapter 9: Utilizzo dell'utilità di diagnostica

L'utilità di diagnostica consente di raccogliere i registri dai computer. Quando si contatta il team del Supporto tecnico di Arcserve in merito a qualsiasi problema, il team si avvale dei registri per analizzare e correggere il problema in questione.

La presente sezione descrive i seguenti argomenti:

Raccolta di informazioni diagnostiche

Le informazioni diagnostiche sono una raccolta di registri, eventi, informazioni sull'applicazione relative al prodotto e al sistema richieste dal team del Supporto tecnico di Arcserve per individuare eventuali errori. Arcserve UDP consente di raccogliere tutte queste informazioni in una posizione, in genere un percorso di rete condiviso. Quando si contatta il Supporto tecnico di Arcserve, tenere queste informazioni a portata di mano. È possibile raccogliere i dati diagnostici per i computer Windows, Linux, VMware e Hyper-V.

Nota: Per i server di backup Linux, l'opzione **Collect Diagnostic Data** (Raccogli dati diagnostici) è disponibile solo dalla visualizzazione **Nodi di <Site_name>: Gruppi di server di backup Linux**.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Attenersi a una delle procedure seguenti a seconda del tipo di nodo:

   Per i server di backup Linux

   - Dal riquadro Navigazione a sinistra, accedere a **Nodi**, quindi fare clic su **Gruppi di server di backup Linux**.
   - Selezionare tutti i nodi Linux dal riquadro centrale.

   Per tutti gli altri nodi e server

   - Dal riquadro Navigazione a sinistra, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.
   - Selezionare tutti i nodi richiesti dal riquadro centrale.
3. Fare clic su **Azioni Collect Diagnostic Data (Raccogli dati diagnostici)**.

   Viene visualizzata la finestra di dialogo **Acquisisci informazioni diagnostiche**.
4. (Facoltativo) Selezionare la casella di controllo.
5. Fornire il percorso di rete condiviso per memorizzare i dati.

   Note:

   - Durante l'acquisizione delle informazioni diagnostiche relative a un sito remoto, è necessario specificare la destinazione come server gateway o qualsiasi altro computer in grado di accedere all'agente o al server RPS su quel determinato sito.

- Se si desidera specificare come destinazione il percorso locale, convertire quest'ultimo in percorso UNC e fornire il percorso UNC. Ad esempio, **C:\test** può essere specificato come **\\<LocalmachineName>\C$\test**.
- Per il backup senza agente basato su host (computer virtuali), l'opzione Collect Diagnostic Data (Raccogli dati diagnostici) raccoglie i dati dal server proxy di Arcserve UDP.
- L'opzione Collect Diagnostic Data (Raccogli dati diagnostici) raccoglie i dati dei computer su cui è installato l'agente Arcserve UDP.

6. Fare clic su **Invia**.

   Viene inviato un processo per la raccolta dei dati.

   Una volta completato il processo, i dati vengono visualizzati nella cartella condivisa. Il nome del file zip ha come suffisso l'indicatore di data/ora corrente.

Acquisizione delle informazioni diagnostiche da un agente standalone

Le informazioni diagnostiche sono una raccolta di registri, eventi, informazioni sull'applicazione relative al prodotto e al sistema che il team del Supporto tecnico di Arcserve richiede per individuare eventuali errori. L'agente Arcserve UDP consente di acquisire tutte le informazioni in una posizione, in genere un percorso di rete condiviso. Quando si contatta il Supporto tecnico di Arcserve, tenere a portata di mano queste informazioni disponibili.

Effettuare le operazioni seguenti:

1. Utilizzando il prompt dei comandi, accedere al percorso seguente:

   ```
   %Programmi% \Arcserve\Unified Data Protection\Engine\BIN\DiagnosticUtility
   ```

2. Immettere il comando seguente per informazioni sull'esecuzione del file batch:

   ```
   arcserveAgentSupport.bat -help
   usage: arcserveAgentSupport.bat [OPTIONS]
   -help print help
   -pass <arg> usrPass (se il percorso di esportazione è una condivisione remota, indica la password utente per accedervi)
   -path <arg> export path (può trattarsi di una condivisione remota)
   -user <arg> usrName (se il percorso di esportazione è una condivisione remota, indica il nome utente per accedervi)
   -xmlConfig <arg> xmlConfigurationFile (facoltativo)
   ```

3. Utilizzare il comando seguente per recuperare le informazioni diagnostiche:

   ```
   arcserveAgentSupport.bat -path <remote share path> -user <username> -pass <password>
   ```

   Esempio: arcserveAgentSupport.bat -path \\remote_share\data -user abc -pass xyz

   dove \\remote_share\data è il percorso, abc è il nome utente e xyz è la password

   È possibile trovare il file .zip delle informazioni diagnostiche nella condivisione remota.

Caricamento delle informazioni diagnostiche sul sito Web di Arcserve mediante FTP

È possibile caricare registri o file sul server FTP del Supporto tecnico di Arcserve mediante il protocollo di trasferimento file (FTP, File Transfer Protocol). Tuttavia, gli utenti (il richiedente del ticket) possono attivare il collegamento FTP durante il processo iniziale di creazione del ticket o durante l'aggiornamento del ticket in linea. Una volta attivato, il server FTP genera il collegamento FTP con le credenziali di accesso. Queste informazioni vengono fornite all'utente tramite un messaggio di posta elettronica automatico. Per caricare e scaricare i file dal server FTP, è possibile utilizzare il nome utente e la password inviati automaticamente tramite posta elettronica.

Quando si accede al server FTP tramite ftp://supportftp.arcserve.com, verrà visualizzata la cartella principale. Se si crea un ticket nel portale del Supporto tecnico di Arcserve, all'interno della cartella principale verrà creata una sottocartella con il numero di ticket. Ad esempio, se si crea un ticket con numero di ticket Ticket-00XXXX30, nella cartella principale viene creata una sottocartella denominata Ticket-00XXXX30.

ftp://supportftp.arcserve.com/Ticket-00XXXX30/

Nome utente e Password: utilizzare il nome utente e la password generati automaticamente inviati automaticamente tramite messaggi di posta elettronica.

Cartella: Ticket-00XXXX30

Nota: per gli utenti in lingua giapponese, la password corrisponde all'indirizzo di posta elettronica del richiedente senza il nome di dominio. Ad esempio, se l'indirizzo di posta elettronica registrato è abc@yahoo.jp, la password è abc.

In seguito alla risoluzione del ticket, il server FTP riceve una notifica. La cartella viene quindi compressa e la cartella originale viene eliminata. La cartella compressa è disponibile per i successivi tre mesi dopo i quali viene eliminata definitivamente.

Importante: Non condividere il nome utente con altri utenti.

Attenersi alla procedura seguente per caricare dei file sul sito Web di Arcserve tramite FTP:

1. Il richiedente del ticket (utente) o l'agente del Supporto tecnico di Arcserve accedono al Portale del Supporto tecnico di Arcserve e creano un ticket di supporto.

   L'agente del Supporto tecnico di Arcserve o il richiedente del ticket seleziona la casella di controllo nel ticket di supporto e aggiorna il ticket.

Viene generato automaticamente un collegamento FTP per la cartella principale. L'autorizzazione viene impostata esclusivamente per il richiedente che ha aperto il ticket.

Ad esempio, la cartella FTP è la cartella seguente:

ftp://supportftp.arcserve.com/<Ticket_number>

2. In seguito alla creazione del collegamento FTP, il Supporto tecnico di Arcserve invia automaticamente al richiedente del ticket (utente) un messaggio di posta elettronica contenente tale collegamento e le credenziali di accesso.
3. L'utente accede al collegamento FTP e carica i file.

   Il processo di caricamento dei file sul server FTP di Arcserve è stato completato correttamente.

Estrazione dei registri dell'agente

I file di registro generati dall'utilità di diagnostica sono inclusi in un formato .ZIP. Per visualizzare i file di registro, è necessario decomprimere i file.

Effettuare le operazioni seguenti:

1. Copiare il file .arcZIP nel computer in cui è stato installato l'agente UDP.

   Il file .arcZIP viene creato mediante l'utilità di diagnostica.

2. Utilizzando il prompt dei comandi, accedere al percorso seguente:

   ```
   %Programmi% \Arcserve\Unified Data Protection\Engine\BIN\DiagnosticUtility
   ```

3. Immettere il comando seguente per informazioni sull'esecuzione del file batch:

   ```
   arcserveAgentSupportInternal.bat -help
   BaseOperation loadDefaultValue
   INFORMAZIONI: Caricamento del percorso di installazione dell'agente C:\Programmi\Arcserve\Unified Data Protection\Engine
   usage: arcserveAgentSupportInternal.bat [OPTIONS] rawfile
   -help         Guida in linea per la stampa
   -keepFile     Mantieni file temporaneo
   -path <arg> percorso in cui è necessario decomprimere il contenuto
   ```

   Viene visualizzata la sezione Guida in linea.

4. Per decomprimere il file, utilizzare il comando seguente:

   ```
   arcserveAgentSupportInternal.bat -path <should_be_the_same_machine_where_you_want_to_unzip> <name_of_the_zip_file>
   ```

   I registri dell'agente vengono decompressi.

Estrazione dei registri della console

I file di registro generati dall'utilità di diagnostica sono inclusi in un formato .ZIP. Per visualizzare i file di registro, è necessario decomprimere i file.

Effettuare le operazioni seguenti:

1. Copiare il file .arcZIP nel computer di cui è installata la console UDP.

   Il file .arcZIP viene creato mediante l'utilità di diagnostica.

2. Utilizzando il prompt dei comandi, accedere al percorso seguente:

   ```
   %Programmi% \Arcserve\Unified Data Protection\Management\BIN\DiagnosticUtility
   ```

3. Immettere il comando seguente per informazioni sull'esecuzione del file batch:

   ```
   arcserveConsoleSupportInternal.bat -help
   BaseOperation loadDefaultValue
   INFORMAZIONI: Caricamento del percorso di installazione dell'agente C:\Programmi\Arcserve\Unified Data Protection\Management \
   usage: arcserveConsoleSupportInternal.bat [OPTIONS] rawfile
   -help              Guida in linea per la stampa
   -ignoreFailed      Ignora l'importazione non riuscita della tabella
   -keepFile          Mantieni file temporaneo
   -noClean           Non pulire il database
   -path <arg>        percorso in cui è necessario decomprimere il contenuto
   -u                 Decomprimere solo il file
   ```

   Viene visualizzata la sezione Guida in linea.

4. Per decomprimere il file, utilizzare il comando seguente:

   ```
   arcserveConsoleSupportInternal.bat -path <should_be_the_same_machine_where_you_want_to_unzip> <name_of_the_zip_file>
   ```

   Nota: Il comando non sovrascrive il database della console. Se si desidera sovrascrivere il database della console, modificare il comando *arcserveConsoleSupportInternal.bat* e rimuovere "*-u*" dal file, quindi salvare il file.

   I registri della console vengono decompressi.

Contenuti della cartella della cronologia dei registri ignorati tramite il Registro di sistema

È possibile utilizzare l'agente UDP per raccogliere tutti i registri, inclusa la cronologia, dal modulo. A volte, durante la raccolta della cronologia dei registri, l'agente UDP elabora i file in modo lento e le dimensioni del file aumentano. Per evitare queste discrepanze, è possibile escludere la cartella LogHistory.

Effettuare le operazioni seguenti:

1. Aggiungere la chiave del Registro di sistema nel seguente percorso:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

2. Immettere le seguenti informazioni:

   KeyName: *SkipLogHistory*

   type: *DWORD(32-bit)*

   Valore: 1 (il valore 1 consente di ignorare LogHistory, mentre 0 viene utilizzato per raccogliere LogHistory)

Raccolta di registri dal computer Gateway tramite la riga di comando

È necessario disporre del prodotto Arcserve UDP Gateway installato per raccogliere i registri dalla riga di comando.

Seguire questi passaggi per raccogliere i registri dalla riga di comando:

1. Aprire il prompt dei comandi e accedere a *<Gateway installation directory>\BIN\Diagnostic Utility*.

   Esempio: C:\Programmi\Arcserve\Unified Data Protection\Gateway\BIN\Diagnostic Utility\

2. Per comprimere i registri, eseguire il seguente comando:

   arcserveGatewaySupport.bat -Path "<Destination path>"

3. Per decomprimere i registri, eseguire il seguente comando:

   arcserveGatewayInternalSupport.bat -Path "<Destination path>" "<source path>"

Raccolta di registri dai server RPS mediante la riga di comando

Per raccogliere i registri RPS dalla riga di comando, il prodotto Arcserve UDP deve essere installato con il componente RPS.

Per raccogliere i registri dalla riga di comando procedere come segue:

1. Aprire il prompt dei comandi e accedere a *<Agent installation directory>\BIN\Diagnostic Utility*.

   Esempio: C:\Programmi\Arcserve\Unified Data ProtectionEngine\BIN\Diagnostic Utility\

2. Per comprimere i registri, eseguire il seguente comando:

   arcserveAgentSupport.bat -path <remote share path> -user <username> -pass <password>

3. Per decomprimere i registri, eseguire il seguente comando:

   arcserveAgentSupportInternal.bat –path <destination> <source(rawfile)>

Note:

- I registri RPS includono i registri dei processi che vengono eseguiti sui server RPS.
- I registri RPS possono essere recuperati solo dalla riga di comando e non dall'interfaccia utente della console.
- Alcuni registri RPS relativi ai processi non possono essere raccolti dall'interfaccia utente della console durante la raccolta di registri del computer virtuale dalla console.

Esempio: quando è configurata un'attività di replica MSP, le attività vengono configurate con due console, in cui Backup è l'attività principale di Console-1 e Replica è l'attività secondaria. In Console-2, l'attività di replica gestita da remoto viene configurata e condivisa con Console-1.

In questo scenario, in Console-2 non è possibile raccogliere i registri dei processi di replica durante la raccolta di registri del computer virtuale dalla console, ma è necessario raccogliere i registri di replica dalla riga di comando nel computer RPS impostato come destinazione del processo di replica.

Raccolta di registri Stub da Hyper-V con l'agente installato

È possibile raccogliere i registri Stub da Hyper-V in cui è installato l'agente. Hyper-V può fungere da proxy anche per la raccolta dei registri Stub Hyper-V.

Quando Hyper-V stesso funge da proxy (il computer Hyper-V deve avere installato l'agente)

Aprire il prompt dei comandi e accedere a *<Agent Installation Directory>\BIN\Diagnostic Utility*.

Esempio: *C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN\Diagnostic Utility*

- Per comprimere i registri: eseguire il comando *arcserveAgentSupport.bat -Path "Destination"*
- Per decomprimere i registri: eseguire il comando *ArcserveAgentInternalSupport.bat -Path "Destination" "source"*

Quando Hyper-V non funge da proxy (raccolta dell'intero host UDP basato sulla cartella di backup del computer virtuale)

Prerequisito: il computer deve disporre di Java.

Effettuare le operazioni seguenti:

1. Importare il Registro di sistema dal percorso sottostante sul computer in cui è installato l'agente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine.

2. Copiare l'intera cartella DiagnosticUtility da un computer in cui è già stato installato l'agente e incollare la cartella nel seguente percorso:

   C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN

   Nota: è necessario creare manualmente la struttura di directory.

3. Creare una cartella vuota denominata "Logs" nel percorso seguente:

   C:\Programmi\Arcserve\Unified Data Protection\Engine

4. Copiare la cartella comune da un computer in cui è già installato l'agente nel seguente percorso:

   C:\Programmi\Arcserve\Unified Data Protection

- Per comprimere i registri: eseguire il comando *arcserveAgentSupport.bat -Path "Destination"*
- Per decomprimere i registri: eseguire il comando *ArcserveAgentInternalSupport.bat -Path "Destination" "source"*

Raccolta dei messaggi dal Visualizzatore eventi Hyper-V

È possibile raccogliere i messaggi del Visualizzatore eventi da Hyper-V con l'agente installato con un nome di cartella *hyperVEventViewerFiles*.

Attenersi a questi passaggi per raccogliere i messaggi del Visualizzatore eventi dalla riga di comando:

1. Aprire il prompt dei comandi e accedere a *<Agent Installation Directory>\BIN\ Diagnostic Utility*.

   Esempio: C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN\Diagnostic Utility\

2. Per comprimere i messaggi del Visualizzatore eventi, eseguire *arcserveAgentSupport.bat -Path "Destination"*
3. Per decomprimere i messaggi del Visualizzatore eventi, eseguire *ArcserveAgentInternalSupport.bat -Path "Destination" "source"*

Raccolta della cartella Ca_lic e dei file OLF

La cartella CA_LIC e i file OLF vengono raccolti nei registri dal computer in cui è installato l'agente e la cui cartella è denominata CA_LIC.

- Per la raccolta tramite CLI: aprire il prompt dei comandi e accedere al percorso *<Agent Installation Directory>\BIN\ Diagnostic Utility*

  Esempio: *C:\Programmi (x86)\Arcserve\SharedComponents\CA_LIC*
- Per la raccolta mediante Console: accedere al nodo Agente, fare clic con il tasto destro del mouse e selezionare **Raccolta di informazioni diagnostiche**.
- Per comprimere i registri: eseguire il comando *arcserveAgentSupport.bat -Path "Destination"*
- Per decomprimere i registri: eseguire il comando *ArcserveAgentInternalSupport.bat -Path "Destination" "source"*

Raccolta degli elenchi di directory dalla destinazione di backup o dalle directory dell'archivio dati

Elenco di directory per le cartelle Modulo e Gestione

Modulo: il registro viene raccolto nella cartella *agentLogs* (dopo aver decompresso arczip) e viene denominato *EngineDirectoryBrowseInfo.log*.

Gestione: il registro viene raccolto in *consoleLogs* (dopo aver decompresso arczip) e viene denominato *ManagementDirectoryBrowseInfo.log*.

Elenco di directory per gli archivi dati:

- **Non di deduplicazione:** il registro viene raccolto per l'archivio dati non di deduplicazione e viene denominato *CommonStorePathDirectoryBrowseInfo.log* (dopo aver decompresso arczip) nella cartella *agentLogs*
- **Deduplicazione:** vengono raccolti quattro registri per gli archivi dati di deduplicazione (in seguito alla decompressione di arczip) nella cartella *agentLogs* con i seguenti nomi:
    1. *CommonStorePathDirectoryBrowseInfo.log*
    2. *HashRolePathDirectoryBrowseInfo.log*
    3. *IndexRolePathDirectoryBrowseInfo.log*
    4. *DataRolePathDirectoryBrowseInfo.log*

Chapter 10: Installazione manuale di Sophos Intercept X Advanced for Server su Arcserve UDP

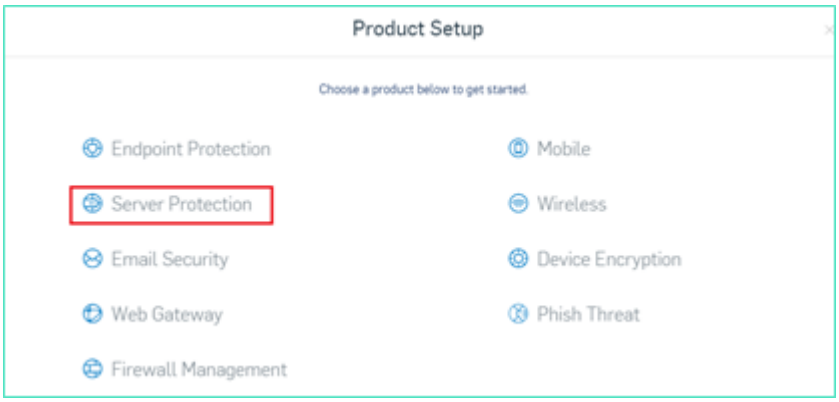
L'installazione di Sophos Intercept X Advanced for Server su Arcserve UDP consente di:

- Proteggere i dati e i backup di sistema da ransomware e altri attacchi
- Protezione degli endpoint che combina il rilevamento di malware basato sulla firma e senza firma.
- Rete neurale di deep learning
- Tecnologia antisfruttamento
- Le tecnologie anti-ransomware CyptoGuard e WipeGuard, per citarne alcune, sono in grado di gestire ogni tipo di minaccia endpoint

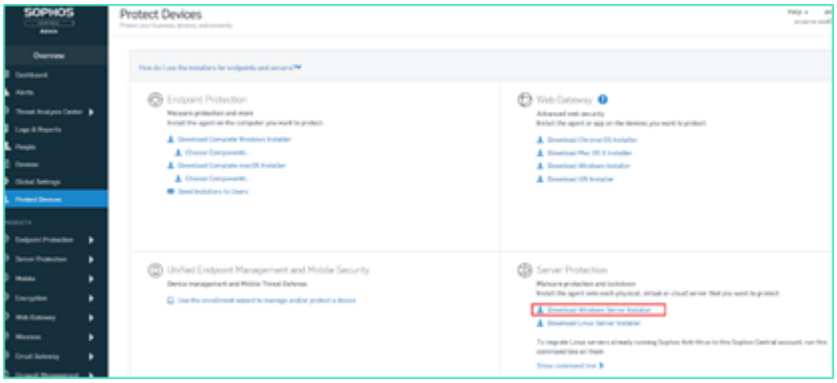
Effettuare le operazioni seguenti:

1. Creare un account nel sito Web del supporto Arcserve.
2. Per richiedere una copia gratuita di Sophos Intercept X Advanced, fornire tutti i dettagli rilevanti nel modulo di richiesta Sophos e inoltrarlo al Supporto tecnico di Arcserve. È obbligatorio condividere i dettagli dell'ID di posta elettronica e dell'ID dell'ordine. Verrà inviato un messaggio di posta elettronica autogenerato.

   Dopo aver confermato l'ID di posta elettronica, Arcserve elabora la richiesta e crea un account su Sophos Central. Invierà quindi un messaggio di posta elettronica contenente le istruzioni per la creazione di una password.
3. Per creare una password per il nuovo account su Sophos Central, seguire le istruzioni riportate nel messaggio di posta.
4. Accedere a Sophos Central.
5. Aprire la finestra di dialogo Configurazione prodotto, quindi selezionare **Protezione server**.



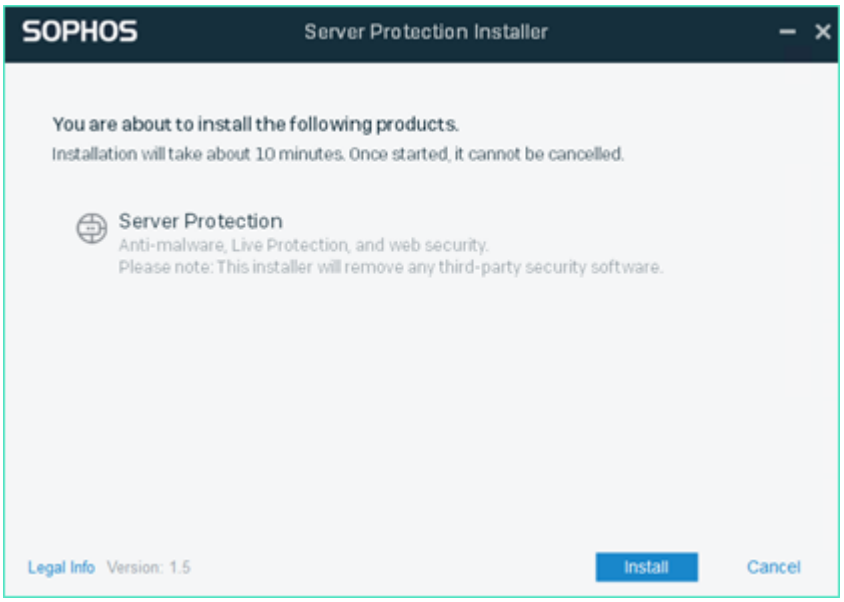
6. Nella sezione Protezione server, fare clic su **Scarica programma di installazione Windows Server**, quindi salvare il programma di installazione **SophosSetup.exe** in una cartella UDP.



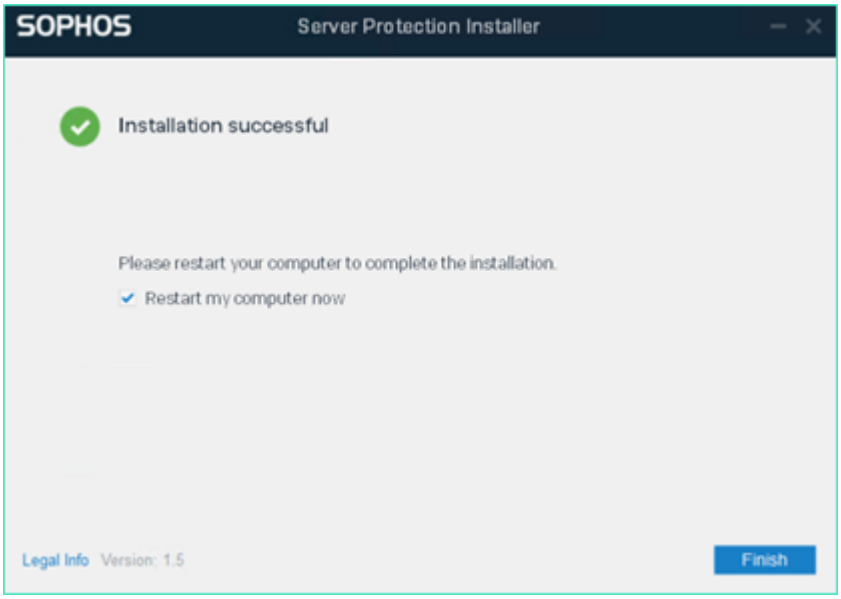
7. Per avviare il programma di installazione, aprire la cartella e fare doppio clic su **SophosSetup.exe**.

   Nota: per evitare comportamenti imprevisti durante l'installazione di Sophos Intercept-X, disattivare Windows Defender e\o altri software antivirus dal server. Sophos rimuoverà alcuni prodotti di protezione non Sophos dai server Windows. Per ulteriori informazioni, consultare la sezione Sophos CRT: Elenco di software di protezione di terze parti rimossi da Sophos.

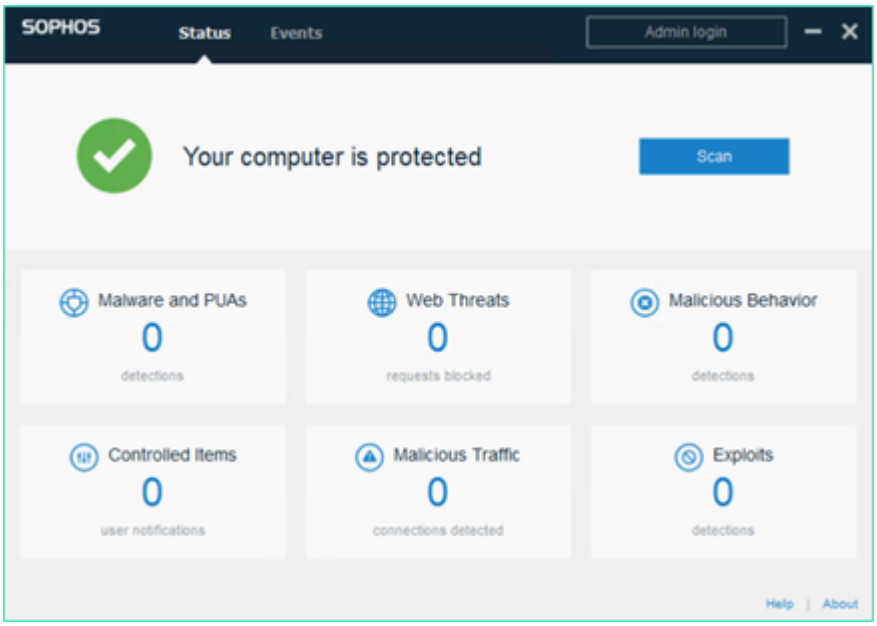
8. Fare clic su **Installa**.



9. Per riavviare immediatamente il sistema, fare clic su **Fine**. Per effettuare il riavvio in un secondo momento, deselezionare l'opzione **Riavviare adesso**.



10. Per visualizzare lo stato di protezione, aprire l'interfaccia **Sophos Intercept X**.



Lo stato indica che Arcserve UDP 8.0 è protetto da attacchi ransomware, malware, minacce Web ed exploit zero-day.

11. Per accedere a Sophos Central, fare clic su **Accesso amministratore**. L'operazione consente di gestire Sophos Intercept X Advanced Server, impostare avvisi e criteri e così via.

    Note:

    - È necessario disporre dell'accesso a Internet in Arcserve UDP per l'installazione di *Sophos Interceptor X Advanced* e di qualsiasi altro aggiornamento correlato. Sophos Interceptor X Advanced è basato su cloud e non è disponibile alcun programma di installazione non in linea.
    - Se in passato è già stata acquistata un'altra versione di UDP e si dispone di un account Sophos mediante Arcserve, utilizzare lo stesso account di Arcserve UDP 8.0.
    - Se si dispone già di un account Sophos mediante qualsiasi altra forma di acquisto, come ad esempio direttamente da Sophos, specificare un altro indirizzo di posta elettronica per ottenere un nuovo account Sophos Central.
    - Se l'installazione di Sophos non riesce, seguire le istruzioni visualizzate sullo schermo o nella posta elettronica fornite insieme al messaggio di errore.
    - Per ricevere gli aggiornamenti di Sophos Intercept X Advanced for Server, come ad esempio gli aggiornamenti delle definizioni di malware e

gli aggiornamenti delle versioni, è necessario disporre di una manutenzione o di una sottoscrizione valida e attiva per Arcserve UDP.

Per ulteriore assistenza, contattare il Supporto tecnico di Arcserve al numero di telefono (800148275) o online, oppure contattare l'ufficio di Supporto tecnico Arcserve locale.

Chapter 11: Procedura consigliata

La presente sezione descrive i seguenti argomenti:

Procedure consigliate per la protezione del server Arcserve UDP

È possibile eseguire la migrazione della console da un server all'altro senza alcuna perdita di dati.

- La soluzione di backup non dovrà essere contenuta nello stesso dominio Active Directory.
- Utilizzare gli account di backup.
- Non utilizzare gli account di amministrazione del dominio per accedere alle attività associate all'utente. Ad esempio, l'amministratore che utilizza i privilegi di amministratore per la lettura dei messaggi di posta elettronica, per la navigazione in linea, e così via.
- Separare la Console UDP dal Recovery Point Server e creare VSB per la Console UDP.
- Se possibile, utilizzare una rete o una vlan di backup dedicata.
- Se possibile, disattivare SMBv1.

  Nota: non è possibile disabilitare l'operazione se si utilizzano Red Hat/Centos v6.6 e versioni precedenti, poiché utilizzano SMB v1.

Esclusione di file dalla scansione antivirus

Il software antivirus può interferire con la corretta esecuzione del processo di standby virtuale bloccando temporaneamente l'accesso ai file o mettendo in quarantena o eliminando i file classificati erroneamente come sospetti o pericolosi. È possibile configurare la maggior parte dei software antivirus in modo da escludere cartelle o file specifici, per evitare di analizzare tali dati. La corretta configurazione del software antivirus è fondamentale per evitare che interferisca con le operazioni di backup e ripristino o con qualsiasi altro processo.

In un server Hyper-V, il software antivirus corrompe il file di configurazione del computer virtuale. Il server Hyper-V modifica lo stato del computer virtuale alla modalità di salvataggio e il computer virtuale diviene corrotto e non può più essere utilizzato. In tali casi, sarà necessario eliminare il computer virtuale ed eseguire una conversione completa per creare un nuovo computer virtuale.

Per fare in modo che il computer virtuale locale e remoto Virtual Standby funzioni normalmente e per evitare che il computer virtuale entri nella modalità di salvataggio, escludere i seguenti file dai computer virtuali Hyper-V di destinazione:

- Directory dei file di configurazione del computer virtuale:

  (Valore predefinito) C:\Programmi\Microsoft\Windows\Hyper-V

  Directory del file di configurazione del computer virtuale Virtual Standby di Arcserve UDP

- Directory dei file del disco rigido del computer virtuale:

  (Valore predefinito) C:\Utenti\Pubblica\Documenti pubblici\Hyper-V\Virtual Hard Disks

  Directory dei file di disco rigido del computer virtuale Virtual Standby di Arcserve UDP

- Directory di file di snapshot:

  (Valore predefinito) %systemdrive%\ProgramData\Microsoft\Windows\Hyper-V\Snapshots

  Directory del file delle snapshot del computer virtuale Virtual Standby di Arcserve UDP

Configurazione dei parametri di multistreaming

Le impostazioni relative alla replica su WAN vengono salvate nella chiave di registro seguente:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\Network]

Il seguente elenco mostra le chiavi di registro e i valori predefiniti corrispondenti:

- "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)

Le impostazioni della chiave di registro sono descritte di seguito:

WAN_EnableAutoTunning

Specifica l'opzione per attivare o disattivare il multistreaming. Se il valore corrisponde a 0, il multistreaming è disattivato. Per gli altri valori, il multistreaming è attivato. Il valore predefinito per l'attivazione del multistreaming è 1.

WAN_ChunkSizeByte

Specifica le dimensioni del blocco per ciascun pacchetto. La dimensione del pacchetto influisce sulla velocità effettiva. Se la larghezza di banda della WAN è superiore, le dimensioni del blocco di dati possono essere ulteriormente aumentate.

Il valore predefinito è 64 KB. L'intervallo è compreso tra 512 byte e 1 MB in codice.

WAN_NumberofStreams

Specifica il numero di flussi da creare sulla WAN se la latenza è superiore al valore di WAN_RTT_Threshhold. Il numero di flussi predefinito è 5. L'intervallo di flussi varia da 1 a 10.

WAN_RTT_Threshold

Se il valore di RTT è superiore a WAN_RTT_Threshold, verranno creati più socket. L'unità di WAN_RTT_Threshold è il millisecondo (ms). Il valore predefinito è 20 millisecondi. L'intervallo è compreso tra 20 ms e 600 ms.

WAN_MultiStreamsMaxCacheSize

Specifica la dimensione della memoria allocata all'attivazione del multistreaming. Questo buffer di memoria verrà utilizzato per il caching della memoria frammentata ricevuta. L'intervallo è compreso tra 16 MB e 64 MB. Il valore predefinito è 64 MB. Se il valore è zero, il valore verrà impostato su 64 MB. Questo valore è espresso in BYTE.

WAN_SendCommandFragDataMerged

Specifica che, se il valore è diverso da zero, la libreria di comunicazione raggruppa i file di piccole dimensioni e li invia in un singolo blocco. Se il valore è zero, i file di piccole dimensioni vengono inviati singolarmente. Il valore predefinito è zero.

Note:

- In un processo di replica, il numero di connessione socket potrebbe non corrispondere al Registro di sistema WAN_NumberofStreams.

  Processo di replica da non GDD a non GDD

  Se il valore di RTT è superiore a WAN_RTT_Threshold, il numero di connessione socket corrisponde a WAN_NumberofStreams.

  Processo di replica da non GDD a GDD o GDD a GDD

  Sono presenti quattro tipi di connessione. La connessione basata sui blocchi di dati può essere utilizzata solamente con la funzionalità multistreaming. Pertanto, se il valore di RTT è superiore a WAN_RTT_ Threshold, la connessione dei socket totali corrisponde a 3+WAN_NumberofStreams.

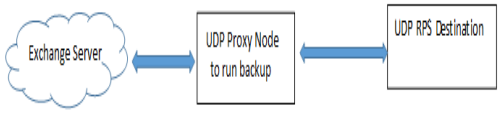
- Il processo di replica rileva lo stato della rete per determinare se la comunicazione è WAN o Non WAN. Se lo stato della rete è debole, è possibile accettare la LAN come WAN.

Problemi correlati a Exchange Online

La presente sezione descrive i seguenti argomenti:

Configurazione per prestazioni ottimali

Topologia possibile:



Il proxy può essere installato sul server RPS o separatamente. Tuttavia, per ottenere prestazioni ottimali, si consiglia di avere entrambi sullo stesso nodo.

Configurazione consigliata per il proxy

- Architettura: computer Windows a 64 bit. Per ulteriori informazioni sui sistemi operativi supportati per Arcserve UDP, fare clic qui.
- Memoria: 8 GB o superiore
- CPU: 2 core

Configurazione consigliata per il Recovery Point Server:

Consultare le Note di rilascio per conoscere i requisiti di sistema.

Procedure consigliate per il backup

- Attendersi una durata più lunga per il primo backup completo con i dati acquisiti dal server Microsoft Exchange Online tramite un collegamento WAN.
- Considerata la durata prolungata del primo backup completo, applicare le configurazioni richieste per la disponibilità di hardware, rete e risorse (ad esempio, spazio su disco nella destinazione, memoria, CPU e così via) durante il backup per evitare interruzioni dovute a problemi dell'ambiente.
- Riprendere il backup dal punto di interruzione durante uno dei seguenti scenari:
  - Assicurarsi che un backup non sia in esecuzione durante un'interruzione pianificata o un periodo di inattività della rete. Se in esecuzione, è necessario annullare il backup. Quando si annulla, il backup mantiene parzialmente il punto di ripristino di cui è stato eseguito il backup e la pianificazione del backup successivo può riprendere dal punto di interruzione.
  - Se durante il backup la macchina incontra un arresto imprevisto o una terminazione del processo, il punto di ripristino del lavoro in corso viene rimosso. Riavviare il backup. Il backup non verrà avviato dal punto di interruzione. Tutti i dati vengono salvati di nuovo.
- È sempre consigliabile utilizzare un nodo con il meccanismo di protezione automatica per proteggere tutte le caselle postali, incluse quelle create subito dopo la creazione del piano.
- In Arcserve UDP, la dimensione supportata dei dati protetti è limitata a 8 TB (compressi) per impostazione predefinita. Per configurare la dimensione, è possibile creare il seguente valore del Registro di sistema sul nodo proxy:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<NodeGUID>]

  " VirtualDiskSize "=dword:00000002

  Nell'esempio la dimensione viene impostata su 2 TB.

  Nota: l'aumento delle dimensioni del disco virtuale converte il processo di backup incrementale successivo in backup completo e influisce sulla velocità dei seguenti processi:

  Copia su nastro, Replica, Copia punto di ripristino su cloud.
- Selezionare la dimensione del disco virtuale in base alle dimensioni dei dati di origine correnti e alla relativa crescita.

Ad esempio, se la dimensione totale di tutti gli utenti è pari a 5 TB e la crescita media dei dati al giorno è dell'1%, ossia 50 GB, è necessario disporre di 5 TB + 50 GB * 30 giorni = 6.5 TB di spazio su disco per contenere il primo backup completo e i 30 backup incrementali giornalieri per un mese.

Di conseguenza, la dimensione minima richiesta per il disco sarà di 7 TB (non compressi). Per mantenere più punti di recupero, utilizzare lo stesso metodo per calcolare le dimensioni.

- Utilizzare correttamente le pianificazioni di limite delle risorse affinché il backup disponga della larghezza di banda desiderata durante gli orari non di ufficio. Eseguire un backup di piccole dimensioni con pochi utenti per valutare l'utilizzo della rete per processo di backup e impostare di conseguenza i valori di limite delle risorse.
- Verificare che l'account di backup soddisfi i requisiti obbligatori. Per ulteriori informazioni, consultare il seguente collegamento.
- Se il collegamento di rete utilizzato per connettersi al server di Exchange Online è instabile e caratterizzato da frequenti annullamenti dei backup, configurare il criterio Conservazione punto di ripristino per memorizzare un numero elevato di sessioni non unite.

  Valore predefinito per i backup incrementali giornalieri: 7

  Valore predefinito per i backup manuali: 31

  Configurare le pianificazioni di backup in modo da conservare almeno un backup giornaliero, uno settimanale e uno mensile.
- Verificare che l'installazione disponga delle licenze necessarie. È possibile gestire le licenze utilizzando Gestione licenze. Per ulteriori informazioni, consultare la domanda 4 nella sezione Domande frequenti.

Procedura consigliata per il ripristino

Verificare che l'account utilizzato per il ripristino disponga delle autorizzazioni richieste per rappresentare l'utente di destinazione selezionato. Per ulteriori informazioni, consultare il seguente collegamento.

Domande frequenti su Exchange Online

1. È possibile utilizzare direttamente il server RPS per il backup degli utenti di Exchange Online senza ricorrere a un proxy?

   Sì, è possibile.

2. È necessario un account di tipo amministratore/amministratore di gruppo per il backup delle caselle di posta di Exchange Online?

   No, l'account di backup richiede soltanto un insieme specifico di autorizzazioni. Per ulteriori informazioni, consultare il seguente collegamento.

3. Qual è la velocità effettiva prevista per i backup di Exchange Online con una buona larghezza di banda Internet?

   Oltre che dalla larghezza di banda della rete, la velocità effettiva è limitata dalla frequenza con cui i dati vengono letti dal server di Exchange, che dipende dalla progettazione di quest'ultimo.

   A volte, il server di Exchange rifiuta la connessione ad Arcserve UDP per leggere i dati. In tali casi, Arcserve UDP continua a eseguire dei tentativi fino a quando non viene stabilita la connessione. Il tempo di attesa prolungato può comportare una velocità effettiva inferiore.

4. Se sono presenti più utenti configurati nel piano di backup rispetto al numero di licenze, è possibile eseguire backup parziali degli utenti con licenza?

   No, non è possibile. Se si esegue il backup per un numero di utenti maggiore rispetto alle licenze disponibili, il backup non verrà eseguito per nessun utente. Ad esempio, se sono stati configurati 100 utenti da proteggere nella console Arcserve UDP mentre sono disponibili 90 licenze, il backup non verrà eseguito. Per la corretta esecuzione del backup, rimuovere 10 o più utenti dall'elenco degli utenti protetti.

5. Come è possibile migliorare le prestazioni di velocità effettiva del backup?

   Per garantire una velocità effettiva ottimale, considerare i seguenti punti:

   - Dividere un backup di grandi dimensioni in processi gestibili più piccoli.
   - Escludere dalle impostazioni del piano le cartelle da non sottoporre a backup. Ad esempio, Messaggi secondari, Problemi di sincronizzazione e così via.
   - Eseguire un controllo periodico dell'infrastruttura di rete interna ed esterna.

Problemi correlati a Microsoft Azure

La presente sezione descrive i seguenti argomenti:

Procedure consigliate per un computer virtuale istantaneo su Microsoft Azure

Per proteggere i nodi in una rete on-premise, è necessario installare la Console UDP sull'host.

- Selezionare HTTPS come protocollo durante l'installazione dei componenti UDP.
- Per creare un gruppo di risorse in modo semplice si consiglia di creare almeno un ambiente di test del computer virtuale. Azure guiderà l'utente attraverso le operazioni di creazione di tutte le risorse per il test del computer virtuale utilizzabile per il computer di standby virtuale.
- (Facoltativo) Creazione di un server RPS in Azure.

  Effettuare le operazioni seguenti:

  1. Aprire le porte TCP 8014 e 8015 in entrata.
  2. Per accedere al server RPS da un browser Web remoto, risolvere il nome del server RPS sull'indirizzo IP pubblico.
  3. Utilizzare l'attività del piano condiviso Replica su server RPS gestito in remoto per effettuare la replica.

Distribuzione di Arcserve UDP su Microsoft Azure

Rivedere le seguenti procedure consigliate prima di distribuire Arcserve UDP in Microsoft Azure:

1. È necessario installare la Console Arcserve UDP per proteggere i nodi contenuti nella rete on premise.
2. Selezionare il protocollo HTTPS durante l'installazione dei componenti Arcserve UDP.
3. La maniera più semplice di creare risorse Azure consiste nella creazione di almeno un computer virtuale di test utilizzabile come computer virtuale di standby in un secondo momento.

4. Creare il Recovery Point Server Arcserve UDP in Azure.
    - Mantenere le porte TCP 8014 e 8015 aperte per le connessioni in entrata.
    - Se si accede a un Recovery Point Server da un browser Web remoto, è necessario risolvere il nome del Recovery Point Server sull'indirizzo IP pubblico.
    - Utilizzare l'attività del piano condiviso **Replica su server RPS gestito in remoto** per effettuare la replica delle attività.

Chapter 12: Risoluzione dei problemi

La presente sezione descrive i seguenti argomenti:

Problemi di comunicazione relativi ad Arcserve UDP

In questa sezione verranno illustrati i seguenti argomenti sulla risoluzione dei problemi relativi ad Arcserve UDP:

- Errore di comunicazione tra Arcserve UDP e i nodi Windows
- Impossibile ricevere gli avvisi di posta elettronica da account di Gmail
- Errore di comunicazione di Arcserve UDP con il server di backup di Linux di Arcserve UDP sui nodi remoti
- Errore di comunicazione di Arcserve UDP con il Recovery Point Server di Arcserve UDP sui nodi remoti
- Errore di comunicazione di Arcserve UDP con il server di backup di Arcserve sui nodi remoti
- Errore di comunicazione di Arcserve UDP con il sito remoto

Errore di comunicazione tra Arcserve UDP e i nodi Windows

Valido per i sistemi operativi Windows.

Sintomo

Errore di comunicazione tra Arcserve UDP e i nodi Windows.

Soluzione

La tabella seguente descrive i motivi per cui Arcserve UDP non è in grado di comunicare con i nodi Windows e l'azione correttiva corrispondente:

Causa	Misura correttiva
La rete non era disponibile o stabile durante l'applicazione dei piani.	Verificare che la rete sia disponibile e stabile e riprovare. Arcserve UDP può eseguire il ping del nodo remoto e il nodo remoto può eseguire a sua volta il ping di Arcserve UDP.
La condivisione di rete Admin$ del nodo remoto non era disponibile mentre Arcserve UDP tentava di stabilire una comunicazione con il nodo.	Verificare che l'Admin$ di rete del nodo remoto sia disponibile e riprovare.
Il nodo Agente Arcserve Unified Data Protection per Windows non è stato in grado di gestire il carico mentre Arcserve UDP tentava di stabilire la comunicazione con il nodo.	Verificare che lo stato della CPU sul nodo dell'Agente Arcserve Unified Data Protection per Windows remoto si normalizzi e riprovare.
Il servizio dell'Agente Arcserve Unified Data Protection per Windows sul nodo remoto non era in esecuzione mentre Arcserve UDP tentava di stabilire la comunicazione con il nodo.	Verificare che il servizio dell'Agente Arcserve Unified Data Protection per Windows sia in esecuzione sul nodo remoto e riprovare.
Per la comunicazione con il nodo è stato utilizzato un protocollo errato o una porta errata.	Utilizzare la porta o il protocollo corretto per aggiungere/aggiornare il nodo remoto nella visualizzazione del nodo di Arcserve UDP.
Il servizio dell'Agente Arcserve Unified Data Protection per Windows non è in grado di stabilire la comunicazione in modo adeguato.	Riavviare il servizio dell'Agente Arcserve Unified Data Protection per Windows sul nodo remoto e riprovare.

Impossibile ricevere gli avvisi di posta elettronica da account di Gmail

L'account di Gmail viene bloccato da Google se utilizzato nelle impostazioni di posta elettronica.

Valido per piattaforme Windows.

Sintomo

Quando si configurano gli account di Gmail, non si ricevono gli avvisi di posta elettronica. Quando si tenta di configurare l'account di Gmail per gli avvisi di posta elettronica e di fare clic su Invia messaggio di posta elettronica di test, viene visualizzato uno dei seguenti messaggi di errore:

Errore del messaggio di posta elettronica di verifica: credenziali utente non corrette.

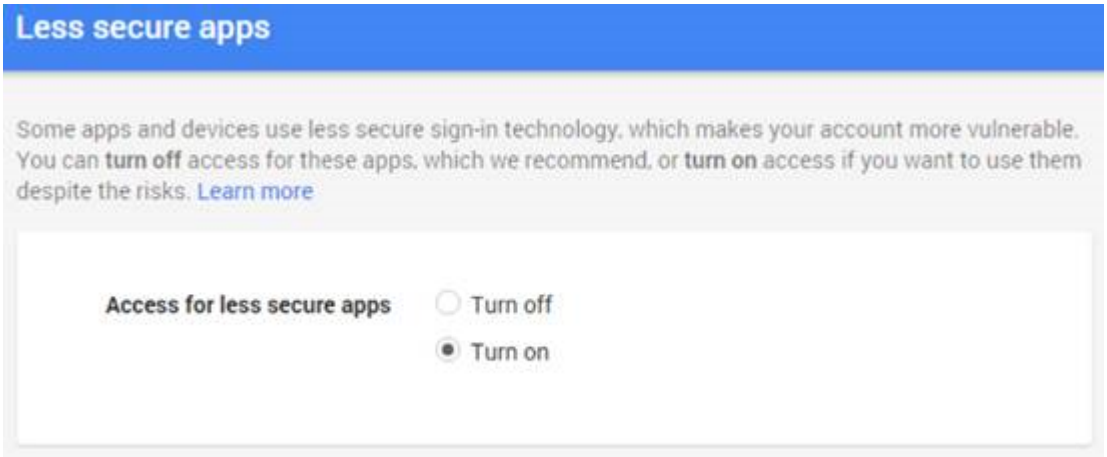
oppure

Impossibile inviare il messaggio di posta elettronica di verifica: Credenziali utente non valide.

Soluzione

1. Specificare le credenziali corrette e riprovare.
2. La protezione di Google blocca i messaggi di posta elettronica da un account di Gmail configurato all'esterno. Per evitare questo problema, nel collegamento seguente, modificare le impostazioni facendo clic su Attivare per utilizzare Access per le applicazioni meno sicure:

   https://www.google.com/settings/security/lesssecureapps



Errore di comunicazione di Arcserve UDP con il server di backup di Linux di Arcserve UDP sui nodi remoti

Valido per i sistemi operativi Linux.

Sintomo

Errore di comunicazione di Arcserve UDP con il server di backup di Linux di Arcserve UDP sui nodi remoti.

Soluzione

La tabella riportata di seguito descrive i motivi per cui Arcserve UDP non è in grado di comunicare con il server di backup di Linux Arcserve UDP sui nodi remoti e l'azione correttiva corrispondente:

Causa	Misura correttiva
La rete non era disponibile o stabile mentre Arcserve UDP tentava di stabilire una comunicazione con il nodo del server di backup di Linux.	Verificare che la rete sia disponibile e stabile e riprovare. Arcserve UDP può eseguire il ping del nodo del server di backup di Linux remoto e il nodo del server di backup di Linux remoto può a sua volta eseguire il ping di Arcserve UDP.
Il nodo del server di backup di Linux di Arcserve UDP non è stato in grado di gestire il carico mentre Arcserve UDP tentava di stabilire la comunicazione con il nodo.	Verificare che lo stato della CPU sul nodo server di backup di Linux di Arcserve UDP sia in stato normale e riprovare.
Il servizio relativo al server di backup di Linux di Arcserve UDP sul nodo remoto non era in esecuzione mentre Arcserve UDP tentava di stabilire una comunicazione con il nodo.	Verificare che il servizio del server di backup di Linux di Arcserve UDP sia in esecuzione sul nodo remoto e riprovare.
Il servizio del server di backup di Linux di Arcserve UDP non era in grado di comunicare correttamente.	Riavviare il servizio del server di backup di Linux di Arcserve UDP sul nodo remoto e riprovare.

Errore di comunicazione di Arcserve UDP con il Recovery Point Server di Arcserve UDP sui nodi remoti

Valido per i sistemi operativi Windows.

Sintomo

Arcserve UDP non è in grado di stabilire una comunicazione con il Recovery Point Server di Arcserve UDP sui nodi remoti.

Soluzione

Nella tabella seguente sono descritti i motivi e l'azione correttiva corrispondente:

Causa	Misura correttiva
La rete non era disponibile o stabile mentre Arcserve UDP tentava di stabilire una comunicazione con il nodo del Recovery Point Server.	Verificare che la rete sia disponibile e stabile e riprovare. Arcserve UDP può eseguire il ping del nodo del Recovery Point Server remoto e il nodo del Recovery Point Server remoto può a sua volta eseguire il ping di Arcserve UDP.
La condivisione di rete Admin$ del nodo del Recovery Point Server di Arcserve UDP non era disponibile mentre Arcserve UDP tentava di stabilire una comunicazione con il nodo.	Verificare che l'Admin$ di rete del nodo del Recovery Point Server sia disponibile e riprovare.
Il nodo del Recovery Point Server di Arcserve UDP non è stato in grado di gestire il carico mentre Arcserve UDP tentava di stabilire la comunicazione con il server.	Verificare che lo stato della CPU sul nodo del Recovery Point Server si torni nello stato normale e riprovare.
Il servizio dell'agente Arcserve UDP, il servizio dell'archivio dati RPS di Arcserve UDP o il servizio di condivisione porta RPS di Arcserve UDP sul nodo remoto non è in esecuzione quando Arcserve UDP tenta di stabilire una comunicazione con il nodo.	Verificare che il servizio dell'agente Arcserve UDP, il servizio dell'archivio dati RPS di Arcserve UDP o il servizio di condivisione porta RPS di Arcserve UDP sia in esecuzione sul nodo remoto e riprovare.
Per la comunicazione con il nodo del Recovery Point Server viene utilizzato un protocollo errato o una porta errata.	Utilizzare la porta o il protocollo corretto per aggiungere/aggiornare il nodo del Recovery Point Server nella visualizzazione del nodo di destinazione di Arcserve UDP.
Il servizio dell'agente Arcserve UDP, il servizio dell'archivio dati RPS di Arcserve UDP o	Riavviare il servizio dell'agente Arcserve UDP, il servizio dell'archivio

il servizio di condivisione porta RPS di Arcserve UDP non è in grado di comunicare correttamente.	dati RPS di Arcserve UDP o il servizio di condivisione porta RPS di Arcserve UDP sul nodo remoto e riprovare.

Errore di comunicazione di Arcserve UDP con il server di backup di Arcserve sui nodi remoti

Valido per i sistemi operativi Windows.

Sintomo

Errore di comunicazione di Arcserve UDP con il server Arcserve Backup sui nodi remoti.

Soluzione

La tabella riportata di seguito descrive i motivi per cui Arcserve UDP non è in grado di comunicare con il server Arcserve Backup sui nodi remoti e l'azione correttiva corrispondente:

Causa	Misura correttiva
La rete non era disponibile o stabile mentre Arcserve UDP tentava di stabilire una comunicazione con il nodo del server Arcserve Backup.	Verificare che la rete sia disponibile e stabile e riprovare. Arcserve UDP può eseguire il ping del nodo del server Arcserve Backup remoto, che a sua volta può eseguire il ping di Arcserve UDP.
Il nodo del server di backup di Linux UDP di Arcserve Backup non è stato in grado di gestire il carico mentre Arcserve UDP tentava di stabilire la comunicazione con il nodo.	Verificare che lo stato della CPU sul nodo server di Arcserve Backup sia in stato normale e riprovare.
Il servizio relativo al server Arcserve Backup sul nodo remoto non era in esecuzione mentre Arcserve UDP tentava di stabilire una comunicazione con il nodo.	Verificare che il server Arcserve Backup sia in esecuzione sul nodo remoto e riprovare.
Per la comunicazione con il nodo del server Arcserve Backup è stato utilizzato un protocollo errato o una porta errata.	Utilizzare la porta o il protocollo corretto per aggiungere/aggiornare il server Arcserve Backup nella visualizzazione del nodo di destinazione di Arcserve UDP.
Il servizio relativo al server Arcserve Backup non è stato in grado di stabilire la comunicazione in modo adeguato.	Riavviare il servizio relativo al server Arcserve Backup sul nodo remoto e riprovare.

Errore di comunicazione di Arcserve UDP con il sito remoto

Valido per i sistemi operativi Windows.

Sintomo

Errore di comunicazione di Arcserve UDP con il sito remoto.

Soluzione

La tabella seguente descrive i motivi per cui Arcserve UDP non è in grado di comunicare con il sito remoto e l'azione correttiva corrispondente:

Causa	Misura correttiva
La rete non è disponibile o non è stabile.	Verificare che la rete sia disponibile e stabile e riprovare.
Arcserve UDP viene reinstallato e il sito remoto non è registrato in Arcserve UDP.	Registrare il sito remoto in Arcserve UDP.
Il nome host o l'indirizzo IP di Arcserve UDP è stato modificato e il sito remoto non è registrato in Arcserve UDP.	Registrare il sito remoto in Arcserve UDP.
Il nome host o l'indirizzo IP del sito remoto è stato modificato e il sito remoto non è registrato in Arcserve UDP.	Registrare il sito remoto in Arcserve UDP.

Problemi correlati a piano, processo e impostazioni

In questa sezione verranno illustrati i seguenti argomenti sulla risoluzione dei problemi relativi al processo e alle impostazioni di backup:

- Errore del processo di backup in seguito alla modifica del nome host/indirizzo IP della console
- Aggiunta di una password di crittografia per una destinazione crittografata esistente
- Errore di applicazione delle impostazioni di backup a un nodo
- Errore durante la distribuzione del piano in seguito alla modifica della password del computer proxy di backup senza agente
- Impostazioni disattivate durante l'apertura dell'interfaccia utente dell'agente
- Mancata sospensione e ripresa quando l'agente non è connesso alla rete
- Esecuzione rallentata del servizio dell'agente Arcserve UDP
- Configurazione del Registro di sistema per ripetere un processo di copia su nastro
- Configurazione del Registro di sistema per la copia di più punti di ripristino dello stesso tipo su un nastro dello stesso processo
- File/cartella ignorati dal backup della cartella NFS condivisa o nome del file o della cartella convertiti in elementi indesiderati
- Errore di backup della cartella NFS condivisa
- Nome del server errato nella richiesta di licenza per i percorsi UNC
- Reimpostazione della console UDP abilitata per MFA quando TOTP non è disponibile

Errore del processo di backup in seguito alla modifica del nome host/indirizzo IP della console

Sintomo

La console e il server RPS sono stati installati sullo stesso computer. Il backup funzionava correttamente ma dopo aver modificato il nome host/indirizzo IP della console, il processo di backup ha prodotto un errore.

Soluzione

Il problema si verifica se sono presenti piani assegnati ai nodi e viene modificato il nome host/indirizzo IP del computer.

Per risolvere il problema, aggiornare manualmente i nodi dell'agente ed eseguire nuovamente il processo di backup.

Effettuare le operazioni seguenti:

1. Accedere alla pagina Nodi: Tutti i nodi.
2. Selezionare il nodo.
3. Fare clic con il tasto destro del mouse e selezionare **Aggiorna**.
4. Fare clic su **OK**.

I nodi vengono aggiornati.

Aggiunta di una password di crittografia per una destinazione crittografata esistente

Sintomo

Si è dimenticato di aggiungere la password di crittografia per la destinazione di copia file.

Soluzione

A questo punto è possibile aggiungere la password di crittografia.

Effettuare le operazioni seguenti:

1. Aprire il piano.
2. Aprire la destinazione di copia file in cui aggiungere la password di crittografia.
3. Modificare il tipo di destinazione da Archiviazione cloud\Condivisione di rete in Condivisione di rete\Archiviazione cloud.
4. Fornire una condivisione di rete o un'archiviazione cloud e salvare.
5. Riaprire il piano e passare alla destinazione di copia file.
6. Modificare la destinazione in Fornitore cloud\Condivisione di rete.
7. Selezionare Fornitore cloud\Condivisione di rete, quindi selezionare il bucket o il percorso Contenitore\Provider.
8. Fornire una password di crittografia valida.
9. Salvare il piano.

Errore di applicazione delle impostazioni di backup a un nodo

Sintomo

Si dispone di due console, console A e console B. Viene aggiunto un Recovery Point Server alla console A e viene creato un piano per il Recovery Point Server. Quindi si aggiunge il Recovery Point Server alla console B. Ora il Recovery Point Server viene gestito dalla console B. Tuttavia, se si aggiorna il nodo agente dalla console A di cui è stato eseguito il backup nel Recovery Point Server, viene visualizzato il seguente errore:

Impossibile applicare le impostazioni di backup al nodo. (Impossibile trovare il piano del Recovery Point Server di Arcserve UDP sul server.)

Soluzione

Per evitare il problema, attenersi alla procedura seguente:

1. Selezionare il piano dalla Console A.
2. Dal riquadro centrale, fare clic su **Azioni**, quindi selezionare **Distribuisci ora**.

   Il piano viene ridistribuito e le impostazioni di backup vengono applicate al nodo.

Errore durante la distribuzione del piano in seguito alla modifica della password del computer proxy di backup senza agente

Sintomo

Se la console e il server proxy appartengono a computer diversi, dopo aver modificato la password del computer proxy, la ridistribuzione del piano non riesce. Viene visualizzato un messaggio di errore indicante le credenziali non corrette.

Soluzione

Per risolvere il problema, attenersi alla procedura seguente:

1. Dalla visualizzazione del nodo nella console, aggiornare il server proxy con le nuove credenziali.
    a. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.
    b. Fare clic con il tasto destro del mouse sul nodo e selezionare **Aggiorna** per aggiornare il server proxy.
2. Se il Recovery Point Server e il proxy si trovano sullo stesso computer, aggiornare il Recovery Point Server con le nuove credenziali.
    a. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.
    b. Fare clic con il tasto destro del mouse sul Recovery Point Server dal riquadro centrale fare e selezionare **Aggiorna**.
3. Riavviare il servizio dell'agente Arcserve UDP nel computer proxy.
4. Ridistribuire il piano.

Impostazioni disattivate durante l'apertura dell'interfaccia utente dell'agente

Se i nodi dell'agente Arcserve UDP (Windows) non vengono rimossi dall'interfaccia utente Arcserve UDP prima della disinstallazione della Console di Arcserve UDP, le impostazioni verranno disattivate durante l'apertura dell'interfaccia utente dell'agente per i nodi dell'agente Arcserve UDP in questione.

Sintomo

Il nodo dell'agente Arcserve UDP (Windows) non viene notificato circa la disinstallazione della console Arcserve UDP. Suppone che venga gestito.

Soluzione

Rimuovere i file RegConfigPM.xml e BackupConfiguration.xml nella directory <UDP_ENGINE_HOME>\Configuration del nodo dell'agente Arcserve UDP (Windows), quindi riavviare il servizio dell'agente Arcserve UDP.

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Mancata sospensione e ripresa quando l'agente non è connesso alla rete

Sintomo

Se l'agente non è connesso alla rete e si tenta di interrompere un piano, il piano non viene interrotto. Allo stesso modo, se l'agente non è connesso alla rete e si tenta di riprendere un piano, il piano non viene ripreso.

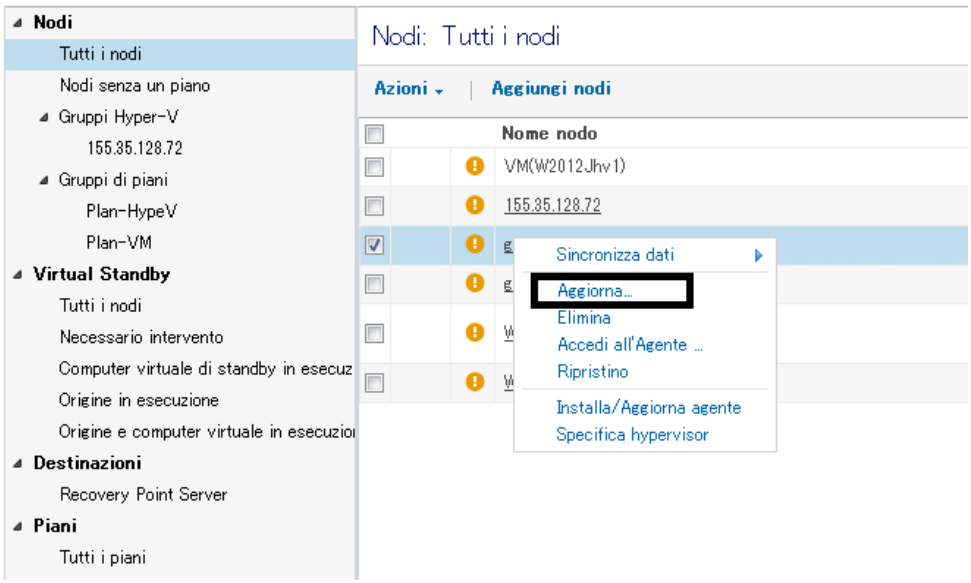
Soluzione

È possibile risolvere il problema aggiornando manualmente il nodo dalla Console.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda Risorse della Console.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su Tutti i nodi.

   Tutti i nodi aggiunti vengono visualizzati nel riquadro centrale.
3. Selezionare il nodo dal riquadro centrale.
4. Fare clic con il tasto destro del mouse e selezionare **Aggiorna**.



Il nodo e il piano vengono aggiornati.

Esecuzione rallentata del servizio dell'agente Arcserve UDP

Valido per i sistemi operativi Windows.

Sintomo 1:

L'esecuzione del servizio dell'agente Arcserve UDP su sistemi dell'agente Arcserve UDP è rallentata. È possibile individuare altri sintomi quali:

- Il servizio dell'agente Arcserve UDP non risponde o occupa il 100% delle risorse della CPU.
- I nodi dell'agente Arcserve UDP presentano prestazioni insufficienti o errori di comunicazione con il servizio Web.

Soluzione 1:

In alcune configurazioni di ambiente, il servizio dell'agente Arcserve UDP richiede tempi di CPU troppo lunghi oppure presenta un ritardo nella risposta. Per impostazione predefinita, Tomcat è configurato per allocare un valore limitato di memoria ai nodi, impostazione che potrebbe non essere adatta all'ambiente in uso. Per verificare questo problema, consultare i seguenti file di 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

Individuare il seguente messaggio:

java.lang.OutOfMemoryError

Per correggere il problema, aumentare il valore di memoria allocata.

Per aumentare la memoria, procedere come segue:

1. Aprire l'Editor del Registro di sistema e selezionare la seguente chiave:

   Sistemi operativi x86:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java

   Sistemi operativi x64:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java

2. Utilizzare una delle seguenti opzioni:

- Se il messaggio presente nel file di registro è il seguente:

  java.lang.OutOfMemoryError: PermGen space

  Aggiungere la stringa seguente al valore di Opzioni.

  -XX:PermSize=128M -XX:MaxPermSize=128M

  Nota: Potrebbe essere necessario aumentare il valore di -XX:MaxPermSize per adattarlo al proprio ambiente.

- Se il messaggio presente nel file di registro è uno dei seguenti:

  java.lang.OutOfMemoryError: Java heap space
  java.lang.OutOfMemoryError: GC overhead limit exceeded

  Aumentare il valore del seguente DWORD:

  JvmMx

3. Riavviare il servizio dell'agente Arcserve UDP.

Sintomo 2

I backup pianificati vengono ignorati e ne viene interrotta l'esecuzione.

Soluzione 2

Quando il valore massimo configurato corrisponde a 20 backup simultanei (o un valore inferiore), eseguire le seguenti operazioni:

1. Aumentare il valore del seguente DWORD:

   JvmMx=256

   Nota: Il valore DWORD viene riportato nella soluzione 1.

2. Aggiungere la stringa seguente al valore di Opzioni.

   -XX:MaxPermSize=128M

   Nota: Il valore DWORD viene riportato nella soluzione 1.

Quando il valore massimo configurato è compreso tra 20 e 50 backup simultanei, eseguire le seguenti operazioni:

1. Aumentare il valore del seguente DWORD:

   JvmMx=512

   Nota: Il valore DWORD viene riportato nella soluzione 1.

2. Aggiungere la stringa seguente al valore di Opzioni.

   -XX:MaxPermSize=256M

   Nota: Il valore DWORD viene riportato nella soluzione 1.

Configurazione del Registro di sistema per ripetere un processo di copia su nastro

Sintomo

Il processo di copia su nastro non è stato eseguito a causa di errori di supporto, pertanto si desidera ripeterlo.

Soluzione

È possibile controllare il numero di ripetizioni e il relativo intervallo di tempo per l'attività di copia su nastro utilizzando le seguenti due chiavi del Registro di sistema. Entrambe le chiavi del Registro di sistema si trovano nel computer in cui è stato installato il server Arcserve Backup:

NumberOfRetryCopyToTapeJob

In caso di errore del processo di copia su nastro, Arcserve Backup tenterà di eseguire il processo non riuscito. Il numero di tentativi è configurato mediante la chiave del Registro di sistema **NumberOfRetryCopyToTapeJob**. Ma se le informazioni sul nodo o punto di ripristino da copiare vengono modificate durante il processo, in Arcserve UDP il numero di errori accumulati viene reimpostato su 0. Ciò significa che dopo aver modificato le informazioni sul nodo o sul punto di ripristino da copiare durante il processo, la copia su nastro può essere eseguita senza limiti dal numero di tentativi. Inoltre, se il servizio Web Arcserve Backup viene riavviato, in Arcserve UDP il numero di errori accumulati viene reimpostato su 0.

La chiave del Registro di sistema si trova nel server Arcserve Backup al percorso seguente:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo\NumberOfRetryCopyToTapeJob

È una chiave di tipo DWORD.

Impostazione predefinita: 1

TimeIntervalOfRetryCopyToTapeJob

Consente di controllare l'intervallo di ripetizione per il processo di copia su nastro non riuscito. Questa chiave del Registro di sistema viene utilizzata con **NumberOfRetryCopyToTapeJob**.

La chiave del Registro di sistema si trova nel server Arcserve Backup al percorso seguente:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo\TimeIntervalOfRetryCopyToTapeJob

È una chiave di tipo DWORD.

Impostazione predefinita: 1 ora

Configurazione del Registro di sistema per la copia di più punti di ripristino dello stesso tipo su un nastro dello stesso processo

Sintomo

Per impostazione predefinita, processo di copia su nastro copia tutti i punti di ripristino qualificati su nastro, anche nel caso in cui siano dello stesso tipo. Di conseguenza, viene consumato più spazio su nastro ed è richiesto più tempo per la copia. È possibile copiare soltanto il punto di ripristino qualificato più recente.

Soluzione

È possibile configurare il Registro di sistema sul nodo del server Arcserve Backup per abilitare la copia del punto di ripristino più recente dello stesso tipo su nastro.

Effettuare le operazioni seguenti:

1. Sul nodo del server Arcserve Backup, aggiungere il seguente valore DWORD al Registro di sistema contenuto in [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo]:

   "CopyLatestRecoveryPointOfSameType"=dword:00000001

2. Riavviare il server Web del server Arcserve Backup per rendere effettive le modifiche.

   Tutti i processi di copia su nastro del nodo server Arcserve Backup copieranno il punto di ripristino più recente dello stesso tipo su nastro.

File/cartella ignorati dal backup della cartella NFS condivisa o nome del file o della cartella convertiti in elementi indesiderati

Sintomo

Quando viene eseguito il backup della cartella NFS condivisa, alcuni file o alcune cartelle sono mancanti nei dati di backup o nel nome di un file o di una cartella convertiti in elementi indesiderati.

Soluzione

Questo problema si verifica se un file o una cartella nella cartella NFS condivisa sono associati a un nome la cui codifica della lingua non è supportata. Come soluzione, esportare una cartella SMB condivisa invece della cartella NFS condivisa. Prendere inoltre in considerazione l'aggiunta un percorso UNC o NFS con il protocollo SMB.

Per ulteriori informazioni sull'aggiunta di un percorso UNC e sulla codifica della lingua supportata, fare riferimento alla sezione Aggiunta di un percorso UNC.

Errore di backup della cartella NFS condivisa

Sintomo

Quando viene eseguito il backup della cartella NFS condivisa, il processo non riesce.

Soluzione

Questo problema si verifica se sono stati modificati i valori GID (identificatore gruppo) e UID (identificatore utente) rispetto ai valori predefiniti. Conservare sempre solo i valori GID e UID predefiniti per il client e il server NFS.

Reimpostazione della console UDP abilitata per MFA quando TOTP non è disponibile

Sintomo

Dopo aver abilitato il processo di accesso con autenticazione a più fattori (MFA) sulla console UDP, potrebbero verificarsi i seguenti scenari:

- Mancata scansione del codice QR
- Perdita del dispositivo mobile contenente un'app di autenticazione
- Disinstallazione dell'app di autenticazione

Soluzione 1

Se si è un amministratore con privilegi avanzati o un utente amministratore o non amministratore, contattare il proprio amministratore o altri utenti amministratori di UDP per reimpostare il codice QR dalla Console UDP.

Soluzione 2

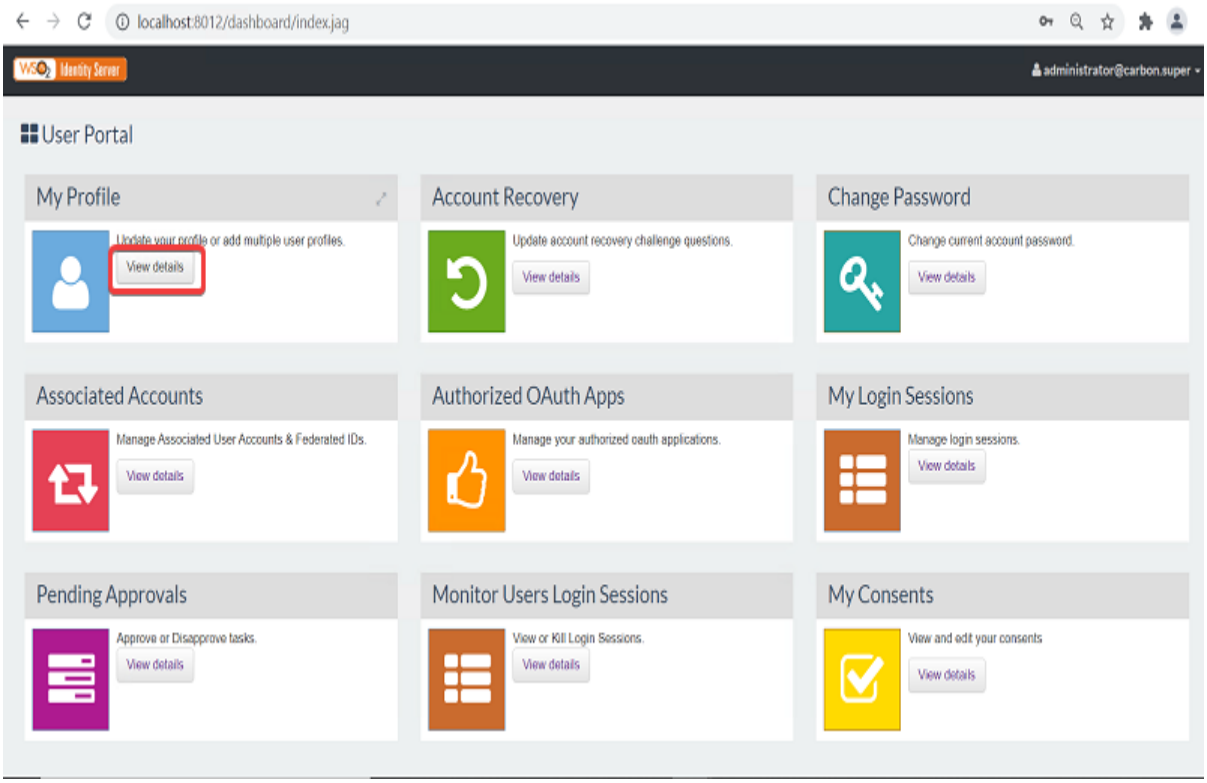
Se si è un amministratore con privilegi avanzati o un utente amministratore, è possibile eseguire la scansione dell'immagine del codice QR per un nuovo TOTP utilizzando il portale del dashboard del Server di identità.

Effettuare le operazioni seguenti:

1. Accedere al dashboard del Server di identità.

   Ad esempio: *https://localhost:8012/dashboard*

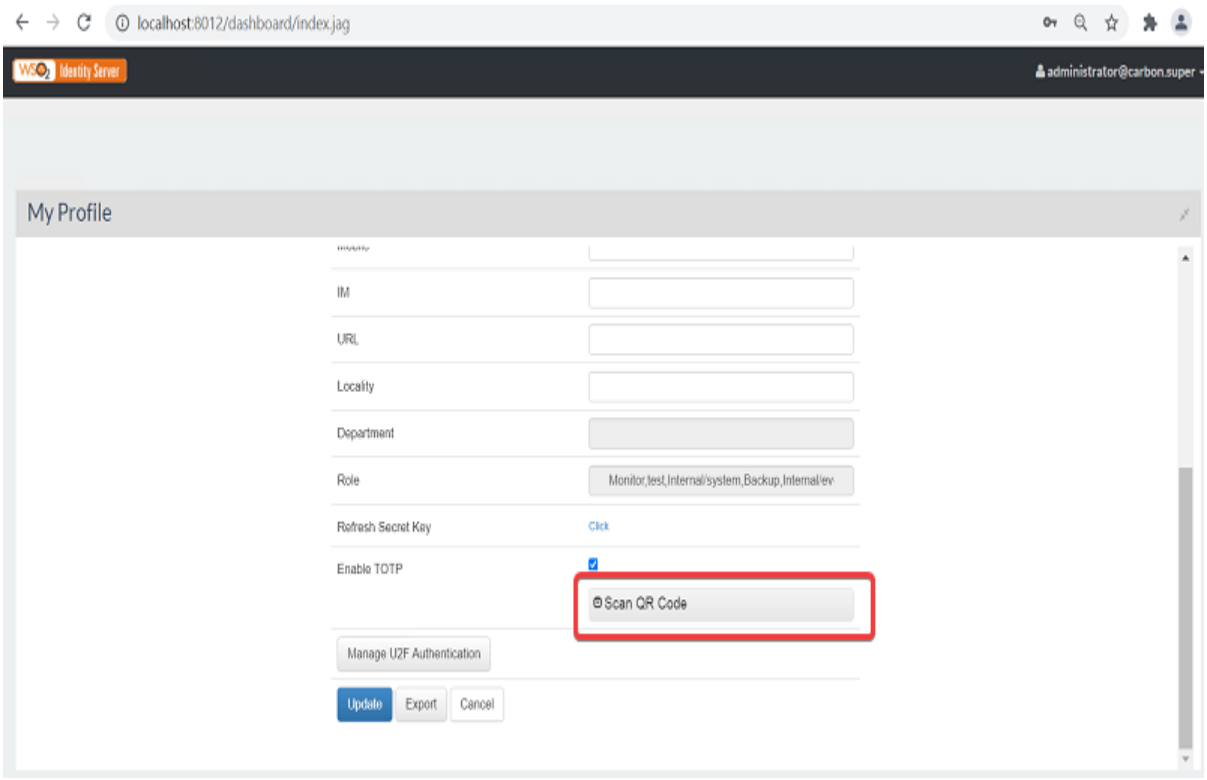
   Verrà visualizzata la pagina Portale utente.



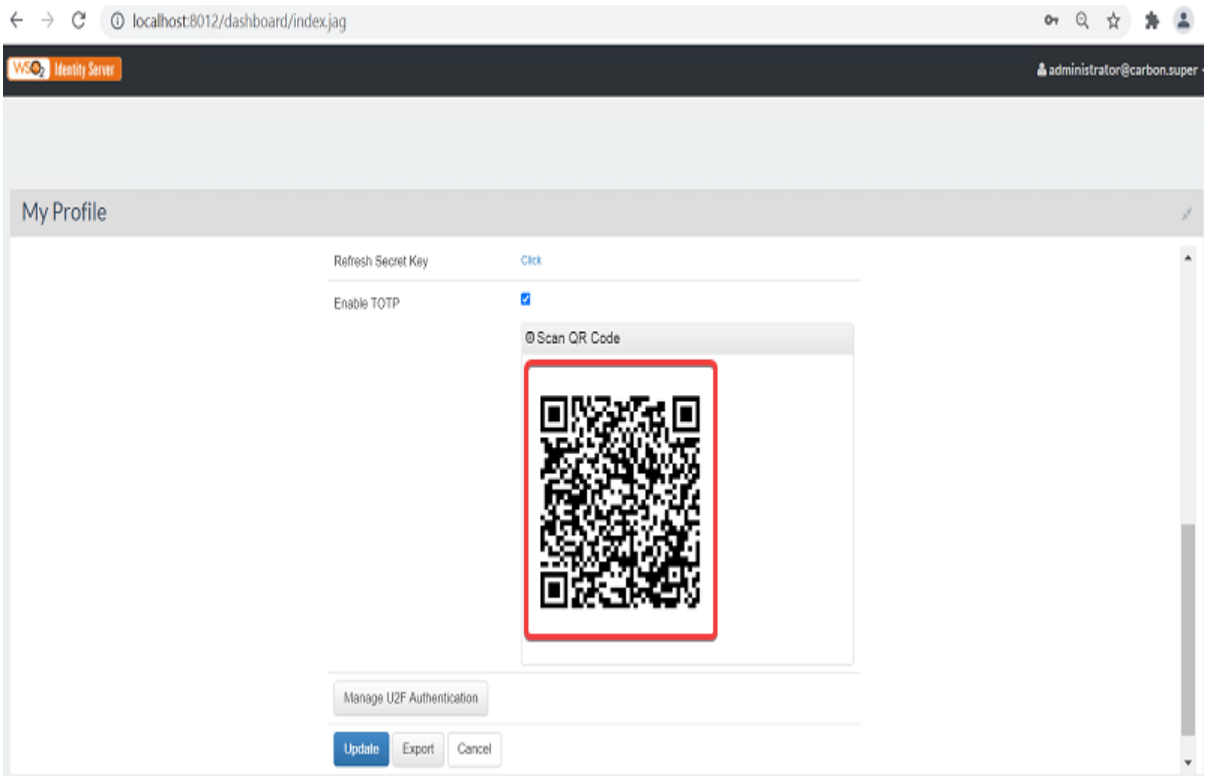
2. Nella pagina Portale utente fare clic su **Visualizza dettagli**.

   Viene visualizzata la pagina Profili personali.

3. Nella pagina Profili personali, in Attiva TOTP, fare clic su **Scansione codice QR** per visualizzare l'immagine del codice QR.



4. Per generare il TOTP, eseguire la scansione dell'immagine del codice QR utilizzando un'app di autenticazione.



5. Accedere alla pagina di accesso della console UDP, quindi effettuare l'accesso utilizzando il TOTP appena generato.

Soluzione 3

Se si è un utente con privilegi avanzati, è possibile rimuovere completamente le impostazioni esistenti.

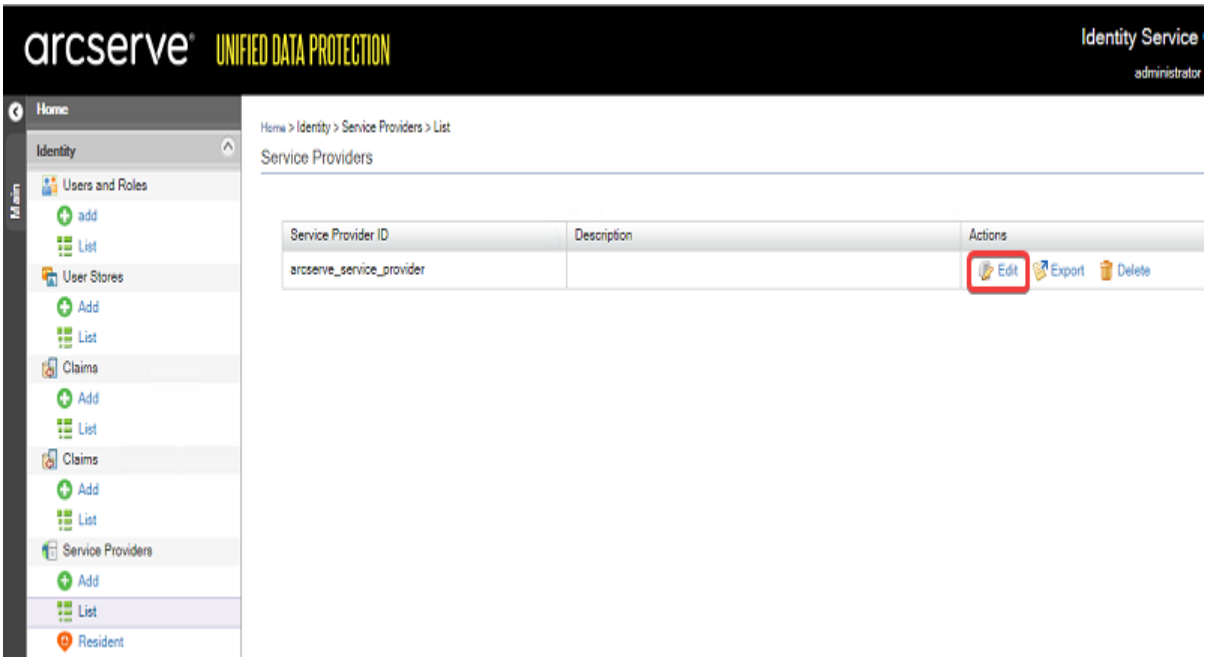
Effettuare le operazioni seguenti:

1. Accedere al percorso *…\Programmi\Arcserve\Unified Data Protection\Management\IdentityServer\repository\conf*, quindi aprire il file *carbon.xml* con un editor di testo.
2. Nel file carbon.xml, aggiungere un commento ai tag XML *HideMenuItemIds* e salvare il file.

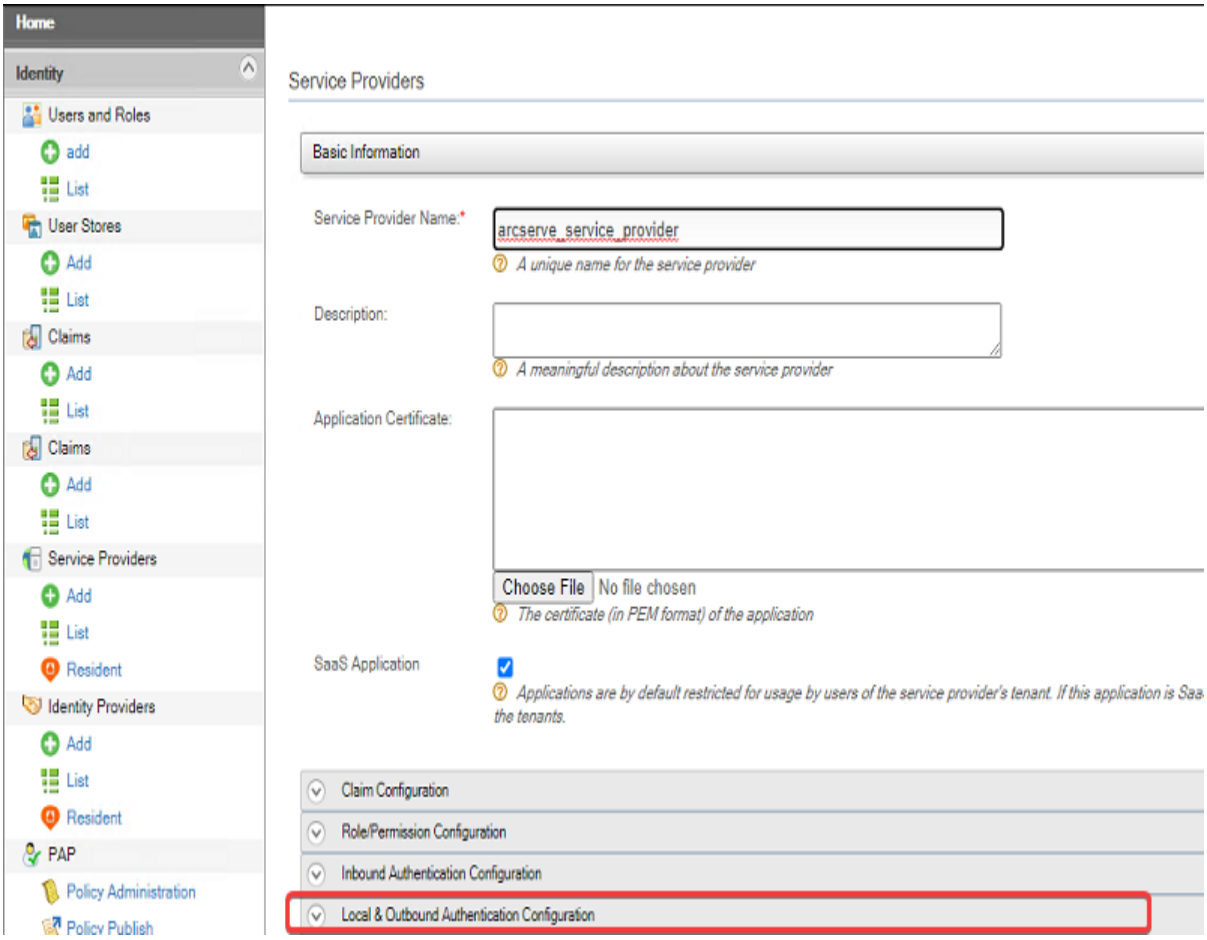


3. Riavviare il Servizio identità di Arcserve UDP.
4. Avviare la console Gestione utenti. Per ulteriori informazioni, consultare la sezione Avvio della Console di gestione degli utenti di Arcserve UDP.

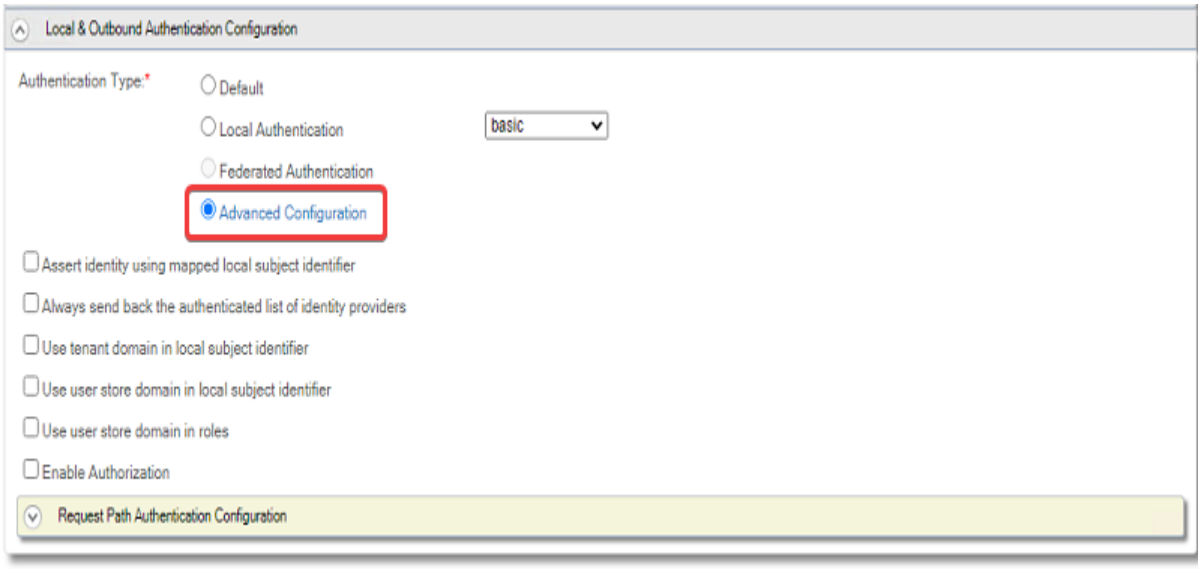
   Viene visualizzata la pagina Console Servizio identità.
5. Accedere a **Pagina principale** > **Identità** > **Provider dei servizi** > **Elenco**.



6. Nell'elenco Provider dri servizi, per *arcserve_service_provider*, fare clic su **Modifica**.



7. Espandere l'elenco a discesa **Configurazione autenticazione locale e in uscita**, quindi selezionare **Configurazione avanzata**.

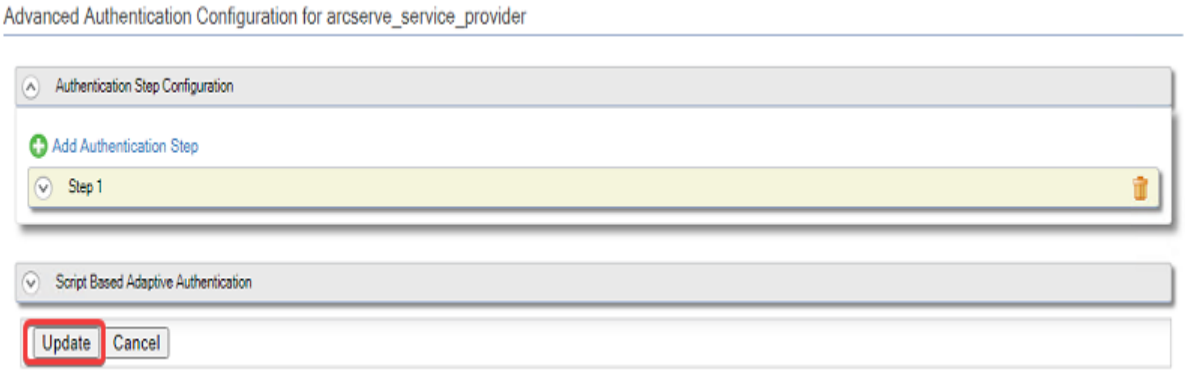


Viene visualizzata la pagina Configurazione avanzata per *arcserve_service_provider*.

8. Nella pagina *Configurazione avanzata per arcserve_service_provider*, in Configurazione passaggio di autenticazione, per rimuovere il passaggio 2, fare clic sull'icona **Elimina**.



9. Fare clic su **Aggiorna** per salvare le modifiche.



Le impostazioni esistenti vengono rimosse.

10. Accedere alla pagina di accesso di UDP, quindi effettuare l'accesso utilizzando il nome utente e la password.
11. Accedere a **Impostazioni** > **Gestione utenti**.
12. Nella sezione Autenticazione a più fattori, per disattivare l'MFA, impostare l'impostazione su **Disattivato**.
13. Fare clic su **Salva**.

    Le impostazioni per l'accesso MFA vengono rimosse correttamente.

Problemi correlati al computer virtuale istantaneo

In questa sezione verranno illustrati i seguenti argomenti sulla risoluzione dei problemi relativi al computer virtuale istantaneo:

- Impossibile creare un computer virtuale istantaneo in VMware a causa del nome duplicato per l'archivio dati NFS
- Impossibile creare un computer virtuale istantaneo utilizzando Windows 2008 come server di ripristino per i server VMware o Windows 2008 R2 Hyper-V
- Errore di avvio di un computer virtuale istantaneo nel caso di un server Windows AD 2008/2012/2016
- Non è possibile attivare il computer virtuale dopo il ripristino di Hyper-V
- Processo del computer virtuale istantaneo non riuscito a causa di un errore del servizio Windows NFS
- Impossibile accedere o eliminare la cartella del file del computer virtuale istantaneo pur disponendo dei privilegi di amministratore
- Mancato avvio del computer virtuale istantaneo in Hyper-V dopo il riavvio del server di ripristino
- Impossibile creare l'archivio dati NFS VMware. Errore visualizzato: Impossibile risolvere il nome host
- Impossibile distribuire il servizio di integrazione al computer virtuale guest in Hyper-V
- Errore del computer virtuale istantaneo Linux su un server Hyper-V in lingua non inglese
- Utilizzo di altre licenze per i percorsi UNC che si trovano in un computer virtuale Hyper-V su licenza
- Visualizzazione di un errore di licenza se si modifica l'edizione o il tipo di licenza e si crea un computer virtuale istantaneo

Impossibile creare un computer virtuale istantaneo in VMware a causa del nome duplicato per l'archivio dati NFS

Sintomo

Impossibile creare il computer virtuale istantaneo. Viene visualizzato il seguente messaggio di errore:

Impossibile creare l'archivio dati NFS [arcserve_UDP_<Hostnam/IP>] con il nome della condivisione NFS [arcserve_UDP_IVM_{GUID}]. Codice errore: 12. Messaggio di errore: Chiave specificata, nome o identificatore già esistente (dettagli:).

Questo errore potrebbe essere causato da un archivio dati NFS con lo stesso nome già esistente e non rimosso oppure da vCenter/Host che contiene ancora riferimenti dell'archivio dati NFS nei relativi record. Tuttavia, se si accede direttamente all'host, viene visualizzato un archivio dati NFS. Questo archivio è solitamente contrassegnato come non attivo oppure in grigio.

Soluzione

Per risolvere questo problema:

1. Accedere all'host ESX e rimuovere l'archivio dati NFS.
2. Riavviare gli agenti di gestione sull'host ESX utilizzando il comando seguente:

   /sbin/services.sh restart

Per ulteriori informazioni sull'utilizzo dell'host ESX, consultare la documentazione di VMware.

Impossibile creare un computer virtuale istantaneo utilizzando Windows 2008 R2 come server di ripristino per i server VMware o Windows 2008 R2 Hyper-V

Sintomo

Quando non è possibile creare il computer virtuale istantaneo, nel registro attività del processo viene riportato l'errore seguente:

Impossibile verificare la firma digitale del file. In seguito a una modifica recente dell'hardware o del software, è possibile che sia stato installato un file danneggiato, con una firma non corretta o che potrebbe essere malware di origine sconosciuta.

Soluzione

Il computer virtuale istantaneo non viene creato perché il relativo driver è firmato con un certificato digitale protetto che non è supportato in Windows 2008 R2 senza applicare una patch di Microsoft.

Applicare la patch 3033929 di Microsoft e riprovare a creare il computer virtuale istantaneo.

Errore di avvio di un computer virtuale istantaneo nel caso di un server Windows AD 2008/2012/2016

Sintomo

Errore di avvio di un computer virtuale istantaneo se il computer virtuale è un server Active Directory di Windows 2008.

Se il computer di origine è un server Active Directory di Windows su cui è in esecuzione il processo del computer virtuale istantaneo, viene visualizzato un errore di avvio del computer virtuale istantaneo e viene visualizzata una schermata blu con il messaggio seguente:

STOP: c00002e2 Directory Services could not start because of the following error: a device attached to the system is not functioning. Stato di errore: 0xc0000001.

Soluzione 1:

Se l'hypervisor di destinazione è un Hyper-V, aggiungere la seguente chiave di registro sull'hypervisor HyperV, quindi attivare il processo del computer virtuale istantaneo.

Se l'hypervisor di destinazione è un ESX/Vcenter, aggiungere la seguente chiave di registro sul computer proxy, la quale viene utilizzata per eseguire il processo del computer virtuale istantaneo. Quindi attivare il processo corrispondente.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\InstantVM
```

Tipo registro: valore DWORD

Nome: RenameADLog

Valore: 1

Limitazioni:

- Se i percorsi del database NTDS e dei file di registro NTDS si trovano su volumi diversi, la soluzione riportata precedentemente non è valida.
- Al momento, la soluzione di cui sopra è valida solo per il server Windows 2008 Active Directory.

Soluzione 2:

Risolvere manualmente il problema mediante l'accesso al computer virtuale istantaneo.

Effettuare le operazioni seguenti:

1. Avviare il computer virtuale istantaneo.
2. Durante l'attivazione del computer, premere F8 prima che venga avviato il caricamento del sistema operativo, quindi scegliere la modalità di **ripristino del servizio Directory.**
3. Rinominare tutti i file *.log nella cartella *C:\Windows\NTDS*. Ad esempio, rinominare il file edb.log in edb.log.old.
4. Eseguire il comando:

   ```
   esentutl /p "C:\Windows\NTDS\ntds.dit"
   ```

5. Riavviare il sistema.

Nota: la soluzione precedente è valida per tutte le versioni di server Windows con Active Directory installato.

Non è possibile attivare il computer virtuale dopo il ripristino di Hyper-V

Sintomo

Non è possibile attivare il computer virtuale dopo il ripristino del computer virtuale Hyper-V. Viene visualizzato un errore simile al seguente:

Porta Ethernet sintetica (ID istanza): impossibile attivare il computer virtuale a causa dell'errore "Tentativo di accedere a un indirizzo non valido".

Soluzione

Questo errore si verifica perché l'indirizzo MAC del computer virtuale ripristinato è in conflitto con quello dei computer virtuali esistenti. Rimuovere la scheda NIC del computer virtuale ripristinato, quindi aggiungerne manualmente una nuova per risolvere il problema e riattivarlo correttamente.

Processo del computer virtuale istantaneo non riuscito a causa di un errore del servizio Windows NFS

Sintomo

Quando nel server di ripristino del computer virtuale istantaneo sono installati l'agente Arcserve UDP e Arcserve Backup, se si crea un computer virtuale istantaneo nel server VMware ESX(i), il servizio NFS di Windows non viene avviato e il processo del computer virtuale istantaneo non riesce.

Soluzione

Il servizio NFS di Windows non viene avviato poiché il numero di porta predefinito di tale servizio è 111, ma questo è utilizzato dal servizio Arcserve Backup **Server di chiamata a procedura remota**.

Per risolvere il problema, cambiare il numero di porta predefinito del servizio Arcserve Backup **Server di chiamata a procedura remota** con un'altra porta e ripetere la creazione del computer virtuale istantaneo. Per ulteriori informazioni sulla modifica della porta predefinita, consultare le sezioni Modifica del file di configurazione delle porte e Porte di comunicazione tra server primario e server membro della documentazione di Arcserve Backup.

Impossibile accedere o eliminare la cartella del file del computer virtuale istantaneo pur disponendo dei privilegi di amministratore.

Sintomo

Non è possibile accedere o eliminare la cartella del file del computer virtuale istantaneo a causa dell'autorizzazione richiesta da parte dell'amministratore anche se l'utente dispone dei privilegi di amministratore.

Soluzione

Si tratta di un problema di NFS. È necessario rimuovere innanzitutto la condivisione NFS per poter eliminare la cartella. Per eliminare la cartella, utilizzare la riga di comando seguente:

nfsshare /delete [nfs share name]

Mancato avvio del computer virtuale istantaneo in Hyper-V dopo il riavvio del server di ripristino

Sintomo

Quando si avvia il computer virtuale istantaneo (IVM) e poi si riavvia il server di ripristino di Hyper-V, il computer virtuale istantaneo non viene avviato.

Soluzione

Per risolvere questo errore di avvio, riavviare il computer virtuale istantaneo.

Impossibile creare l'archivio dati NFS VMware. Errore visualizzato: Impossibile risolvere il nome host

Valido per VMware

Sintomo

Impossibile creare il computer virtuale istantaneo. Viene visualizzato il seguente messaggio di errore:

Impossibile creare l'archivio dati VMWARE NFS con il server <hostname of recovery server>.

Messaggio di errore: Si è verificato un errore durante la configurazione dell'host.

Dettagli: Operazione non riuscita. Rapporto di diagnostica: Impossibile risolvere il nome host <one hostname but not recovery server>.

Esempio

Impossibile creare l'archivio dati VMWARE NFS con il server 'host1'.

Messaggio di errore: Si è verificato un errore durante la configurazione dell'host.

Dettagli: Operazione non riuscita. Rapporto di diagnostica: Impossibile risolvere il nome host 'host2'.

Soluzione

Questo errore deriva dal fatto che sul server ESX sono elencati tutti gli archivi dati NFS quando si crea un archivio dati NFS InstantVM, anche se alcuni non sono più disponibili. Ad esempio, l'archivio dati NFS creato da **host2** è ancora presente anche se **host2** non è disponibile perché il computer è stato eliminato. Pertanto, il server ESX non è in grado di risolvere il nome host.

Per risolvere il problema, eliminare l'archivio dati non disponibile dal server ESX.

Effettuare le operazioni seguenti:

1. Accedere al server ESX utilizzando il protocollo SSH.
2. Digitare il seguente comando:

   ```
   esxcfg-nas -l
   ```

   Nella riga di comando viene visualizzato lo stesso errore.

   ```
   Errore durante l'operazione: Impossibile risolvere
   il nome host 'host2'.
   ```

3. Aggiungere il mapping nel file **/etc/hosts** del server ESX per risolvere il problema.

   <IP address> <hostname>

Nota: L'indirizzo IP deve essere raggiungibile.

Esempio: 10.57.X.X host2

4. Elencare tutti gli archivi dati NFS utilizzando il comando seguente:

```
esxcfg-nas -l
```

```
arcserve_UDP_<hostname> is /arcserve_UDP_IVM_{ESX_
generated_number} from <hostname> unmounted una-
vailable
```

Esempio: esxcfg-nas –l

arcserve_UDP_host2 is /arcserve_UDP_IVM_{991555E6-09A4-4D80-A47E-522831A62Axx} from host2 unmounted unavailable

5. Per eliminare l'archivio dati non disponibile, utilizzare il comando seguente:

```
esxcfg-nas -d arcserve_UDP_host2
```

6. Rimuovere il mapping <hostname> nel file **/etc/hosts** dal server ESX.

A questo punto è possibile utilizzare la funzione NFS come di consueto.

Nota: Per ulteriori informazioni su questo problema, consultare l'articolo della Knowledge Base di VMware.

Impossibile distribuire il servizio di integrazione al computer virtuale guest in Hyper-V

Sintomo

Quando si esegue il backup di un computer virtuale con l'applicazione SQL o Exchange installata, il punto di ripristino non include le informazioni del writer e il registro attività del processo di backup riporta il seguente messaggio di avviso:

Impossibile distribuire il servizio di integrazione al computer virtuale.

Soluzione

Questo problema si verifica spesso quando Strumentazione gestione Windows (WMI) viene disabilitato dal firewall sul computer virtuale guest. Per risolvere questo problema, procedere come segue:

1. Accedere al computer virtuale guest.
2. Aprire il Pannello di controllo.
3. Aprire Windows Firewall.
4. Fare clic su Consenti app o funzionalità attraverso Windows Firewall.
5. Abilitare Strumentazione gestione Windows (WMI).
6. Fare clic su OK.

Errore del computer virtuale istantaneo Linux su un server Hyper-V in lingua non inglese

Errore del computer virtuale istantaneo di Linux sul server Hyper-V in lingua non inglese dovuto a un errore di connessione anche nel caso in cui il firewall sia disattivato.

Sintomo

La creazione del computer virtuale istantaneo mostra il seguente errore:

Impossibile stabilire la connessione all'host Hyper-V [Target Hyper-V ServerName]. Verificare che l'indirizzo dell'host sia corretto o che le credenziali siano valide.

Soluzione

Una configurazione errata delle informazioni di connessione del server Hyper-V potrebbero causare il problema.

Per ulteriori informazioni, consultare la sezione **Configurazione delle informazioni di connessione del server Hyper-V per il computer virtuale istantaneo** nella *Guida per l'utente dell'agente Arcserve UDP per Linux*.

Utilizzo di altre licenze per i percorsi UNC che si trovano in un computer virtuale Hyper-V su licenza

Sintomo

I percorsi UNC che si trovano in un computer virtuale all'interno di un hypervisor utilizzano una licenza socket aggiuntiva anche se l'host dell'hypervisor è già dotato di licenza. Questo determina un utilizzo di licenze aggiuntive.

Soluzione

I backup dell'host dell'hypervisor e i percorsi UNC che risiedono nello stesso hypervisor utilizzano la stessa licenza. Tuttavia, durante il backup dei percorsi UNC che risiedono in qualsiasi computer virtuale all'interno dello stesso hypervisor, i percorsi UNC o le condivisioni utilizzano una licenza aggiuntiva. Questo problema si verifica solo se il computer virtuale non viene aggiunto/importato come un nodo alla console e anche quando i percorsi UNC vengono aggiunti con un nome diverso da quello fornito durante l'aggiunta del computer virtuale alla console.

Effettuare le operazioni seguenti:

1. Aggiungere il nodo (il computer virtuale con i percorsi UNC) alla console e specificare i dettagli dell'hypervisor per il nodo oppure importare il nodo dall'hypervisor.
2. Aggiungere i percorsi UNC o le condivisioni con lo stesso nome specificato nel passaggio 1.

Visualizzazione di un errore di licenza se si modifica l'edizione o il tipo di licenza e si crea un computer virtuale istantaneo

Sintomo

Dopo aver aggiunto o modificato un tipo di licenza o un'edizione nella console e aver creato un computer virtuale istantaneo senza aver eseguito alcun processo di backup, viene visualizzato un messaggio indicante un errore della licenza. Tuttavia, alla successiva esecuzione di un computer virtuale istantaneo, identifica correttamente la nuova licenza e crea un computer virtuale istantaneo.

Soluzione

Effettuare le operazioni seguenti:

1. Dopo aver aggiunto una nuova licenza alla console UDP per il piano esistente, eseguire il processo di backup.
2. È ora possibile creare un computer virtuale istantaneo.

Problemi correlati all'agente Linux

In questa sezione verranno illustrati i seguenti argomenti sulla risoluzione dei problemi relativi all'agente Linux di Arcserve UDP:

- Impostazioni della destinazione di backup disattivate durante l'apertura dell'interfaccia utente dell'agente Linux
- Lo stato del processo, la cronologia del processo e il Registro attività non sono visibili

Impostazioni della destinazione di backup disattivate durante l'apertura dell'interfaccia utente dell'agente Linux

Se il server di backup di Linux non viene rimosso dalla Console di Arcserve UDP prima della disinstallazione della Console stessa, le impostazioni della destinazione di backup saranno disattivate durante l'apertura dell'interfaccia utente del server di backup.

Sintomo

Il server di backup non viene notificato circa la disinstallazione della Console di Arcserve UDP. Il server di backup suppone che sia ancora gestito dalla console.

Soluzione

Accedere al server di backup e immettere il seguente comando:

```
# /opt/Arcserve/d2dserver/bin/d2dreg --release
```

Il server di backup viene rilasciato dalla Console ed è quindi possibile modificare le impostazioni di backup dall'interfaccia utente del server di backup.

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Lo stato del processo, la cronologia del processo e il Registro attività non sono visibili

Sintomo

Non è possibile visualizzare lo stato del processo, la cronologia del processo e il registro attività per i nodi Linux della console Arcserve UDP.

Soluzione

Il server di backup Linux non è in grado di connettersi a Arcserve UDP mediante il nome host.

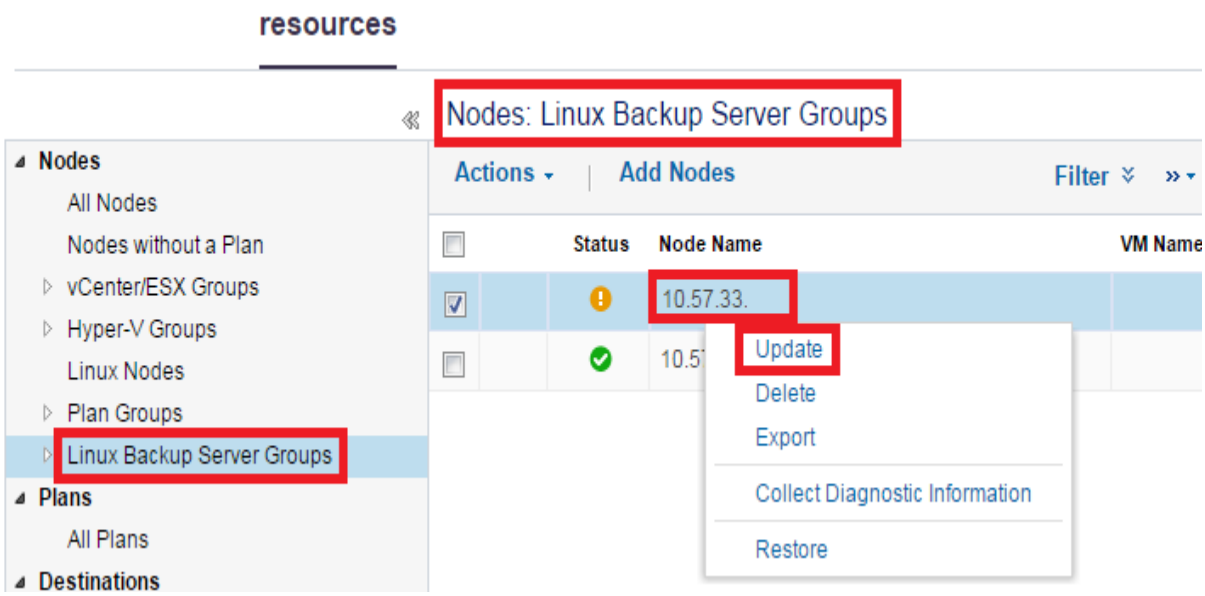
Effettuare le operazioni seguenti:

1. Creare il file server_ip.ini nel seguente percorso di Arcserve UDP:

   "UDP installation path"\Management\Configuration\server_ip.ini

2. Immettere l'indirizzo IP di Arcserve UDP nel file.
3. Accedere alla console Arcserve UDP e aggiornare il server di backup Linux e i nodi Linux.

   Nota: il server di backup Linux può essere aggiornato solamente da gruppi di server di backup Linux, in cui vengono elencati tutti i server di backup Linux.



Lo stato del processo, la cronologia del processo e il Registro attività sono visibili.

Non è possibile ripristinare il volume di sistema di SUSE15 con file system XFS

Il ripristino del volume di sistema di SUSE15 con file system XFS non è riuscito.

Sintomo

Non è possibile eseguire il processo di ripristino del nodo SUSE15 con file system XFS.

Soluzione

Il problema si verifica perché il volume di sistema non è stato montato. Creare un CD CentOS 7.5 Live e utilizzarlo per eseguire un ripristino bare metal standard o immediato.

Se il problema persiste, utilizzare la Chat in tempo reale per contattare il Supporto tecnico di Arcserve. La Chat in tempo reale consente di ottimizzare la comunicazione con il team del supporto tecnico per la risoluzione diretta di dubbi e problemi continuando a mantenere l'accesso al prodotto.

Problemi correlati al ripristino

In questa sezione verranno illustrati i seguenti argomenti sulla risoluzione dei problemi relativi al ripristino:

- Errore di ripristino dei file
- Aggiunta del database del contenuto ripristinato all'applicazione Web originale
- Impossibile eseguire il montaggio del database durante il ripristino del database di Microsoft Exchange
- Il campo Da non viene visualizzato correttamente nei messaggi di posta elettronica inviati dagli utenti che dispongono delle autorizzazioni per conto di altri per una casella di posta condivisa
- Processi di ripristino non riusciti dopo backup di integrazione leggeri

Errore di ripristino dei file

Sintomo

A causa di una limitazione di Microsoft, i dati dei file sui volumi di deduplicazione NTFS di un sistema Windows 2012 R2 non possono essere letti da un sistema Windows 2012. Di conseguenza, se l'agente UDP su un sistema Windows 2012 viene utilizzato per il ripristino di un computer virtuale con sistema operativo guest Windows 2012 R2 contenente i volumi di deduplicazione NTFS, è possibile che si verifiche il seguente problema. Il problema si verifica soltanto durante un'operazione di ripristino a livello di file o di montaggio del punto di ripristino.

Il file o la directory saranno corrotti o non leggibili.

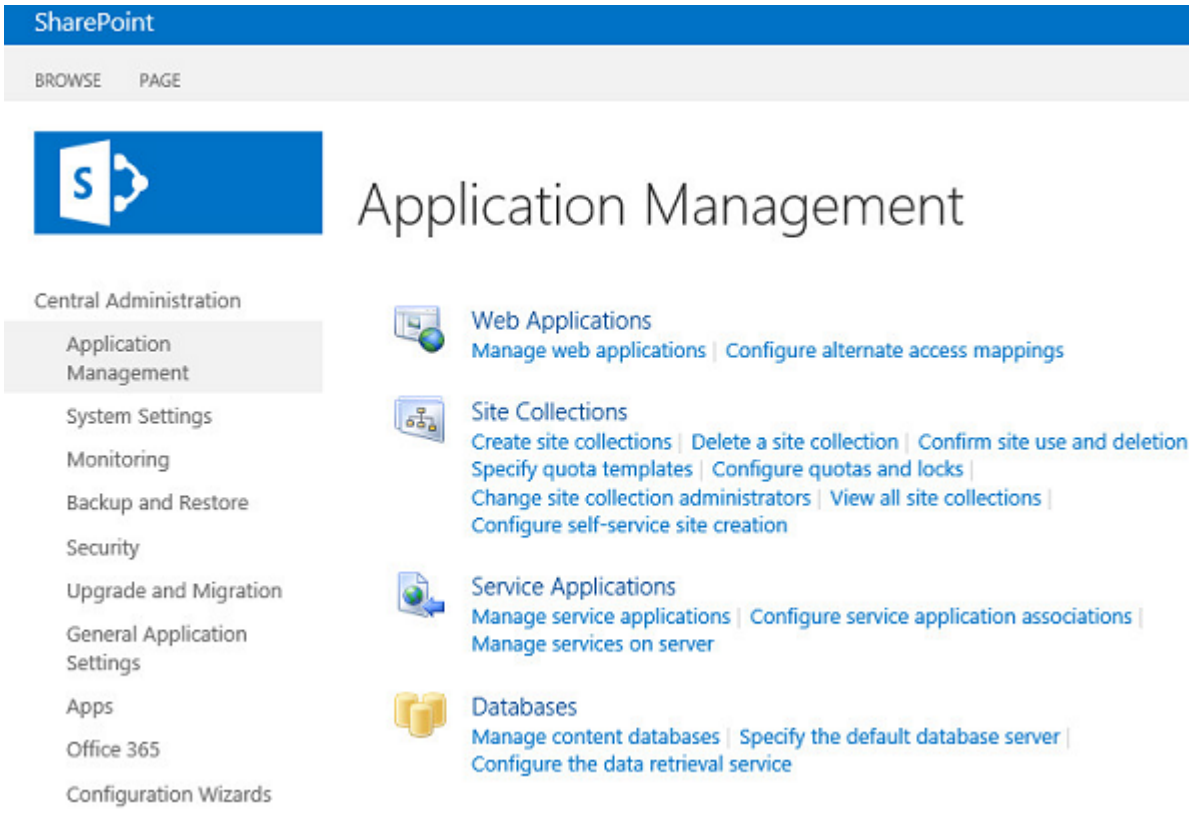
Soluzione

Se si verifica questo problema, avviare il processo di ripristino da un agente UDP installato su un sistema Windows 2012 R2.

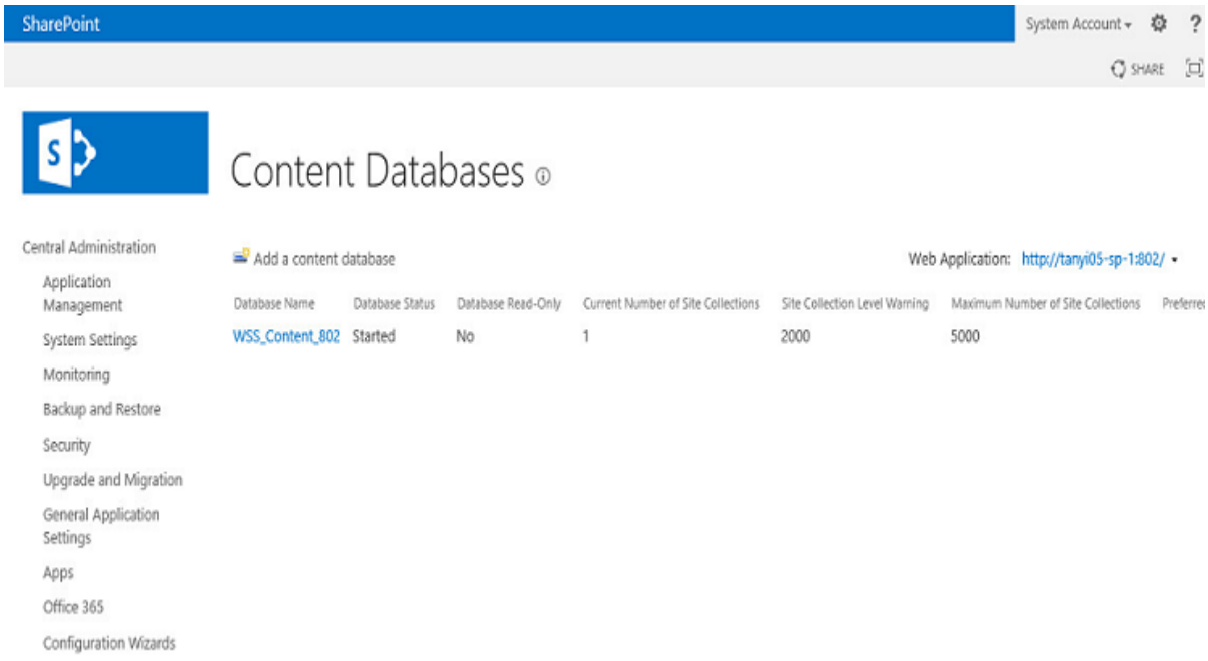
Aggiunta del database del contenuto ripristinato all'applicazione Web originale

Effettuare le operazioni seguenti:

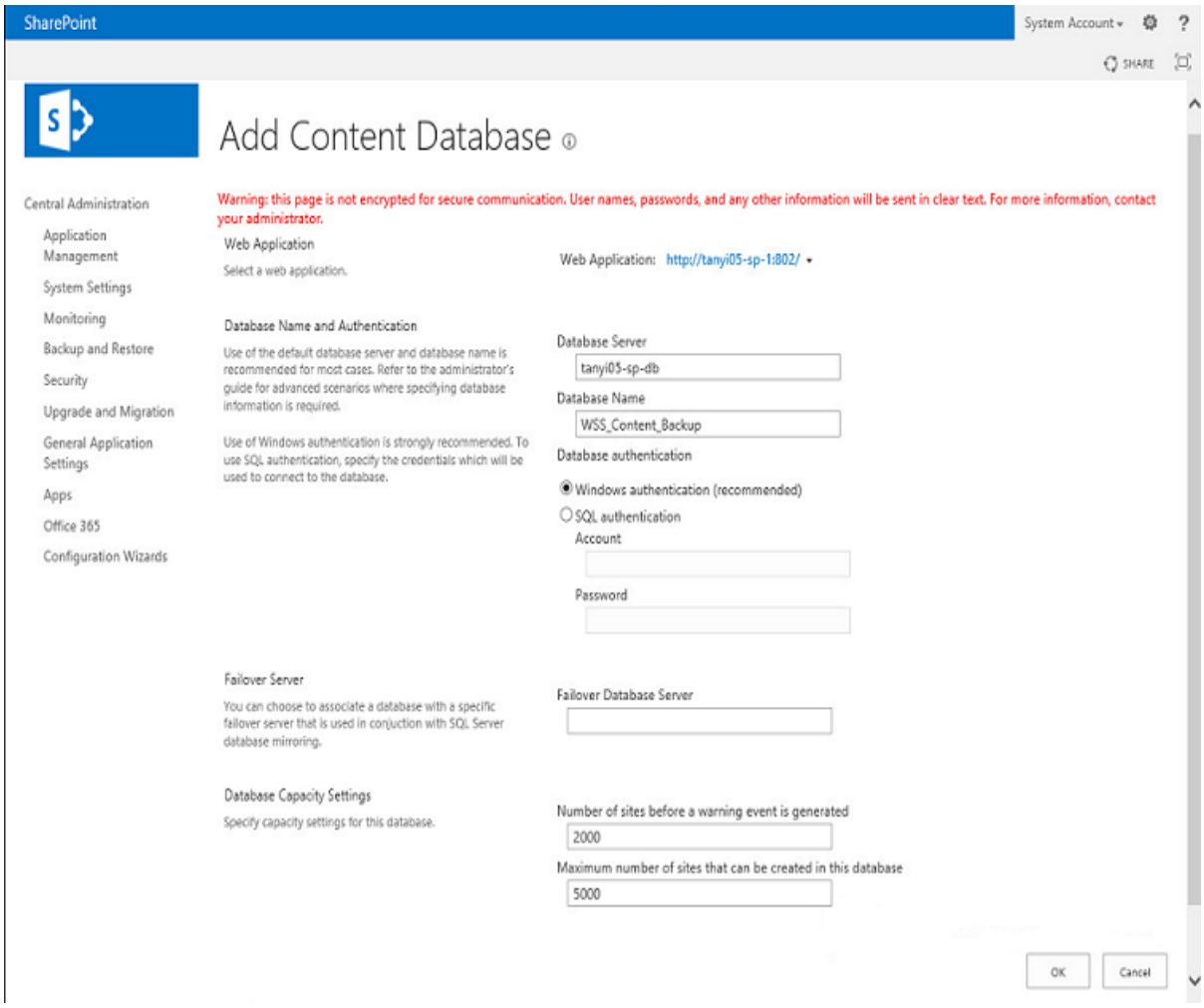
1. Aprire Amministrazione centrale SharePoint e selezionare Gestione applicazioni.



2. Selezionare i database del contenuto di gestione.



3. Selezionare l'applicazione Web e fare clic su Aggiungi database del contenuto.
4. Inserire i valori per il server di database e il nome del database (ad esempio, WSS_ Content_Backup), quindi fare clic su OK.



Il database del contenuto è stato associato all'applicazione Web originale.

Impossibile eseguire il montaggio del database durante il ripristino del database di Microsoft Exchange

Sintomo

Durante il ripristino di un database di Microsoft Exchange, non è possibile eseguire il montaggio del database. I registri necessari non sono presenti o i registri transazioni non sono contigui. Nel registro eventi sono presenti gli errori di evento 454, 455 e 2006.

L'errore di montaggio del database potrebbe essere causato dai due motivi seguenti:

Motivo 1: L'opzione di eliminazione del registro di Exchange è attivata nelle impostazioni di UDP e causa l'eliminazione dei registri transazioni dopo ogni backup. Quindi, l'utente tenta di ripristinare la sessione precedente dopo diversi backup in cui si è verificata l'eliminazione del registro.

Motivo 2: Gli utenti hanno eliminato manualmente i registri transazioni o i registri vengono eliminati da altri programmi come ad esempio il software antivirus.

Soluzione

Soluzione 1: Se è stata attivata l'opzione di eliminazione del registro di Exchange e i registri transazioni non sono contigui, ripristinare tutte le sessioni una alla volta, a partire dall'ultima, fino alla mancata riuscita del ripristino della sessione. Se il ripristino dell'ultima sessione non riesce, provare con la soluzione numero 2.

Soluzione 2: Se la soluzione numero 1 non funziona, provare con la soluzione numero 2. Questa soluzione consente di risolvere entrambi i problemi.

Ad esempio, si desidera ripristinare il database Test dalla sessione numero 1. Nella procedura riportata di seguito, Test è il nome del database.

1. Accedere all'Exchange Server su cui si trova il database.
2. Eliminare tutti i file (come *.edb, *.log, *.jrs, *.chk) dalla cartella del database.
3. Eseguire il montaggio del database per creare un database vuoto.

   Mount-Database -Identity Test
4. Ripristinare nuovamente la stessa sessione nella posizione originale.

   Se il ripristino viene eseguito correttamente, non è necessario seguire la procedura riportata di seguito. Se il ripristino non riesce, procedere come segue.
5. Ripetere il montaggio del database.

Mount-Database -Identity Test

6. Creare un database temporaneo.

   new-mailboxdatabase -name OtherDatabase

7. Spostare la casella di posta in un altro database.

   get-mailbox -datatbase Test -resultsize unlimited | new-moverequest -targetdatabase OtherDatabse

8. Rimuovere il database della casella di posta dal computer di destinazione.

   remove-mailboxdatabase -identity Test

9. Creare un database della casella di posta con lo stesso nome.

   new-mailboxdatabase -name Test

10. Ripristinare nuovamente la stessa sessione nella posizione originale.

    Il montaggio del database è stato eseguito correttamente.

Il campo Da non viene visualizzato correttamente nei messaggi di posta elettronica inviati dagli utenti che dispongono delle autorizzazioni per conto di altri per una casella di posta condivisa

Sintomo

Dopo il ripristino della posta di Exchange, le informazioni del campo "Da" non vengono visualizzate correttamente se il messaggio di posta elettronica viene inviato da un utente con privilegi "per conto di altri" per una casella di posta condivisa. Nel campo "Da" viene visualizzato solo il nome <mittente host>.

Soluzione

Per risolvere il problema, attenersi alla procedura seguente:

1. Eseguire una delle seguenti operazioni:

   Per il backup senza agente

   - Sul server proxy HBBU, creare un file grtcfg.ini nella cartella Configurazione:

     [product_installed_path]\ Engine\Configuration

   Per il backup basato su agente

   - Sul computer dell'agente, creare un file grtcfg.ini nella cartella Configurazione:

     [product_installed_path]\ Engine\Configuration

2. Aggiungere il contenuto seguente al file grtcfg.ini:

   [common]

   0xFF07_enable=1

3. Inoltrare nuovamente il processo di ripristino.

Processi di ripristino non riusciti dopo backup di integrazione leggeri

Sintomo

Quando si inviano backup di integrazione leggeri da Arcserve Backup Manager al nodo Exchange Online dal server RPS, il nodo ha già eseguito il backup con una sessione di copia su nastro. I processi hanno esito negativo quando i dati di origine includono sessioni Arcserve D2D precedentemente sottoposte a backup da Arcserve Backup. Nel Registro attività viene visualizzato il messaggio di errore AW0813.

Soluzione

Il comportamento della progettazione di Arcserve Backup è responsabile di questo comportamento. È necessario modificare questo comportamento per consentire ad Arcserve Backup di eseguire il backup delle sessioni Arcserve D2D precedentemente sottoposte a backup.

Effettuare le operazioni seguenti:

1. Dal server Arcserve D2D (nodo) di cui si sta eseguendo il backup, aprire l'editor del Registro di sistema Windows.
2. Aprire la seguente chiave:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\ClientAgent\Parameters\AllowRedundantD2DBackups
3. Modificare il valore DWORD di AllowRedundantD2DBackups in 1.

   Nota: se la chiave di registro non è presente nel nodo, è necessario creare tale chiave.
4. Chiudere l'editor del Registro di sistema di Windows.

   Per ulteriori informazioni, consultare l'articolo della Knowledge Base.

Modifica del nome del file in un elemento indesiderato causata dal ripristino sulla cartella NFS condivisa

Sintomo:

Quando viene eseguito un ripristino su una cartella NFS condivisa, i file e le cartelle vengono ripristinati con un nome indesiderato.

Soluzione:

UDP non supporta il ripristino di file e cartelle in una cartella NFS condivisa. Si consiglia di esportare una cartella Server Message Block (SMB) condivisa ed effettuare il ripristino sulla stessa cartella.

Nota: se il nome del file o della cartella viene convertito in un elemento indesiderato durante la sessione di backup NFS, anche in seguito al ripristino, il nome del file o della cartella resta un elemento indesiderato.

Problemi correlati a gateway, server RPS, archivio dati, console e database

In questa sezione verranno illustrati i seguenti argomenti sulla risoluzione dei problemi relativi a Recovery Point Server (RPS), archivio dati e database:

- Il nome dell'archivio dati è già in uso
- Impossibile connettersi all'archivio dati a causa di un problema DNS
- Passaggio dell'archivio dati alla modalità di solo ripristino
- Errore in caso di versione RPS precedente alla versione della console
- Aggiunta della stessa risorsa in siti diversi non supportata
- Abilitazione dei troncamenti di registro quando il database SQL è in modalità di ripristino Estesa
- Punti di ripristino disponibili non mostrati con Sfoglia punti di ripristino quando il server RPS è configurato con il nome FQDN
- Accesso negato durante l'aggiunta del server RPS
- Impossibile passare alla visualizzazione UDP per il punto di ripristino
- Errore di accesso negato durante l'aggiunta o l'aggiornamento dei nodi
- Errore di apertura della console UDP in caso di modifica della password dell'amministratore di SQL
- Impossibile montare i punti di ripristino a causa del timeout
- Aggiornamento delle credenziali del server gateway
- Aggiornamento del gateway in caso di modifica delle credenziali per il proxy gateway
- Messaggio Avvio del server di identità in corso mostrato nella console

Il nome dell'archivio dati è già in uso

Sintomo:

Quando si crea un archivio dati, a volte viene visualizzato il messaggio seguente anche se si specifica un nuovo nome per l'archivio dati:

Questo nome è già utilizzato da un altro archivio dati sul server. Specificare un nome diverso per l'archivio dati.

Soluzione:

Ciò si verifica quando si dispone di un archivio dati esistente ma per una ragione qualsiasi l'UUID dell'archivio dati nel Registro di sistema è corrotto. È possibile eliminare l'archivio dati dall'interfaccia utente grafica, ma il nome rimane nel Registro di sistema del server del punto di ripristino.

Per risolvere il problema, specificare un nuovo nome.

Impossibile connettersi all'archivio dati a causa di un problema DNS

Sintomo:

Durante il ripristino bare metal, non è possibile connettersi alla cartella condivisa presente nel server RPS. Anche se il nome utente e la password sono corretti, non è possibile accedere al nodo sul server RPS.

Soluzione:

Quando sul server RPS è abilitato il controllo UAC di Windows, anche un account compreso nel gruppo di amministratori locali potrebbe non riuscire ad accedere a una cartella condivisa dell'archivio dati se l'accesso alla condivisione non è stato consentito in modo esplicito.

Utilizzando il ruolo di amministratore integrato nel server RPS, concedere all'account utilizzato per il ripristino bare metal l'autorizzazione di accesso in lettura/scrittura alla cartella condivisa presente nell'archivio dati specificato.

Passaggio dell'archivio dati alla modalità di solo ripristino

Sintomo

Si rileva che un archivio dati è passato alla modalità di solo ripristino e non è pertanto possibile eseguire il backup dei dati.

Soluzione

Quando un disco utilizzato da un archivio dati rimane senza spazio su disco, l'archivio dati passa alla modalità di solo ripristino. Questa modalità consente di eseguire il ripristino dei dati ma senza backup sull'archivio dati. Inoltre, quando l'allocazione di memoria indicata è utilizzata completamente, aumentare l'allocazione di memoria o passare l'archivio dati dalla modalità di memoria alla modalità SSD. Anche in tali casi, l'archivio dati passa alla modalità di solo ripristino.

Per risolvere il problema, spostare l'archivio dati in un disco di dimensioni superiori mediante importazione.

Copiare le cartelle contenute nel disco pieno in un disco di dimensioni superiori con spazio libero, quindi importare l'archivio dati dalla console.

La funzionalità **Importa archivio dati** consente di aggiungere un archivio dati al Recovery Point Server. È possibile importare in un Recovery Point Server qualsiasi archivio dati esistente. Gli archivi dati eliminati in precedenza da un Recovery Point Server sono disponibili per l'importazione.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic sulla scheda **Risorse.**
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Recovery Point Server**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: Recovery Point Server**.
3. Eseguire una delle seguenti operazioni:
   - Fare clic su un Recovery Point Server.
   - Selezionare un Recovery Point Server e dal menu centrale fare clic sul menu a discesa **Azioni**.
4. Fare clic su **Importa archivio dati**.

   Viene visualizzata la pagina **Importa archivio dati**.
5. Selezionare le opzioni seguenti e fare clic su **Avanti**:

- **Sfogliare** per selezionare la **Cartella di destinazione del backup** in cui importare l'archivio dati.
- Immettere la **Password di crittografia**.

Nota: Lasciarla vuota se l'archivio dati non è crittografato.

Dopo avere autenticato la **Cartella di destinazione del backup**, la pagina **Importa archivio dati** mostra i dettagli dell'archivio dati.

6. Modificare i dettagli, se necessario, quindi fare clic su **Salva**.

   Se sono state copiate cartelle della Destinazione dati, Destinazione indice e della Destinazione hash per l'archivio dati di deduplicazione, sarà necessario modificare il percorso della cartella.

   Nota: Non è possibile abilitare o disabilitare l'opzione di crittografia per un archivio dati esistente.

   L'archivio dati viene aggiunto al Recovery Point Server e visualizzato nella finestra di dialogo **Destinations: Recovery Point Servers** (Destinazioni: Recovery Point Server).

   L'archivio dati è ora disponibile per il backup.

Errore in caso di versione RPS precedente alla versione della console

Sintomo

Esiste un piano con un'attività di backup o replica la cui destinazione è un Recovery Point Server (RPS). Il server RPS presenta una versione precedente, mentre la console è aggiornata alla versione più recente. Durante le operazioni di creazione, modifica, ridistribuzione, sospensione o ripresa di un piano, se sono presenti una o più versioni precedenti del server RPS, viene visualizzato l'errore seguente:

La versione del Recovery Point Server 'rps1' di destinazione è precedente alla versione della console corrente. Per continuare, è necessario aggiornare il Recovery Point Server.

Soluzione

Questo errore si verifica quando il piano utilizza una versione precedente del server RPS. Per risolvere l'errore, aggiornare il server RPS utilizzato nel piano. In caso di aggiornamento manuale del server RPS, senza console, ripetere l'aggiornamento tramite la console.

Aggiornare il server RPS nel seguente ordine di preferenza:

Eseguire la replica su un server RPS gestito in remoto (RPS3) > Attività di replica (RPS2) > Attività di backup (RPS1)

Aggiornare RPS3 per primo, quindi aggiornare RPS2. Infine aggiornare RPS1.

Attenersi ai seguenti passaggi per aggiornare la versione:

1. Dalla scheda **risorse**, accedere alla pagina Destinazioni: Recovery Point Server.
2. Selezionare il Recovery Point Server.
3. Fare clic con il pulsante destro del mouse e selezionare **Installa/Aggiorna Recovery Point Server**.
4. Fare clic su **OK**.

Attenersi ai seguenti passaggi per altri aggiornamenti:

1. Dalla scheda **risorse**, accedere a Destinazioni nel riquadro sinistro, quindi fare clic su Recovery Point Server.
2. Selezionare il Recovery Point Server.
3. Fare clic con il tasto destro del mouse e selezionare **Aggiorna**.
4. Fare clic su **OK**.

Aggiunta della stessa risorsa in siti diversi non supportata

Sintomo

Quando si aggiunge un archivio dati in un sito remoto, viene restituito il seguente messaggio di errore:

Cannot submit job for a Hyper-v VM or ESX VM (Impossibile inoltrare il processo per un computer virtuale Hyper-V o ESX)

Soluzione

L'errore si verifica perché la stessa risorsa è già presente in un altro sito (nodo, server RPS, server ASBU, server Hyper-V, server ESX, server proxy). Per risolvere l'errore, eliminare la risorsa da tutti i siti, quindi aggiungerla soltanto in un unico sito.

Abilitazione dei troncamenti di registro quando il database SQL è in modalità di ripristino Estesa

Sintomo

Se il database è in modalità Estesa e viene eseguito un backup completo del database, non è possibile troncare il registro di troncamento SQL.

Soluzione

Per risolvere questo problema, aggiungere un valore del Registro di sistema per consentire ad Arcserve UDP di eseguire il comando BACKUP LOG per eseguire il backup del registro transazioni. Questo comando contrassegna lo spazio, già scritto nel file di database, come riutilizzabile.

Per aggiungere il valore del Registro di sistema, attenersi alla procedura seguente:

1. Aprire l'editor della tabella del Registro di sistema sul computer dell'agente utilizzando il comando seguente:

   ```
   regedit
   ```

2. Accedere alle seguenti chiavi a seconda del tipo di backup: basato su agente o senza agente:

   Per il backup basato su agente per sistemi operativi a 32 bit e a 64 bit, individuare la chiave seguente nel computer dell'agente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Se si utilizza una versione precedente a Arcserve UDP v6.5 Aggiornamento 2, per il backup senza agente accedere alla chiave seguente. Creare il valore di tabella del Registro di sistema nel computer virtuale che si desidera sottoporre a backup sul server proxy. Se la chiave della tabella del Registro di sistema non è disponibile, creare il percorso completo della chiave.

   - **Sistema operativo a 32 bit:**

     HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   - **Sistema operativo a 64 bit:**

     HKEY_LOCAL_MACHINE\SOFTWARE\WoW6432Node\Arcserve\Unified Data Protection\Engine\AFBackupDll

3. Creare i due valori seguenti per il Registro di sistema e impostare entrambi su 1:

- valore dword denominato BackupSQLLog4Purge
- valore dword denominato ForceShrinkSQLLog

  Il valore del Registro di sistema è stato aggiunto.

La soluzione è attiva alla successiva esecuzione del processo di eliminazione.

Punti di ripristino disponibili non mostrati con Sfoglia punti di ripristino quando il server RPS è configurato con il nome FQDN

Valido per i sistemi operativi Windows

Sintomo

Se il server RPS non è compreso in un dominio di cui si è configurato il nome FQDN (aggiungendo il suffisso DNS) nella console UDP, l'opzione Sfoglia punti di ripristino non mostra un risultato preciso. Anche se si esegue il backup di alcune sessioni nel server RPS, il numero dei punti di ripristino mostrato è pari a zero.

Poiché il server RPS non è compreso in un dominio, non è in grado di identificarsi utilizzando il nome FQDN.

Soluzione

Per risolvere il problema, aggiungere il suffisso DNS all'host RPS.

Effettuare le operazioni seguenti:

1. Aprire il pannello di controllo e accedere a **Sistema e sicurezza**, **Sistema**.
2. Fare clic su **Cambia impostazioni** per le impostazioni Nome computer, Dominio e Gruppo di lavoro.

   Viene visualizzata la finestra di dialogo Proprietà del sistema.
3. Nella scheda **Nome computer**, fare clic su **Cambia**.

   Viene visualizzata la finestra di dialogo **Cambiamenti dominio/nome computer**.
4. Fare clic su **Altro**.

   Viene visualizzata la finestra di dialogo **Suffisso DNS e nome NetBIOS del computer**.
5. Nel campo Suffisso DNS primario del computer, aggiungere il suffisso DNS di rete e fare clic su **OK**.

   Ad esempio, aggiungere ABC.com.
6. Riavviare il sistema.

Accesso negato durante l'aggiunta del server RPS

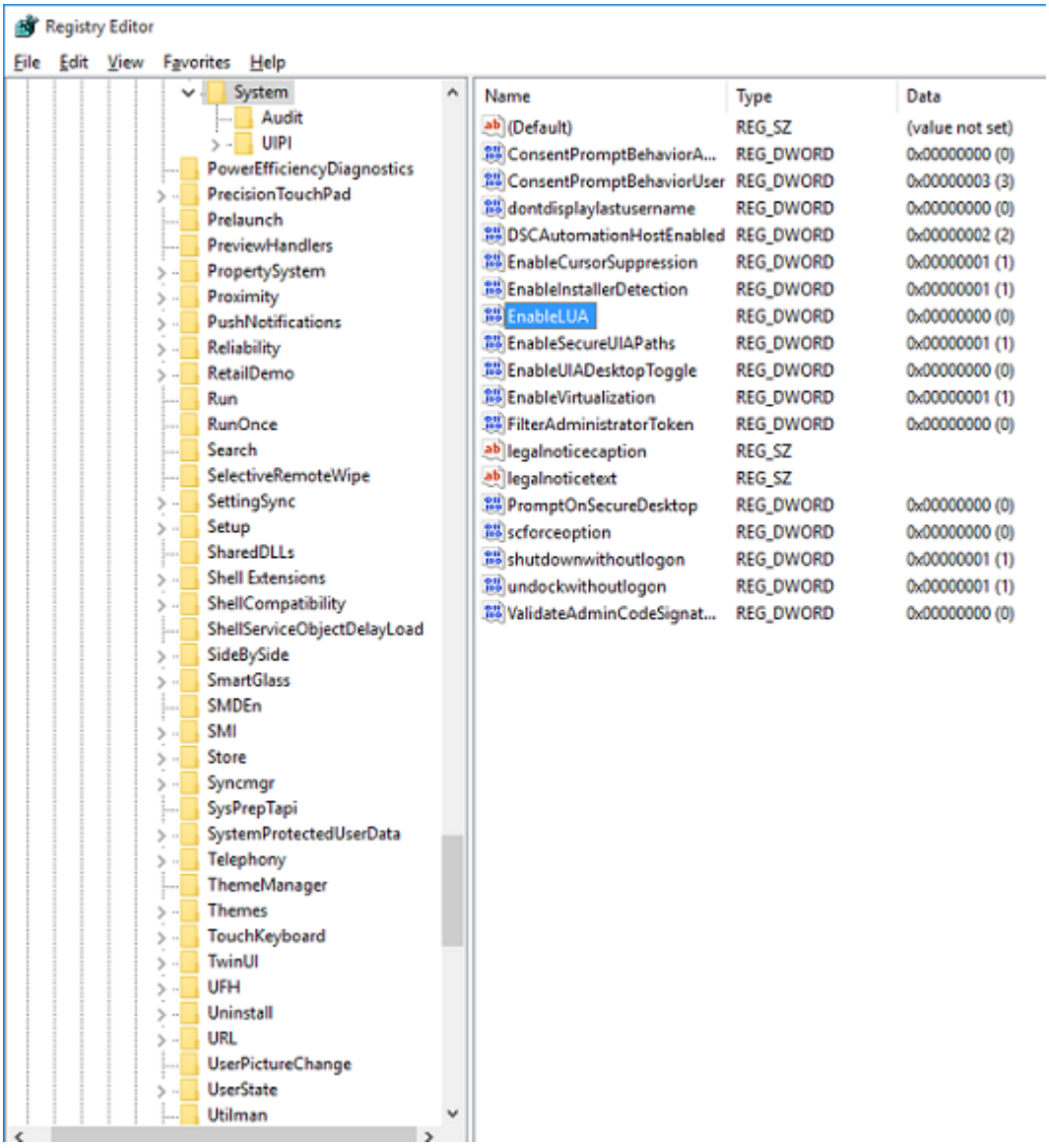
Sintomo:

Se si aggiunge Windows 10 come server RPS e l'account utente remoto non è in esecuzione, viene visualizzato un messaggio di errore:

Accesso negato. L'account potrebbe non disporre dei privilegi di amministratore o trattarsi di account di amministratore non integrato con il controllo UAC attivato.

Soluzione:

Per Windows 10, per disattivare l'account utente remoto, modificare il valore della chiave di registro non solo modificando il livello su "Non notificare mai" nel Pannello di controllo, ma anche in base al diagramma del registro di sistema indicato di seguito.



Impostare il registro di sistema "EnableLUA" su 0 per disabilitare l'UAC completamente e riavviare il computer.

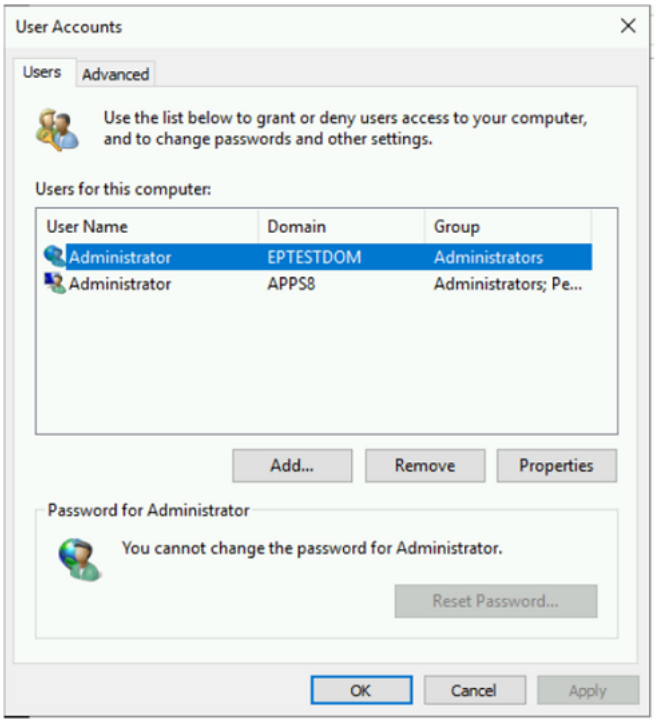
Aggiungere quindi Windows 10 come server RPS nella Console.

Assegnazione di privilegi e ruoli di amministratore a un utente di dominio

In questa sezione vengono fornite informazioni su come assegnare privilegi e ruoli di amministratore a un utente di dominio.

Effettuare le operazioni seguenti:

1. Per configurare il computer della console UDP per il dominio, utilizzare le credenziali di accesso dell'amministratore.
2. Assicurarsi che l'utente del dominio faccia parte del gruppo di amministratori. Per aggiungere un utente al gruppo di amministratori, nella finestra Account utente fare clic sul pulsante **Aggiungi**.



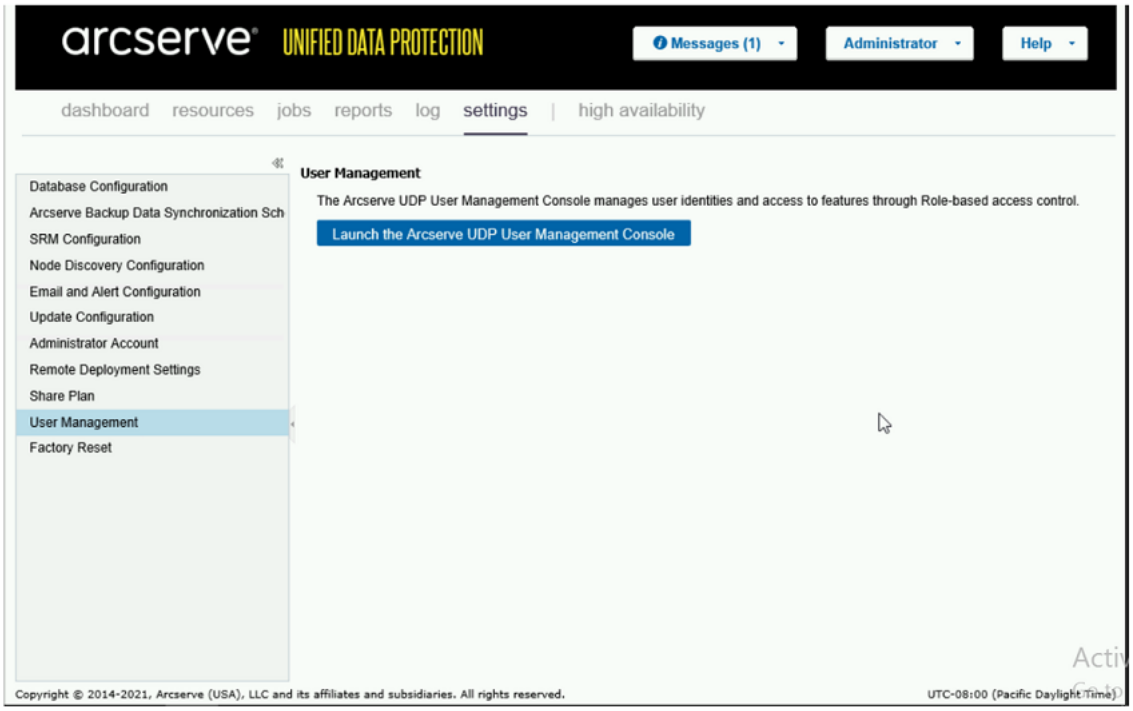
3. Dopo aver aggiunto l'utente al gruppo di amministratori, riavviare il servizio di gestione.
4. Per aggiungere il ruolo di amministratore a un utente di dominio mediante la Console di gestione utenti di Arcserve UDP, procedere come segue:

a. Accedere alla console Arcserve UDP utilizzando le credenziali di amministratore.

b. Fare clic sulla scheda **Impostazioni**.

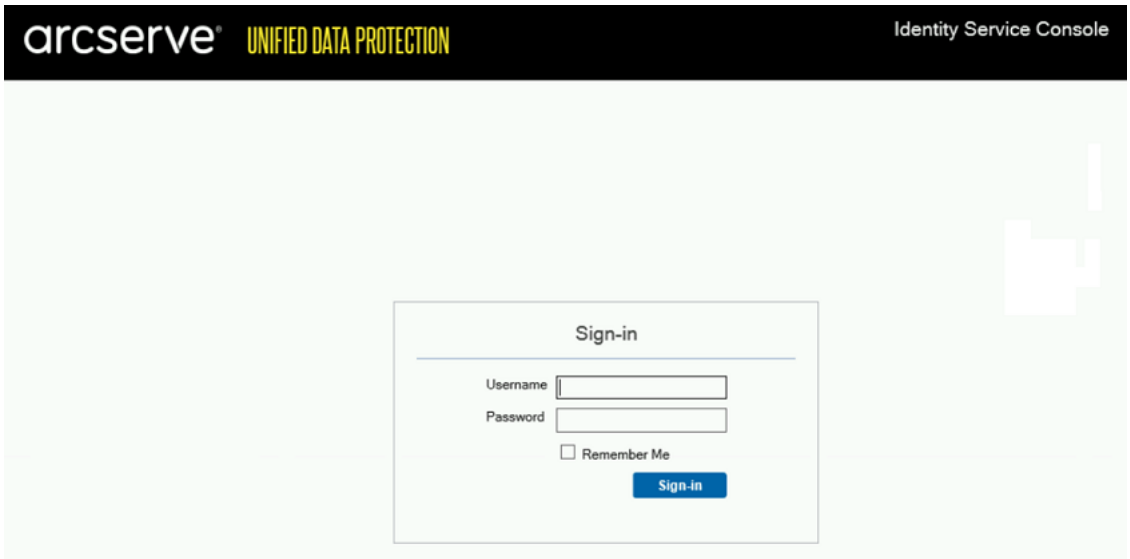
c. Dal riquadro sinistro, fare clic su **Gestione utenti**.

   Viene visualizzata la pagina Gestione utenti.



d. Fare clic sul pulsante **Avvia Console di gestione utenti Arcserve UDP**.

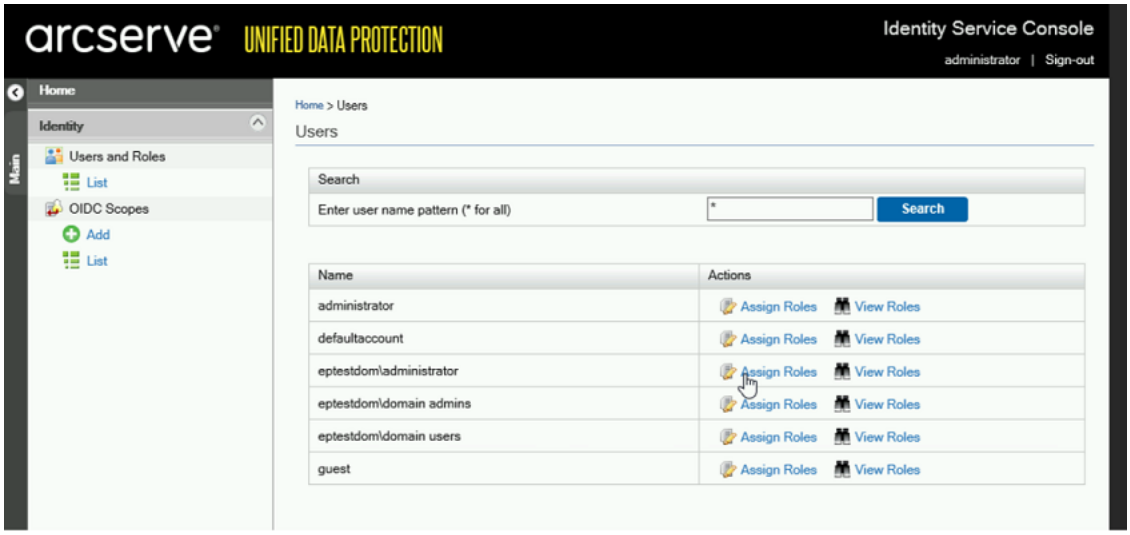
   La console del servizio identità viene visualizzata in una nuova finestra.



e. Fornire le credenziali di amministratore, quali nome utente e password, quindi fare clic su **Accedi**.

   Viene visualizzata la pagina principale Console servizio identità.

f. Accedere alla pagina **Utenti**, quindi da un elenco di utenti selezionarne uno e fare clic su **Assegna ruoli** per applicare le autorizzazioni di amministratore.



g. Accedere alla console UDP utilizzando le credenziali de dominio.

Impossibile passare alla visualizzazione UDP per il punto di ripristino

Sintomo:

Quando si passa alla visualizzazione UDP per il punto di ripristino RPS, a volte vengono restituiti messaggi di errore, ad esempio relativi all'accesso negato.

Soluzione:

Disabilitare il controllo UAC per risolvere il problema. Per ulteriori informazioni, consultare la sezione Disattivazione di un account utente remoto per un amministratore non integrato.

Errore di accesso negato durante l'aggiunta o l'aggiornamento dei nodi

Valido per i sistemi operativi Windows

Sintomo

A volte, durante l'aggiunta o l'aggiornamento di nodi, viene visualizzato il seguente errore:

Accesso negato. L'account potrebbe non disporre dei privilegi di amministratore o trattarsi di account di amministratore non integrato con il controllo UAC attivato.

Soluzione

Questo errore si verifica negli scenari seguenti:

- È stato eseguito l'accesso come utente locale o utente di dominio non incluso nel gruppo di amministratori locali del nodo da aggiungere o aggiornare.
- È stato eseguito l'accesso come utente compreso nei gruppi di amministratori locali del nodo, ma si dispone di un account di amministratore non integrato del nodo da aggiungere o aggiornare.

Per risolvere il problema, attenersi alla procedura seguente:

1. Aggiungere l'utente locale o di dominio ai gruppi di amministratori locali del nodo.
2. Disabilitare il controllo UAC del nodo.

   Per disabilitare il controllo UAC, attenersi alla procedura seguente:

   a. Fare clic su Start, digitare regedit nel campo Cerca programmi e file e premere Invio.

   b. Viene visualizzato l'editor del Registro di sistema di Windows.

      Nota: Potrebbe essere necessario fornire le credenziali di amministratore per accedere all'editor del Registro di sistema di Windows.

   c. Individuare e fare clic sulla chiave di registro seguente:

      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

   d. Dal menu Modifica, fare clic su Nuovo e selezionare il valore DWORD (32 bit).

   e. Specificare LocalAccountTokenFilterPolicy come nome della nuova voce e premere Invio.

f. Fare clic con il pulsante destro del mouse su LocalAccountTokenFilterPolicy, quindi selezionare Modifica.

g. Specificare 1 nel campo Dati valore e fare clic su OK.

h. Uscire dall'editor del Registro di sistema.

Note:

- Questa procedura non è analoga a quella per disabilitare il controllo UAC. Permette di disabilitare soltanto alcune funzionalità UAC.
- Poiché viene utilizzata la tecnologia WMI remota per l'importazione, verificare che non sia bloccata dal firewall.

Per ulteriori informazioni sul comportamento di Windows, consultare la documentazione di Microsoft.

Errore di apertura della console UDP in caso di modifica della password dell'amministratore di SQL

Sintomo:

La Console Arcserve UDP utilizza SQL server come database e l'amministratore SQL "sa" per la connessione al database. In caso di modifica della password "sa", la pagina principale della console non viene aperta restituendo il seguente messaggio:

SQL Server non è attualmente disponibile. Verificare lo stato del servizio, quindi riavviare il servizio di gestione Arcserve UDP.

Soluzione:

1. Eseguire <homedir>\Management\BIN\DBAccountUpdate.bat
2. Digitare updatePassword.
3. Digitare la nuova password e premere Invio.

Impossibile montare i punti di ripristino a causa del timeout

Sintomo

Quando il server RPS presenta un carico di lavoro eccessivo, il sistema operativo richiede più tempo per associare il volume montato, producendo un errore dei punti di ripristino di montaggio. Nei registri attività viene riportato il seguente messaggio:

Il montaggio del volume richiede più tempo del previsto (2 minuti). Questo errore si può verificare in caso di carico di lavoro eccessivo del server. Riprovare quando il carico del server è minore o consultare le istruzioni di risoluzione dei problemi nella documentazione in linea per aumentare il valore di timeout.

Soluzione

Per risolvere il problema, aumentare il valore di timeout.

Effettuare le operazioni seguenti:

1. Accedere al server RPS, quindi passare al percorso seguente:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFStorHBAMgmt
   ```

   ```
   "WaitDeviceReadyTimeoutS"=dword:00000078
   ```

   Impostazione predefinita: 120 secondi

2. Modificare il valore di timeout con uno più alto.

   Ad esempio, cambiare il valore di timeout in 600 secondi (10 minuti).

Aggiornamento delle credenziali del server gateway

Sintomo

Se è stato modificato il nome utente o è scaduta la password per l'installazione del gateway, durante la distribuzione del piano viene restituito il seguente messaggio di errore:

Distribuzione dell'agente non riuscita.

Impossibile rappresentare l'utente che ha installato il gateway di gestione remota Arcserve mediante le credenziali memorizzate. Verificare se le credenziali sono ancora valide e ripetere la distribuzione.

Soluzione

Per risolvere il problema, aggiornare il nome utente o la password dell'account del gateway.

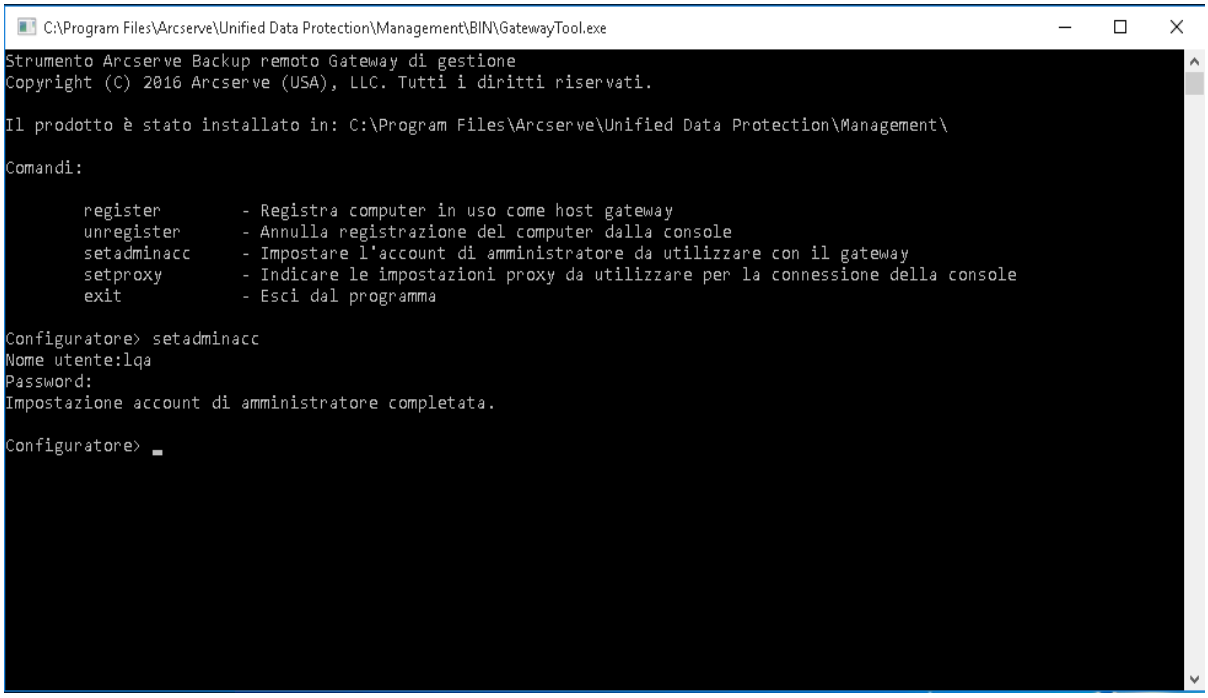
Effettuare le operazioni seguenti:

1. Accedere al server gateway.
2. Accedere alla cartella BIN nella directory di installazione di Arcserve UDP.

   Ad esempio, C:\Programmi\Arcserve\Unified Data Protection\Management\BIN\GatewayTool.exe
3. Fare clic con il pulsante destro del mouse su GatewayTool.exe, quindi fare clic su Esegui come amministratore.
4. Nella finestra del prompt dei comandi, digitare **setadminacc**.
5. Specificare il nuovo nome utente.
6. Specificare la nuova password.

   Se i dettagli sono corretti, viene visualizzato il messaggio seguente:

   ```
   Impostazione account di amministratore completata.
   ```



7. Ridistribuire il piano.

Aggiornamento del gateway in caso di modifica delle credenziali per il proxy gateway

Sintomo

Se si modificano le credenziali del server proxy, la connessione al gateway viene interrotta. Durante la connessione al gateway viene restituito il seguente messaggio di errore:

Impossibile contattare il gateway del sito proxy. Controllare lo stato del sito e verificare che il gateway sia in esecuzione.

Soluzione

Per risolvere il problema, aggiornare i parametri setproxy in GatewayTool.exe.

Per aggiornare il server gateway, attenersi alla procedura seguente:

1. Accedere al server gateway.
2. Accedere alla cartella BIN nella directory di installazione di Arcserve UDP.

   Ad esempio, C:\Programmi\Arcserve\Unified Data Protection\Management\BIN\GatewayTool.exe
3. Fare clic con il pulsante destro del mouse su GatewayTool.exe, quindi fare clic su Esegui come amministratore.
4. Nella finestra del prompt dei comandi, digitare **setproxy**.
5. Digitare **2** per selezionare Proxy personalizzato perché il proxy di Internet Explorer non supporta le credenziali al momento.
6. Specificare l'indirizzo IP del server proxy.
7. Specificare la porta del server proxy.
8. Digitare **Y** per l'autenticazione.

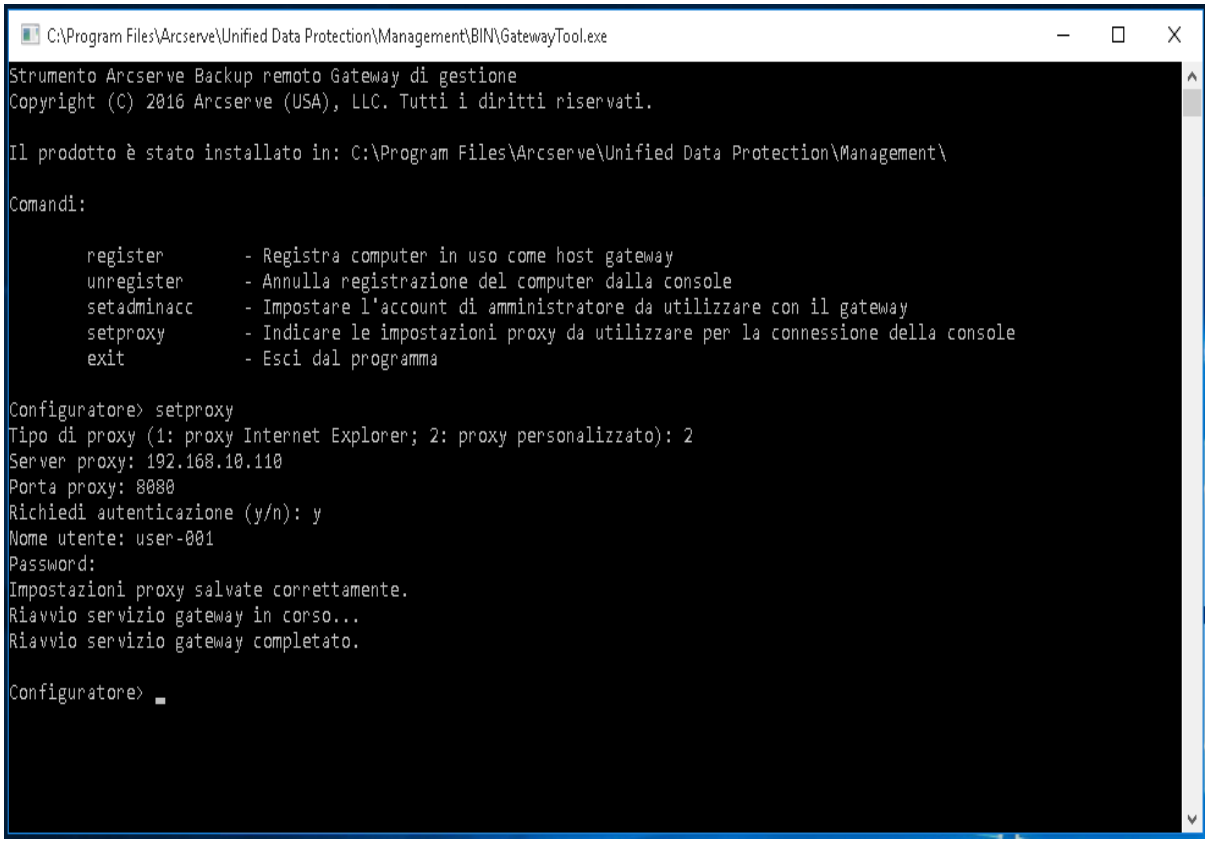
   Nota: Se si digita N, si indica di disabilitare le credenziali.
9. Specificare il nuovo nome utente.
10. Specificare la nuova password.

    Se i dettagli sono corretti, viene visualizzato il messaggio seguente:

    ```
    Le impostazioni proxy sono state salvate correttamente. Riavviare il servizio gateway.
    ```

    Nota: Se le credenziali del proxy gateway sono abilitate in un piano, aggiornare il nome utente e la password del proxy in tale piano.

Allo stesso modo, è possibile modificare le altre impostazioni quali il tipo di proxy, l'indirizzo IP e il numero di porta in **setproxy**.



Se viene visualizzato il messaggio **Impossibile riavviare il servizio gateway. Riavviarlo manualmente** nella finestra prompt dei comandi, procedere come segue:

a. Eseguire **services.msc** per cercare il **servizio gateway di gestione remota Arcserve**, quindi riavviare tale servizio.

b. Se il servizio remoto si interrompe dopo il riavvio, utilizzare Gestione attività per terminare l'attività **tomcat8.exe** manualmente.

c. Aggiornare **services.msc** e riavviare il **servizio gateway di gestione remota Arcserve**.

Messaggio "Avvio del server di identità in corso" mostrato nella console

Sintomo

Impossibile accedere alla console Arcserve UDP. Nella console viene visualizzato il messaggio seguente anche dopo cinque minuti dall'accesso:

Identity Service is starting (Avvio del servizio di identità in corso)

Soluzione

Per risolvere questo problema, aprire la console del servizio Windows e riavviare il servizio della console di Arcserve UDP, ovvero il **servizio di gestione di Arcserve UDP**.

Problemi correlati a backup e ripristino del computer virtuale

In questa sezione verranno illustrati i seguenti argomenti sulla risoluzione dei problemi relativi a Recovery Point Server (RPS), archivio dati e database:

- Aggiunta delle autorizzazioni per VDDK a livello del server vCenter
- Processo di backup per il modello di computer virtuale convertito sempre in backup completo
- Dischi indipendenti ignorati dal processo di backup del modello di computer virtuale
- Processo di backup per computer virtuale su condivisione SMB 3.0 non riuscito con messaggio di errore
- Processo di ripristino per computer virtuale non riuscito in caso di ripristino del computer virtuale su una condivisione di file predefinita di Windows
- Informazioni sul volume non disponibili per il punto di ripristino
- Autorizzazioni per il backup senza agente basato su host e Virtual Standby a livello del server vCenter
- Conversione del backup incrementale in backup di verifica in quanto le snapshot del computer virtuale sono state modificate dopo l'ultimo processo di backup o richiedono il consolidamento
- Errore del backup senza agente per computer virtuale VMware per una periferica CD/DVD del computer virtuale
- Backup senza agente basato su host per Hyper-V non riuscito dopo l'aggiornamento di Arcserve UDP
- Errore del backup senza agente basato su host in VMware ESXi 6.0
- Impossibile creare una snapshot per computer virtuali Hyper-V quando sono in esecuzione più processi
- Impossibile eseguire il backup del disco virtuale. Errore di sistema=[La periferica non è pronta(21)]
- Errore del processo di backup
- Errore di importazione dei computer virtuali VMware da vCenter
- Errore di applicazione delle impostazioni di backup a un nodo
- Backup non riusciti a causa della licenza ESXi

- Modalità di trasporto HotAdd non utilizzata dal backup senza agente basato su host
- Modalità di trasporto HotAdd non funzionante durante il backup di un computer virtuale VMware
- Modalità di trasporto NBD o NBDSSL utilizzata dal processo di backup o ripristino senza agente basato su host anche quando è disponibile la modalità SAN
- Controllo più granulare per VSS su un sistema operativo guest Windows disattivato
- Errore delle operazioni di recupero durante il recupero dei dati mediante la modalità di trasporto HotAdd o SAN
- Operazione di recupero del computer virtuale non riuscita se è selezionata una porta non predefinita
- Errori del processo di backup incrementale o completo pianificato per il computer virtuale Hyper-V
- Errore del writer Hyper-V VSS NTDS durante l'acquisizione di snapshot VSS nel computer virtuale
- Le modifiche all'indirizzo MAC non vengono memorizzate dopo il ripristino del computer virtuale
- Snapshot VSS non creata con Hyper-V
- Impossibile aprire i file VMDK
- Problemi causati da UUID duplicati del computer virtuale
- Errore del processo di catalogo file system o della verifica del punto di ripristino per il backup senza agente basato su host
- Conversione del backup incrementale per verificare il backup o aumento delle dimensioni di backup in Hyper-V
- Backup senza agente basato su host non riuscito per un computer virtuale Hyper-V con una speciale configurazione del disco di differenziazione
- Backup Job Fails for a VMware Virtual Machine (Il processo di backup non riesce per un computer virtuale VMware)
- Ripetizione analisi disabilitata per le schede HBA quando l'origine e il proxy si trovano in server VMware ESX diversi
- Creazione di snapshot consecutive disabilitata in un computer virtuale VMware per il backup

- Arresto anomalo del backup senza agente basato su host quando si utilizza Windows 2003 R2 a 64 bit come proxy di backup
- Blocco in fase di avvio del computer virtuale in seguito al ripristino da una versione successiva dell'host ESXi a una versione precedente dell'host ESXi
- RAM utilizzata al 99% durante l'inoltro dei processi di backup al computer virtuale
- Errore del processo di ripristino Hyper-V. Errore di connessione dell'utilità sull'host
- Errore della protezione automatica durante il rilevamento e la protezione del computer virtuale
- Impostazione della dimensione del blocco di lettura durante il backup del file VMDK

Aggiunta delle autorizzazioni per VDDK a livello del server vCenter

Se non si dispone delle autorizzazioni appropriate, il processo di backup per un computer virtuale basato su host e il processo Virtual Standby non vengono completati.

Per risolvere questo problema, verificare di disporre delle autorizzazioni appropriate. Pe gli utenti di vCenter non è necessario disporre dell'autorizzazione di amministratore a livello del server vCenter, ma è sufficiente disporre di un'autorizzazione di amministratore a livello del datacenter. Inoltre, è necessario disporre delle autorizzazioni seguenti a livello di server vCenter:

- Global, DisableMethods and EnableMethods
- Global, License

Per ulteriori informazioni, consultare l'articolo della Knowledge Base di VMware.

Per ulteriori informazioni sulle autorizzazioni, consultare la sezione Autorizzazioni per il backup senza agente basato su host e Virtual Standby a livello del server vCenter.

Autorizzazioni per il backup senza agente basato su host e Virtual Standby a livello del server vCenter

Quando vCenter viene configurato per la gestione di computer virtuali, nella maggior parte delle occasioni gli utenti e i gruppi vengono configurati con i privilegi di amministrazione di vCenter. Questo approccio garantisce che gli account di vCenter abbiano accesso illimitato alle funzionalità e alle attività vCenter. È inoltre possibile creare utenti e gruppi vCenter e gruppi per facilitare soltanto le operazioni di backup o le operazioni di backup e ripristino.

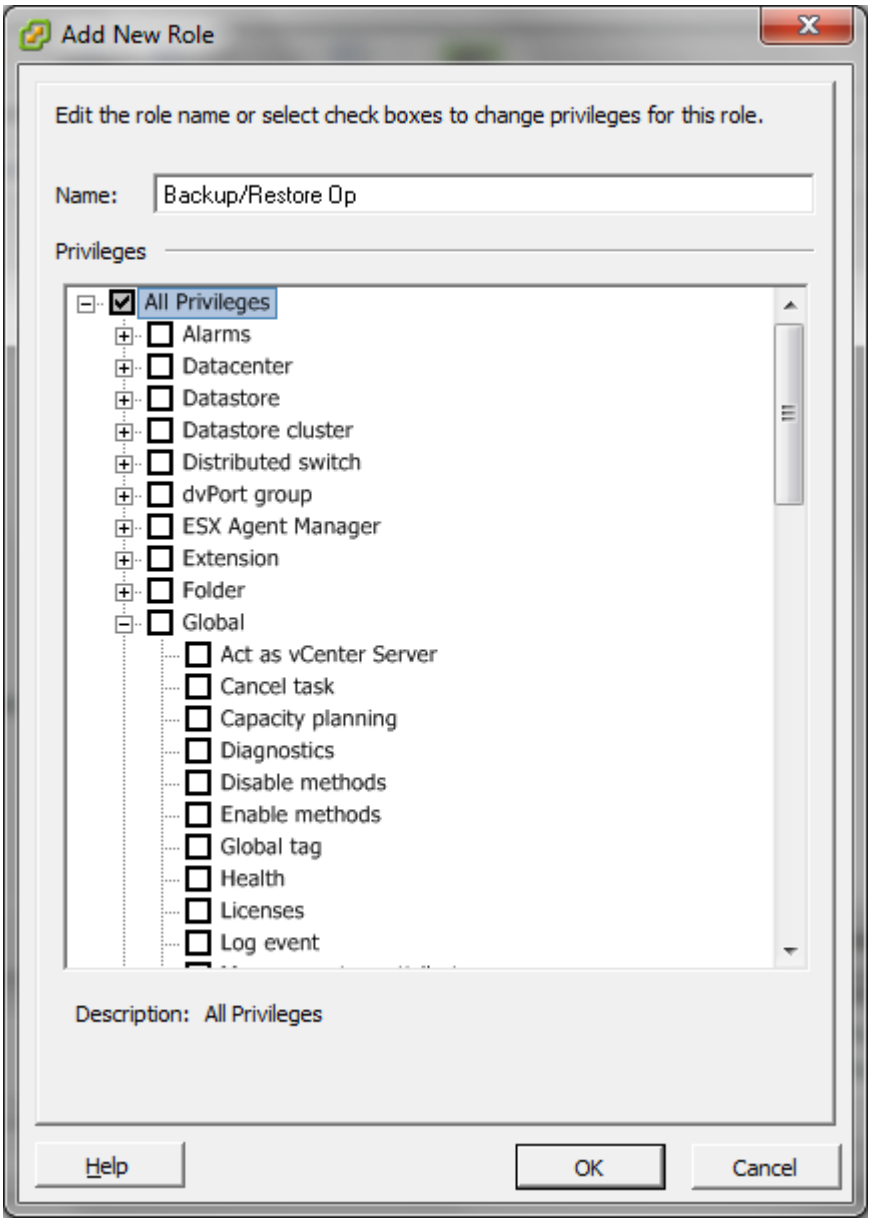
Quando si utilizzano account vCenter non amministrativi per facilitare le operazioni di backup e ripristino, vengono creati dei ruoli vCenter e assegnati i privilegi a tali ruoli che verranno applicati a utenti singoli o a gruppi.

Nota: Come procedura consigliata, VMware suggerisce di consentire agli account utente vCenter non amministrativi di essere membri del gruppo degli amministratori locali di Windows.

Importante! Le fasi seguenti suppongono che l'utente disponga delle conoscenze necessarie per la configurazione di utenti, gruppi, ruoli e autorizzazioni di vCenter. Consultare la documentazione di vCenter per qualsiasi riferimento.

Effettuare le operazioni seguenti:

1. Accedere a vCenter mediante il client VI.
2. Aprire la finestra di dialogo Add New Roles e specificare il nome del ruolo.



3. Espandere All privileges.
4. **(Facoltativo)** per consentire al ruolo di **facilitare solamente le operazioni di backup**, specificare i privilegi seguenti:

   Importante! Per consentire al ruolo di facilitare le operazioni di backup e ripristino, passare alla fase successiva.

   - Espandere Virtual Machine e Configuration, quindi specificare i seguenti privilegi:
     - Rilevamento delle modifiche del disco
     - Lease del disco
     - Aggiunta di un disco esistente

- Aggiunta di un nuovo disco
- Aggiunta o rimozione di un dispositivo
- Modificare risorsa
- Rimozione del disco
- Impostazioni

- Espandere Virtual Machine e Provisioning, quindi specificare i seguenti privilegi:
  - Consentire l'accesso di sola lettura al disco
  - Consentire il download nel computer virtuale
- Espandere Virtual Machine e specificare i seguenti privilegi:

  vSphere 4: Espandere State e specificare Create Snapshot e Remove snapshot.

  vSphere 5: Espandere Snapshot management, espandere State e specificare Create Snapshot e Remove snapshot.
- Espandere Global e specificare i seguenti privilegi:
  - Disattivare metodi
  - Attivare metodi
  - Licenze

  Andare al passaggio 6.

5. Per consentire al ruolo di **facilitare le operazioni di backup,** specificare i privilegi seguenti:
   - Espandere Datastore e specificare i seguenti privilegi:
     - Allocare spazio
     - Sfogliare l'archivio dati
     - Operazioni file di basso livello
   - Espandere Global e specificare i seguenti privilegi:
     - Disattivare metodi
     - Attivare metodi
     - Licenze
   - Espandere Host, espandere Local Operations e specificare Reconfigure virtual machine.

Nota: Questo privilegio è richiesto soltanto quando è necessario eseguire operazioni di backup e ripristino mediante la modalità di trasporto HotAdd.

- Espandere Network e specificare Assign Network.
- Espandere Resource e fare clic su Assign Virtual Machine to resource pool.
- Espandere Virtual Machine e Configuration, quindi specificare i seguenti privilegi:
  - Aggiunta di un disco esistente
  - Aggiunta di un nuovo disco
  - Aggiunta o rimozione di un dispositivo
  - Avanzato
  - Modifica del numero di CPU
  - Modificare risorsa
  - Rilevamento delle modifiche del disco
  - Lease del disco
  - Periferica USB host
  - Memoria
  - Modifica impostazione periferica
  - Periferica non formattata
  - Ricarica dal percorso
  - Rimozione del disco
  - Rinomina
  - Ripristino informazioni guest
  - Impostazioni
  - Posizionamento swapfile
  - Aggiornamento hardware virtuale
- Espandere Virtual Machine e Guest Operations, quindi specificare i seguenti privilegi:
  - Modifiche a operazione guest
  - Esecuzione del programma di operazione guest
  - Query dell'operazione guest (vSphere 5)
- Espandere Virtual Machine e Interaction, quindi specificare i seguenti privilegi:

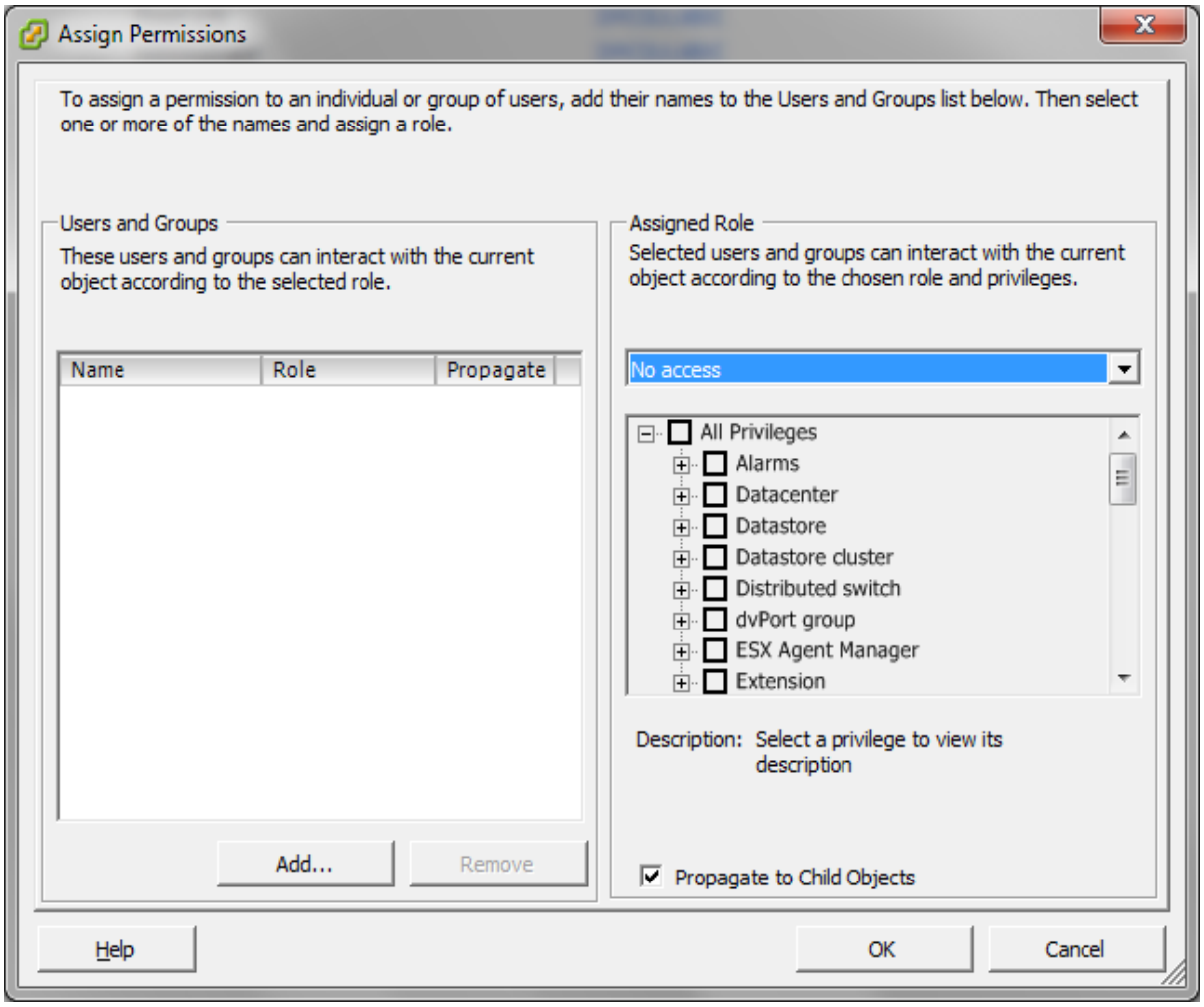
- Disattiva
- Attiva

- Espandere Virtual Machine e Inventory, quindi specificare i seguenti privilegi:
  - Creazione nuovo
  - Registrarla
  - Rimuovi
  - Annullamento registrazione
- Espandere Virtual Machine e Provisioning, quindi specificare i seguenti privilegi:
  - Consentire l'accesso al disco
  - Consentire l'accesso di sola lettura al disco
  - Consentire il download nel computer virtuale
- Espandere Virtual Machine e specificare i seguenti privilegi:

  vSphere 4: espandere State e specificare Create snapshot, Remove snapshot e Revert to snapshot.

  vSphere 5: espandere Snapshot management,espandere State, quindi specificare Create snapshot, Remove snapshot e Revert to snapshot.

6. Fare clic su OK per creare il ruolo.
7. Aprire la finestra di dialogo Assign Permissions per assegnare il nuovo ruolo creato a utenti, a gruppi o a entrambi.



8. Dall'elenco Users and Groups, selezionare l'utente personalizzato che si desidera utilizzare per i backup e i ripristini.

   Dall'elenco a discesa Assigned Role, specificare il ruolo che si desidera applicare agli utenti o ai gruppi.

9. Fare clic OK per applicare il ruolo agli utenti o ai gruppi.

   Le autorizzazioni vengono definite per i ruoli vCenter.

Il processo di backup per il modello di computer virtuale viene sempre convertito in backup completo e la dimensione dei dati di backup corrisponde alla dimensione di provisioning del disco virtuale

Sintomo

Durante il backup di un modello di computer virtuale, il processo di backup viene convertito in un backup completo e la dimensione dei dati elaborati è uguale alla dimensione di provisioning del disco virtuale. Nel registro attività viene riportato il seguente messaggio di avviso.

Poiché il computer virtuale è configurato come modello, il processo sarà un backup completo e i dischi virtuali saranno sottoposti a backup come dischi interi.

Soluzione

Si tratta del comportamento previsto per il backup del modello di computer virtuale. Per risolvere il problema, convertire il modello in computer virtuale all'inizio del backup, effettuarne il backup e riconvertirlo in modello una volta terminato il processo di backup. Per attuare questa soluzione, attenersi alla procedura seguente per impostare un valore del Registro di sistema nel computer proxy.

1. Accedere al computer proxy.
2. Creare un valore del Registro di sistema a livello di server proxy o di computer virtuale.

   Nota: Se si aggiunge il valore del Registro di sistema sia a livello di computer virtuale che di proxy, sarà l'impostazione a livello di computer virtuale a prevalere.

   A livello di server proxy (applicabile a tutti i processi di backup in esecuzione sul server proxy)

   a. Aprire la chiave del Registro di sistema dal percorso seguente:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

   b. Aggiungere il valore DWORD *TemplateDirectBackup* e specificare 0 come valore.

   A livello di computer virtuale

a. Aprire la chiave del Registro di sistema dal percorso seguente:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Aggiungere il valore DWORD *TemplateDirectBackup* e specificare 0 come valore.

Nota: Dopo aver abilitato questa opzione, non è possibile riconvertire il computer virtuale in modello se il backup viene interrotto in modo anomalo (ad esempio, in caso di blocco del processo o riavvio del computer proxy).

I dischi indipendenti vengono ignorati dal processo di backup del modello del computer virtuale

Sintomo

Quando si esegue il backup di un modello del computer virtuale, il processo di backup Ignora i dischi indipendenti e nel registro attività viene visualizzato il seguente messaggio di avviso:

Impossibile eseguire il backup del disco virtuale [datastore_720_4] shuli02-t235/-shuli02-t235_1.vmdk, perché è un disco indipendente.

Soluzione

Questo comportamento è previsto per il backup del modello del computer virtuale. La causa principale è un limite di VMware che impedisce all'applicazione di backup di aprire il file VMDK di dischi indipendenti. Una soluzione alternativa consiste nell'impostare i dischi dipendenti come dischi indipendenti all'inizio del backup, eseguirne il backup e impostarli nuovamente come dischi indipendenti al termine del processo di backup. Se si preferisce questa soluzione alternativa, eseguire la procedura seguente per impostare un valore del registro di sistema nel computer proxy.

1. Accedere al computer proxy.
2. Creare un valore del registro di sistema a livello di server proxy o computer virtuale.

   Nota: Se si aggiunge il valore del registro di sistema sia il livello di computer virtuale e proxy, l'impostazione del registro di sistema a livello di computer virtuale contiene la priorità sull'impostazione nel registro di sistema livello Proxy.

   A livello di server proxy (adatto a tutti i processi di backup in esecuzione sul server proxy)

   a. Aprire la chiave del Registro di sistema dal percorso seguente:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

   b. Aggiungere un valore DWORD con nome *ConvertIndependentVMDK* e specificare il valore come 1.

   A livello di computer virtuale

a. Aprire la chiave del Registro di sistema dal percorso seguente:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Aggiungere un valore DWORD con nome *ConvertIndependentVMDK* e specificare il valore come 1.

Note:

- Dopo aver abilitato questa opzione, non è più possibile impostare nuovamente i dischi indipendenti nel caso in cui il backup venga interrotto in modo anomalo (ad esempio, quando si blocca il processo o il computer proxy viene riavviato).
- Questa opzione non funziona quando è attivata l'opzione "conversione del modello in computer virtuale durante il backup" (il valore del registro di sistema TemplateDirectBackup viene creato con il valore 0).

Processo di backup per computer virtuale su condivisione SMB 3.0 non riuscito con messaggio di errore

Nota: Valido per Hyper-V.

Sintomo

Il computer virtuale risiede su Hyper-V 2012 o 2012 R2 e contiene file nella condivisione SMB 3.0. Il processo di backup fallisce ripetutamente generando uno dei messaggi di errore seguenti:

Impossibile acquisire la snapshot VSS. Errore di sistema=[VSS_E_VOLUME_NOT_SUPPORTED_BY_PROVIDER]

Impossibile acquisire la snapshot VSS. Errore di sistema = [VSS_E_BAD_STATE]

Soluzione

1. Se la condivisione SMB è in hosting in un file server Windows, aggiungere il ruolo di servizio dell'agente VSS del file server sul file server e assicurarsi che sia installato l'agente del servizio Copia Shadow del file server Microsoft.
2. Se la condivisione SMB è in hosting in dispositivi NAS di terze parti o altre soluzioni simili, verificare se tali dispositivi o soluzioni supportano SMB 3.0 e i protocolli VSS remoti del file server. Per ulteriori informazioni, contattare il rivenditore del prodotto di terze parti.

Nota:

- Per i computer virtuali che risiedono su Hyper-V 2016, il Servizio agente copia shadow file server non è necessario.
- Configurare correttamente la condivisione SMB 3.0 prima di eseguire il backup del computer virtuale al suo interno con Arcserve UDP. Per conoscere i requisiti dettagliati sulla condivisione SMB 3.0, consultare la sezione sui requisiti e le configurazioni supportate nella documentazione di Microsoft.

Processo di ripristino per computer virtuale non riuscito in caso di ripristino del computer virtuale su una condivisione di file predefinita di Windows

Nota: Valido per Hyper-V.

Sintomo

Durante il ripristino di un computer virtuale, se si definisce la condivisione di file predefinita di Windows (ad esempio, \\hostname\C$\abc) come percorso di destinazione, il processo di ripristino non riesce restituendo il seguente messaggio di errore:

Impossibile creare il nuovo computer virtuale durante il recupero del computer virtuale.

Soluzione

L'errore è previsto perché non è possibile archiviare i file del computer virtuale nella condivisione di file predefinita di Windows. È supportata solo la condivisione di file Microsoft SMB 3.0. Per ulteriori informazioni, fare riferimento alla *documentazione di Microsoft*.

Informazioni sul volume non disponibili per il punto di ripristino

Sintomo

Nella procedura guidata di ripristino di file o computer virtuali, nella schermata del punto di ripristino non vengono visualizzati file o volumi durante il montaggio o la copia del punto di ripristino. Viene invece visualizzato il seguente messaggio:

Informazioni sul volume non disponibili per il punto di ripristino.

Soluzione

Questo è il comportamento previsto quando il computer virtuale di origine non dispone del sistema operativo Windows e, di conseguenza, Arcservev UDP non è in grado di analizzare i dischi virtuali del computer virtuale per ottenere informazioni sul volume. È possibile ripristinare l'intero computer virtuale o eseguire una copia del punto di ripristino. Se il computer virtuale di origine dispone del sistema operativo del computer virtuale Linux, è inoltre possibile ripristinare i file dal punto di ripristino utilizzando un server di backup Linux.

Conversione del backup incrementali in backup di verifica in quanto le snapshot del computer virtuale sono state modificate dopo l'ultimo processo di backup o richiedono il consolidamento

Nota: Valido per piattaforme Windows.

Sintomo

I backup incrementali per i computer virtuali VMware vengono convertiti in backup di verifica. Il registro attività visualizza il seguente messaggio:

"Conversione del backup incrementale in backup di verifica in quanto le snapshot del computer virtuale sono state modificate dopo l'ultimo processo di backup o richiedono il consolidamento."

Soluzione

Utilizzare il client VMware vSphere per consolidare le snapshot del computer virtuale. Per ulteriori informazioni sul consolidamento delle snapshot, consultare l'articolo sulla Knowledge Base di VMware.

Nota: Il consolidamento delle snapshot per un computer virtuale può produrre un errore causato dai file bloccati. Se il processo di backup utilizza la modalità di trasporto HOTADD, verificare che le impostazioni del computer virtuale di proxy di backup sul server ESXi non contengano dischi rigidi HOTADD. Consolidare quindi le snapshot del computer virtuale.

Errore del backup senza agente per il computer virtuale VMware se la periferica CD/DVD del computer virtuale viene associata a un'immagine ISO contenuta in un archivio dati NFS non connesso

Sintomo

Per risolvere il problema, eseguire le seguenti operazioni:

1. Preparare un'immagine ISO su un archivio dati NFS connesso all'host ESX.
2. Associare l'immagine ISO alla periferica CD/DVD di un computer virtuale.
3. Disconnettere l'archivio dati NFS dalla rete.
4. Eseguire il backup senza agente per il computer virtuale.

In questo caso, il processo di backup produce un errore e viene visualizzato il seguente messaggio di errore "Impossibile acquisire la snapshot del computer virtuale. Errore del server ESX/vCenter: Si è verificato un errore generale di sistema."

Soluzione

A causa del limite di ESX, non è possibile acquisire snapshot se il computer virtuale elimina l'associazione dell'immagine ISO. Per risolvere il problema, disconnettere l'immagine ISO dalla periferica CD/DVD del computer virtuale prima del backup.

Errore del backup senza agente basato su host per computer virtuale Hyper-V dopo l'aggiornamento di Arcserve UDP

Valido per Hyper-V

Sintomo

Dopo l'aggiornamento all'ultima versione di Arcserve UDP da Versione 5.0 Aggiornamento 2 o precedenti, l'avvio del backup senza agente basato su host non è riuscito con il seguente messaggio di errore:

Il processo di backup viene annullato. Per una snapshot VSS, il writer VSS Hyper-V deve salvare il computer virtuale, ma questa opzione non si applica nel piano attuale. Per riavviare il processo di backup, modificare l'impostazione del metodo snapshot Hyper-V nel piano. Per ulteriori informazioni su come impostare il metodo snapshot Hyper-V in un piano, consultare la documentazione del prodotto.

Il backup senza agente basato su host funzionava prima dell'aggiornamento.

Soluzione

In Arcserve UDP Versione 5.0 Aggiornamento 2 o precedenti, se il computer virtuale non supporta il metodo di backup in linea, il comportamento predefinito prevede l'adozione del metodo di backup non in linea. Il metodo di backup non in linea consente di salvare il computer virtuale durante l'acquisizione di una snapshot. Nello stato Salvato, il computer virtuale è inaccessibile. Tuttavia, i computer virtuali critici devono essere sempre accessibili.

Nella Versione 5.0 Aggiornamento 3 e versioni successive, se il computer virtuale deve essere impostato nello stato Salvato, il comportamento predefinito prevede l'annullamento del processo di backup per evitare tempi di inattività del computer virtuale. Se non si desidera annullare il processo di backup, modificare l'opzione **Hyper-V Snapshot Method** (Metodo snapshot Hyper-V) nel piano. Per ulteriori informazioni sull'opzione Hyper-V Snapshot Method (Metodo snapshot Hyper-V) nel piano, consultare la sezione Creazione di un piano di backup del computer virtuale basato su host.

È inoltre possibile fare riferimento all'articolo della Knowledge Base di Arcserve per ulteriori informazioni su questo problema.

Errore del backup senza agente basato su host in VMware ESXi 6.0

Sintomo

I backup senza agente di Arcserve UDP potrebbero non riuscire se si tenta di effettuare il backup di un computer virtuale in VMware ESXi 6.0 e la funzione Change Block Tracking (CBT) è abilitata.

Si tratta di un problema noto di VMware. Quando il backup non riesce, possono verificarsi i due comportamenti seguenti:

- Arcserve UDP potrebbe non connettersi alla funzione CBT dell'host ESXi. Di conseguenza, Arcserve UDP non sarà in grado di ricevere dal computer virtuale le informazioni sul blocco di dati utilizzate o modificate.
- Arcserve UDP potrebbe non riuscire ad acquisire le snapshot disattivate del computer virtuale (ciò può verificarsi ogni volta che Arcserve UDP acquisisce una snapshot o quando l'utente acquisisce manualmente una snapshot nel client vSphere).

Soluzione

La build più recente di VMware, ESXi 6.0 Build 2715440, contiene una soluzione a questo problema. Per risolvere il problema, è possibile installare la patch ESXi600-201505001. Per ulteriori informazioni sul download e l'installazione della patch, consultare l'articolo della Knowledge Base di VMware.

Se non è possibile applicare la patch, è possibile risolvere il problema apportando le seguenti modifiche alla chiave del Registro di sistema:

Soluzione per l'errore di connessione CBT.

Se Arcserve UDP non riesce a connettersi a CBT, può tuttavia proseguire con il processo di backup. Invece di eseguire un backup incrementale, per impostazione predefinita Arcserve UDP eseguirà un backup completo del disco del computer virtuale. Se non si desidera che venga eseguito automaticamente un backup completo, è possibile aggiungere una chiave del Registro di sistema per modificare questo comportamento predefinito. Se si aggiunge la chiave e si imposta il valore su 1, Arcserve UDP non sarà in grado di completare il processo di backup in caso di errore CBT.

È possibile aggiungere la chiave del Registro di sistema nel server proxy come segue:

A livello di server proxy (adatto per tutti i processi di backup in esecuzione sul server proxy)

1. Aprire la chiave del Registro di sistema dal percorso seguente:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

2. Immettere il comando dword seguente:

   "BackupEntireDiskOnCBTBitmapFailure"=dword:00000001

3. Salvare la chiave del Registro di sistema.

A livello di computer virtuale

1. Aprire la chiave del Registro di sistema dal percorso seguente:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

2. Immettere il comando dword seguente:

   "BackupEntireDiskOnCBTBitmapFailure"=dword:00000001

3. Salvare la chiave del Registro di sistema.

Nota: Se si aggiunge la chiave del Registro di sistema nel Registro di sistema a livello del computer virtuale e del proxy, l'impostazione nel Registro di sistema a livello del computer virtuale avrà la priorità sull'impostazione nel Registro di sistema a livello del proxy.

Soluzione per l'errore delle snapshot disattivate

Verificare che l'opzione **Acquisire la snapshot senza disattivazione guest in caso di errore della snapshot di disattivazione** sia selezionata nella scheda Origine del piano di backup senza agente basato su host.

Arresto anomalo del backup senza agente basato su host quando si utilizza Windows 2003 R2 a 64 bit come proxy di backup

Si verifica un arresto anomalo del backup senza agente basato su host per computer virtuale VMware quando si utilizza Windows 2003 R2 a 64 bit come proxy di backup

Valido per VMware

Sintomo

Quando si utilizza un computer Windows 2003 R2 a 64 bit come server proxy di backup per proteggere il computer virtuale VMware, a volte il backup può subire un arresto anomalo. Nel file di registro di debug relativo al processo di backup si possono consultare i messaggi di errore come riportato di seguito:

[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)}

Soluzione

In Arcserve UDP versione 7.0, VMware VDDK 6.x è integrato, ma VDDK 6.x non supporta ufficialmente Windows 2003 R2. Per risolvere il problema, è possibile utilizzare una delle seguenti opzioni:

- Utilizzare proxy ufficialmente supportato da VDDK 6.x. Ad esempio, il proxy con Windows 2008 R2, Windows 2012 o Windows 2012 R2.
- Sostituire la versione integrata di VDDK 6 con VDDK 5.5, supportata anche da UDP 7.0. Per ulteriori informazioni sulla sostituzione di VDDK, fare riferimento alla sezione *Applicazione di una versione differente di VDDK rispetto alla versione integrata in Arcserve UDP.*

Modalità di trasporto HotAdd non utilizzata dal backup senza agente basato su host

Sintomo

Ai fine del backup dei dati, il processo di backup basato su host non utilizza la modalità di trasporto HotAdd neanche quando è disponibile. Questo errore si verifica quando il computer virtuale di origine viene importato nella Console di Arcserve UDP da un host ESX, invece che dal server vCenter, e l'host ESX è gestito da un server vCenter.

Soluzione

Per risolvere il problema, completare una delle seguenti attività:

- Eliminare il nodo del computer virtuale dalla Console di Arcserve UDP. Importare nuovamente il nodo dal server vCenter che gestisce l'host ESX.
- Disconnettere l'host ESX dal server vCenter.

Modalità di trasporto NBD o NBDSSL utilizzata dal processo di backup o ripristino senza agente basato su host anche quando è disponibile la modalità SAN

Valido per piattaforme Windows. Valido solo per il computer virtuale VMware.

Sintomo

Sebbene la modalità di trasporto SAN sia disponibile, i processi di backup o ripristino senza agente utilizzano ancora la modalità di trasporto NBD o NBDSSL.

Soluzione

I seguenti prerequisiti devono essere rispettati affinché i processi di backup e ripristino senza agente possano utilizzare la modalità di trasporto SAN.

- Il computer proxy deve essere un computer fisico e non virtuale.
- Il computer proxy deve essere connesso alla LUN SAN in cui si trova il computer virtuale.
- Sul computer proxy, il criterio SAN di un disco SAN deve essere configurato su OnlineAll.

  Per configurare il disco, procedere come segue:

  1. Accedere al sistema proxy di backup mediante un account con privilegi di amministratore.
  2. Aprire la riga di comando di Windows.
  3. Dalla riga di comando, digitare i comandi seguenti:
     a. Digitare diskpart, quindi premere Invio.
     b. Digitare SAN, quindi premere Invio.

        Vengono visualizzati i criteri SAN correnti.

     c. Digitare SAN POLICY=OnlineAll, quindi premere Invio.
- Se si desidera eseguire il ripristino del computer virtuale tramite la modalità di trasporto SAN, il disco SAN deve essere configurato per essere scrivibile.

  Per cancellare il flag di sola lettura, procedere come segue:

  1. Accedere al sistema proxy di backup mediante un account con privilegi di amministratore.
  2. Aprire la riga di comando di Windows.
  3. Dalla riga di comando, digitare i comandi seguenti:

a. Digitare diskpart, quindi premere Invio.

b. Digitare list disk e premere Invio.

   Viene visualizzato l'elenco dei dischi.

c. Digitare select disk xxx, quindi premere Invio per selezionare il disco SAN che verrà configurato per essere scrivibile.

d. Digitare attribute disk clear readonly, quindi premere Invio.

- Ai fini del ripristino di computer virtuali, la modalità di trasporto SAN offre le prestazioni migliori per i dischi thick e quelle peggiori per i dischi thin. Pertanto, per i dischi thin il ripristino di computer virtuali si basa sulla modalità di trasporto NBD o NBDSSL per impostazione predefinita. Se si desidera utilizzare la modalità di trasporto SAN anche per i dischi thin, è possibile aggiungere un valore stringa EnforceTransportForRecovery impostato su SAN in HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFRestoreDll (se non esiste ancora, creare la chiave AFRestoreDll).
- Durante l'acquisizione della snapshot nel corso del backup, vengono generati alcuni file aggiuntivi. Pertanto è necessario spazio libero nella periferica di archiviazione in cui risiedono i file VMDK del computer virtuale. La modalità di trasporto SAN richiede più spazio libero rispetto alla modalità di trasporto NBD/NBDSSL. Quindi assicurarsi che la LUN SAN disponga di spazio libero sufficiente, se si desidera utilizzare la modalità di trasporto SAN.

Impossibile creare una snapshot per computer virtuali Hyper-V quando sono in esecuzione più processi

Sintomo

Durante l'esecuzione di più processi, la creazione di snapshot per computer virtuali Hyper-V CSV richiede molto tempo e non riesce. Non riesce neanche dopo vari tentativi. Il messaggio seguente viene riportato nel registro attività del rispettivo computer virtuale.

Creazione della snapshot in corso. È possibile creare solo una snapshot per volta.

Riprovare tra 600 secondi.

Soluzione

Questo errore si verifica perché è possibile creare una sola snapshot alla volta.

Per risolvere il problema, è possibile aumentare il numero di tentativi o l'intervallo fino al nuovo tentativo. È inoltre possibile aumentare il numero di processi simultanei che è possibile eseguire.

Nota: Il valore predefinito per i tentativi è 3, mentre quello per l'intervallo fino al nuovo tentativo è 10 minuti.

Per aumentare il numero di tentativi, completare i passaggi seguenti sul server proxy:

1. Aprire il Registro di sistema di Windows.
2. Accedere a HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Creare una chiave denominata **VSSWrap**.
4. Fare clic con il pulsante destro del mouse su **VSSWrap**, selezionare **Nuovo**, quindi selezionare il valore **DWORD (32 bit)** e specificare il nome **VssAsynchMaxRetryTimes**.
5. Specificare il valore come richiesto.

Per aumentare l'intervallo fino al nuovo tentativo, completare i passaggi seguenti sul server proxy:

1. Aprire il Registro di sistema di Windows.
2. Accedere a HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Creare una chiave denominata **VSSWrap**.
4. Fare clic con il pulsante destro del mouse su **VSSWrap**, selezionare **Nuovo**, quindi selezionare il valore **DWORD (32 bit)** e specificare il nome **VssA-**

synchMaxRetryInterval.

5. Specificare il valore come richiesto.

Per aumentare il numero di processi simultanei, completare i passaggi seguenti sul server proxy:

1. Aprire il Registro di sistema di Windows.
2. Accedere a HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Fare clic con il pulsante destro del mouse su **HyperVMaxJobNum,** selezionare **Modifica** e specificare il valore richiesto.

Snapshot VSS non creata con Hyper-V

Il backup dei computer virtuali basato su host Hyper-V non avviene correttamente su un host Hyper-V e viene visualizzato il messaggio seguente:

Impossibile acquisire la snapshot VSS.

Sintomo

Gli errori di backup possono essere dovuti ai seguenti motivi:

- Uno o più volumi sull'host Hyper-V non sono stati formattati con NTFS/Refs.
- Uno o più volumi sull'host Hyper-V hanno meno di 100 MB di spazio libero.
- Attività eccessiva del disco durante il backup.

Soluzione

Risolvere i problemi dell'ambiente ed eseguire nuovamente il backup.

Impossibile eseguire il backup del disco virtuale a causa di un errore di sistema=[la periferica non è pronta (21)]

Valido per piattaforme Windows.

Sintomo

Se si verifica un errore di rete o il server Hyper-V viene riavviato mentre è in corso un'operazione di backup, il registro attività indicherà se si tratta di un errore di rete o di un errore file system.

Soluzione

Riavviare il processo di backup in seguito al riavvio del server Hyper-V.

Errore del processo di backup

Sintomo

Si verifica un errore del processo di backup con il seguente messaggio di errore visualizzato nei registri attività:

Impossibile eseguire la riconfigurazione del backup nello stato corrente. Arrestare il computer virtuale e tentare nuovamente di eseguire il processo di backup. (È possibile avviare il computer virtuale durante o in seguito alla fase di acquisizione della snapshot).

Soluzione

Impostare i valori del registro di sistema per non riconfigurare disk.enableUUID.

Effettuare le operazioni seguenti:

Viene applicato a livello di proxy e riguarda tutti i computer virtuali VMware.

1. Accedere al server proxy di backup.
2. Aprire l'editor del Registro di sistema e cercare la seguente chiave:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll
3. Aggiungere un valore DWORD denominato DoNotReconfigDiskUUID e specificare 1 come valore corrispondente.

Riguarda un livello specifico del computer virtuale. Riguarda soltanto il computer virtuale specificato.

1. Accedere al server proxy di backup.
2. Aprire l'editor del Registro di sistema e cercare la seguente chiave:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM-InstanceUUID>

   Nota: Sostituire <VM-InstanceUUID> con il valore UUID del computer virtuale richiesto dall'applicazione. Il valore può essere reperito nell'URL del computer virtuale utilizzato durante la connessione all'agente Arcserve UDP.
3. Aggiungere un valore DWORD denominato DoNotReconfigDiskUUID e specificare 1 come valore corrispondente.

Tenere presenti le seguenti considerazioni:

- Il livello del computer virtuale ha la precedenza se sono configurati entrambi i registri di sistema a livello di computer virtuale e di proxy.

- Se il registro di sistema non esiste, il valore del registro di sistema è pari a 0, ovvero sarà necessario riconfigurare disk.enableUUID.
- Se è stato specificato di non riconfigurare il parametro disk.EnableUUID, i dati sottoposti a backup potrebbero non essere uniformi.

Per ulteriori informazioni, consultare la sezione Articolo della Knowledge Base di VMware.

Errore di importazione dei computer virtuali VMware da vCenter

Sintomo

ARCserve UDP non è in grado di importare computer virtuali VMware da vCenter, anche se il server vCenter è operativo ed è in grado di connettersi con il browser e client vSphere. Nel file ARCAPP.log del server della Console di Arcserve UDP, viene visualizzato il messaggio di errore seguente:

com.sun.xml.ws.client.ClientTransportException: HTTP transport error: javax.-net.ssl.SSLHandshakeException: java.security.cert.CertificateException: Certificates does not conform to algorithm constraints

Tuttavia, modificando le due righe riportate di seguito nel file "C:\P-rogrammi\Arcserve\Unified Data Pro-tection\Common\JRE\lib\security\java.security" e riavviando il servizio di gestione Arcserve UDP, è possibile effettuare la connessione allo stesso server vCenter tra-mite Arcserve UDP:

Righe esistenti:

jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024

jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768

Righe modificate:

jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 512

jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 512

Causa:

Il server vCenter presenta un certificato con una chiave pubblica breve o il relativo algoritmo è disattivato dal JRE in Arcserve UDP. Un certificato con chiave pubblica inferiore a 1024 bit viene considerato non sicuro (le stesse condizioni si applicano per l'algoritmo MD5). Vengono disabilitati dal JRE utilizzato da Arcserve UDP.

Soluzione

Generare un nuovo certificato per il server vCenter. Verificare che le dimensioni della chiave pubblica del nuovo certificato siano superiori a 1024 bit e che venga utilizzato un algoritmo più sicuro.

Backup non riusciti a causa della licenza ESXi

Valido per piattaforme Windows.

Sintomo

I processi di backup completo, incrementale e di verifica producono un errore. Viene visualizzato il seguente messaggio nel Registro attività di Arcserve UDP:

Il server del computer virtuale <server_name> non dispone di una licenza ESX acquistata.

Soluzione

A causa di una limitazione di VMware, non è possibile eseguire il backup dei computer virtuali in esecuzione sui server ESXi con una licenza gratuita. Per proteggere questi computer virtuali, applicare una licenza acquistata.

Modalità di trasporto HotAdd non funzionante durante il backup di un computer virtuale VMware

Sintomo

La modalità di trasporto HotAdd non è supportata per questo computer virtuale e di conseguenza il backup non riesce nella modalità NBDSSL (periferica di blocco rete crittografata). (L'esecuzione del processo di backup è lenta). Il backup di un computer virtuale VMware non utilizza la modalità di trasporto HotAdd. Per ulteriori informazioni sul trasporto HotAdd, consultare il seguente collegamento.

Verificare i seguenti prerequisiti per la modalità HotAdd:

- Il proxy di backup HotAdd deve essere un computer virtuale. La modalità HotAdd implica il collegamento di un disco virtuale al proxy di backup, simile alla connessione di un disco a un computer virtuale.
- Il proxy HotAdd deve disporre dell'accesso allo stesso archivio dati del computer virtuale di destinazione.
- La versione VMFS e le dimensioni del blocco di dati del computer virtuale di destinazione devono corrispondere a quelle dell'archivio dati in cui si trova il proxy HotAdd. Se il proxy HotAdd è un computer virtuale che risiede su un volume VMFS-3, scegliere un volume con una dimensione di blocco appropriata per le dimensioni massime del disco virtuale dei computer virtuali che i clienti desiderano sottoporre a backup, come descritto nella sezione relativa alla dimensione del blocco VMFS-3 per il proxy di backup HotAdd. Questa nota non è valida per i volumi VMFS-5, che dispongono sempre di una dimensione di blocco di file pari a 1 MB.

  Nella tabella seguente viene riportata la dimensione di blocco VMFS-3 per il proxy di backup HotAdd:

Dimensione di blocco VMFS	Dimensione massima del disco di destinazione
1 MB	256 GB
2 MB	512 GB
4 MB	1024 GB
8 MB	2048 GB

- In vSphere 5.1 e versioni precedenti, la dimensione VMDK massima supportata è di 1,98 TB.
- I dischi su cui effettuare l'HotAdd devono essere dischi SCSI. Le unità IDE non sono compatibili con HotAdd.

- VMware Tools deve essere installato e aggiornato sul computer virtuale e sul proxy di backup.
- Nell'archivio dati deve essere disponibile una quantità di spazio sufficiente per una snapshot del computer virtuale.
- La modalità HotAdd potrebbe non riuscire se sono stati creati dei dischi con una versione hardware più recente rispetto a quella del computer virtuale sottoposto a backup. Ad esempio, se un disco è stato spostato da un computer virtuale con versione hardware 8 a un computer virtuale con versione hardware 7. Per risolvere questo problema, aggiornare la versione hardware del computer virtuale.
- Un controller SCSI singolo può disporre di un numero massimo di 15 dischi collegati. Per eseguire più processi simultanei con più di 15 dischi, è necessario aggiungere più controller SCSI al computer proxy di backup.
- In caso di connessione ESX standalone (il server ESX non è gestito da vCenter), è possibile effettuare l'HotAdd soltanto dei dischi dei computer virtuali che si trovano sullo stesso ESX del computer proxy di backup.
- Il processo di HotAdd potrebbe non riuscire se si sta tentando di eseguire il backup del computer virtuale mediante l'ESX aggiunto in UDP come server standalone ma che in realtà è gestito da vCenter.
- Il processo di HotAdd potrebbe non riuscire se il computer virtuale che si sta tentando di sottoporre a backup e il server proxy si trovano in cluster diversi.

Soluzione

Disabilitare automount sul computer proxy di backup mediante l'utilità diskpart.

Controllo più granulare per VSS su un sistema operativo guest Windows disattivato

Sintomo

Si desidera specificare un controllo più granulare per VSS durante la creazione di una snapshot di disattivazione per il sistema operativo guest Windows.

Soluzione

A partire da vSphere 6.5, l'API del servizio Web vSphere supporta i seguenti controlli più granulari per VSS durante la creazione delle snapshot di disattivazione per il sistema operativo guest Windows:

- È possibile configurare qualsiasi timeout da cinque minuti a quattro ore (il valore predefinito è 15 minuti) per la disattivazione dei computer virtuali.
- Tipo di backup VSS: in precedenza, per la creazione delle snapshot veniva utilizzato VSS_BT_COPY per impostazione predefinita Ora sono disponibili anche VSS_BT_FULL, VSS_BT_INCREMENTAL, VSS_BT_DIFFERENTIAL e VSS_BT_LOG. Il troncamento del registro viene attivato in base alle impostazioni dell'applicazione.
- Per imporre la disattivazione dell'applicazione (contesto VSS_CTX_BACKUP) o del file system (contesto VSS_CTX_FILE_SHARE_BACKUP), è stato introdotto il contesto di backup per VSS.

Utilizzando Arcserve UDP, è possibile specificare i parametri nel Registro di sistema per l'implementazione del controllo.

Nota: nello specifico, nel sistema operativo del computer virtuale guest deve essere installato VMware Tools 10.1.0 o versione successiva

Effettuare le operazioni seguenti:

1. Accedere al computer proxy.
2. Creare un valore del registro di sistema a livello di server proxy o computer virtuale.

   Nota: Se si aggiunge il valore del registro di sistema sia il livello di computer virtuale e proxy, l'impostazione del registro di sistema a livello di computer virtuale contiene la priorità sull'impostazione nel registro di sistema livello Proxy.

   A livello di server proxy (adatto a tutti i processi di backup in esecuzione sul server proxy)

a. Aprire la chiave del Registro di sistema dal percorso seguente:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

b. Aggiungere i seguenti valori DWORD con i valori appropriati:

- VssUseEnhancedSnapshot
- VssTimeoutMinute
- VssBackupType
- VssBackupContext
- VssBootableSystemState
- VssPartialFileSupport

A livello di computer virtuale

a. Aprire la chiave del Registro di sistema dal percorso seguente:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Aggiungere i seguenti valori DWORD con i valori appropriati:

- VssUseEnhancedSnapshot
- VssTimeoutMinute
- VssBackupType
- VssBackupContext
- VssBootableSystemState
- VssPartialFileSupport

Possibili valori dei valori del Registro di sistema:

VssUseEnhancedSnapshot

- 0 - Non utilizza il controllo avanzato e i valori inferiori del Registro di sistema non hanno effetto
- 1 - Utilizza il controllo avanzato e i valori inferiori del Registro di sistema hanno effetto

VssTimeoutMinute

Intervallo da 5 a 240

VssBackupType

- 0 - VSS_BT_COPY (predefinito)
- 1 - VSS_BT_FULL
- 2 - VSS_BT_INCREMENTAL
- 3 - VSS_BT_DIFFERENTIAL
- 4 - VSS_BT_LOG

VssBackupContext

- 0 - ctx_auto
- 1 - ctx_backup (predefinito)
- 2 - ctx_file_share_backup

VssBootableSystemState

- 0 - False
- 1 - true (predefinito)

VssPartialFileSupport

- 0 - false (predefinito)
- 1 - true

Non è possibile configurare il computer virtuale per abilitare il parametro "Disk.EnableUUID"

Sintomo

Si verifica un errore durante la riconfigurazione del computer virtuale per abilitare il parametro "disk.EnableUUID", necessario per un backup coerente con l'applicazione. Questo problema si verifica quando l'ambiente virtuale è stato ripristinato dopo un errore.

Soluzione

Questo problema è specifico dell'ambiente VMware. Questo problema si verifica quando Microsoft VSS tenta di eseguire una snapshot di un'applicazione disattivata, ma non riesce a leggere il valore UUID o il numero di serie di uno o più dischi del computer virtuale.

È necessario configurare il parametro disk.EnableUUID del computer virtuale. I computer virtuali creati con le versioni 4.1 (o versioni successive) dispongono del parametro abilitato per impostazione predefinita. Il processo di backup viene configurato automaticamente per evitare incoerenze a livello di dati ed eseguire un

backup coerente con l'applicazione. Se il processo di backup non riesce ad abilitare disk.EnableUUID, configurare manualmente il parametro procedendo come segue:

Effettuare le operazioni seguenti:

1. Disattivare il computer virtuale.
2. Accedere al server vCenter o all'host ESX/ESXi mediante il client vSphere.
3. Fare clic con il pulsante destro del mouse sul computer virtuale e scegliere Modifica impostazioni.
4. Fare clic sulla scheda Opzioni.
5. Accedere ad Avanzate > Generale > Parametri di configurazione.
6. Aggiungere o modificare la riga disk.EnableUUID impostandola su True.
7. Fare clic su OK per salvare.
8. Fare clic su OK per uscire.
9. Riavviare il computer virtuale per attivare le modifiche.

   Nota: se il parametro è già impostato su True, come soluzione alternativa non distruttiva è possibile modificare il file vmx e impostare il valore di disk.enableUUID su false, quindi migrare il computer virtuale con vMotion (a qualsiasi altro host) per ricaricare il file vmx nella memoria dell'host. Questo disabilita efficacemente la disattivazione a livello di applicazione (la disattivazione a livello di file system è ancora disponibile).

Errore delle operazioni di recupero durante il recupero dei dati mediante la modalità di trasporto HOTADD o SAN

Valido per piattaforme Windows.

Sintomo

Errore delle operazioni di recupero durante il recupero dei dati mediante la modalità di trasporto HOTADD o SAN. Il seguente messaggio viene visualizzato nel Registro attività:

Si è verificato un errore sconosciuto. Contattare il Supporto Tecnico.

Soluzione

Errore delle operazioni di recupero con la modalità di trasporto HOTADD o SAN quando le impostazioni del disco non sono configurate correttamente.

Per configurare l'operazione il disco, procedere come segue:

1. Accedere al sistema proxy di backup mediante un account con privilegi di amministratore.
2. Aprire la riga di comando di Windows.
3. Dalla riga di comando, immettere il seguente comando:

   diskpart

   Premere Invio.
4. Digitare SAN, quindi premere Invio.

   Vengono visualizzati i criteri SAN correnti.
5. Digitare il seguente comando e premere Invio:

   SAN POLICY = OnlineAll

   Il criterio SAN viene configurato in modo da non eseguire il montaggio automatico dei volumi SAN.
6. Per cancellare l'attributo di sola lettura di un determinato disco SAN, selezionare il disco dall'elenco, quindi immettere il seguente comando e premere Invio:

   attribute disk clear readonly
7. Digitare exit, quindi premere Invio.

   Il disco viene configurato e sarà possibile inoltrare nuovamente il processo.

   Se il processo riporta errori ancora una volta, montare i dischi HOTADD manualmente utilizzando la gestione disco sul sistema proxy.

Per montare i dischi manualmente, procedere come segue:

1. Accedere al sistema proxy di backup mediante un account con privilegi di amministratore.
2. Aprire il Pannello di controllo di Windows e fare doppio clic su Strumenti di amministrazione.

   Viene visualizzata la finestra di dialogo degli strumenti di amministrazione.
3. Dall'elenco Preferiti, fare doppio clic su Gestione computer.

   Viene visualizzata la finestra della Gestione computer.
4. Espandere Archiviazione, quindi fare clic sulla Gestione disco.

   Vengono visualizzati i dischi.
5. Fare clic con il tasto destro del mouse sul disco che si desidera montare, quindi fare clic su In linea.

   Il disco viene montato e sarà possibile inoltrare nuovamente il processo.

Operazione di recupero del computer virtuale non riuscita se è selezionata una porta non predefinita

Sintomo

L'operazione di recupero del computer virtuale non riesce se è selezionata una porta non predefinita per il server VMware vCenter.

Soluzione

Per risolvere il problema, impostare il numero di porta non predefinita di vCenter sul valore VDDKport nel Registro di sistema del computer proxy di backup.

Per impostare il numero VDDKport, completare i passaggi seguenti sul server proxy:

1. Aprire il Registro di sistema di Windows.
2. Accedere a HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Fare clic con il pulsante destro del mouse su VDDKport, selezionare Modifica e specificare il valore richiesto.

Errori del processo di backup incrementale o completo pianificato per il computer virtuale Hyper-V

Sintomo

A volte, il processo di backup incrementale o completo pianificato produce un errore per i computer virtuali Hyper-V. Vengono visualizzati i seguenti messaggi di errore nel visualizzatore eventi dell'host Hyper-V:

- Operazione di aggiunta della memoria dinamica per il computer virtuale <vm name> non riuscita con l'errore: Memoria esaurita (0x8007000E) (ID computer virtuale <vm ID>)
- Impossibile creare punto di controllo di backup per la macchina virtuale <vm name>: Operazione restituita perché il periodo di timeout è scaduto. (0x800705B4). (ID macchina virtuale <ID vm>)
- Impossibile creare punto di controllo di backup per la macchina virtuale <vm name>: Elemento non trovato. (0x80070490). (ID macchina virtuale <ID vm>)
- I writer VSS all'interno del computer virtuale <vm name> non hanno potuto eseguire l'operazione BackupComplete nella rispettiva copia shadow (snapshot VSS): È stata eseguita una chiamata di funzione quando l'oggetto era in uno stato errato per tale funzione (0x80042301). (ID computer virtuale)
- L'Hyper-V VSS writer ha rilevato un errore durante l'elaborazione del computer virtuale. (Per ulteriori informazioni sugli errori del writer Hyper-V VSS, fare riferimento alla documentazione di prodotto).

Soluzione 1

Per risolvere il problema, aumentare la memoria RAM del server Hyper-V e inviare nuovamente il processo di backup.

Soluzione 2

Se il writer VSS del computer virtuale non funziona correttamente, il processo di backup produrrà un errore. Per risolvere il problema, verificare il registro eventi sia per l'host Hyper-V che per il computer virtuale. Verificare gli avvisi e gli errori VSS, quindi eseguire le azioni corrispondenti.

Errore del writer Hyper-V VSS NTDS durante l'acquisizione di snapshot VSS nel computer virtuale

Sintomo

In un Controller di dominio del computer virtuale, se la funzionalità AutoMount non viene abilitata, il writer VSS NTDS produce un errore durante l'acquisizione della snapshot VSS nel computer virtuale. Di conseguenza, l'Hyper-V VSS writer produce un errore durante l'acquisizione della snapshot VSS sull'host Hyper-V.

Il processo di backup HBBU Hyper-V produce un errore nel seguente Registro attività:

L'Hyper-V VSS writer ha rilevato un errore durante l'elaborazione del computer virtuale. (Per ulteriori informazioni sugli errori del writer Hyper-V VSS, fare riferimento alla documentazione di prodotto).

Soluzione

Abilitare la funzionalità *AutoMount* per il computer virtuale.

Effettuare le operazioni seguenti:

1. Aprire la finestra del prompt dei comandi.
2. Aprire diskpart ed eseguire il comando seguente:

   automount enable

Le modifiche all'indirizzo MAC non vengono memorizzate dopo il ripristino del computer virtuale

Valido su piattaforme Windows e computer virtuali VMware

Sintomo

Gli indirizzi MAC di computer virtuali non vengono mantenuti dopo il recupero di computer virtuali.

Soluzione

Gli indirizzi MAC non vengono mantenuti durante il ripristino per evitare la presenza di duplicati. Per mantenere le informazioni relative all'indirizzo MAC, impostare la seguente chiave di registro sul server proxy:

Posizione: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
Nome chiave: RetainMACForVDDK
Tipo valore: Stringa

Valore chiave: 1

Errore di ripristino del computer virtuale - Impossibile aprire i file VMDK

Sintomo

Il ripristino del computer virtuale non riesce e viene visualizzato il seguente messaggio di errore nei registri:

Impossibile aprire il file vmdk (nome di file con l'estensione .vmdk). VMware ha riscontrato il seguente errore: non si dispone dei diritti di accesso al file. Per ulteriori informazioni, consultare il registro di debug del ripristino. Se necessario, contattare il Supporto tecnico di Arcserve.

Nel registro di debug del ripristino sono disponibili i messaggi seguenti:

- [VDDKLOG] CnxAuthdConnect: restituisce false perché la verifica SSL richiesta e l'authd di destinazione non supportano SSL
- [VDDKLOG] CnxConnectAuthd: restituisce false perché CnxAuthdConnect non è riuscito
- [VDDKLOG] Cnx_Connect: restituisce false perché CnxConnectAuthd non è riuscito
- [VDDKLOG] Cnx_Connect: Messaggio di errore: SSL necessario

Soluzione

È possibile che l'autenticazione SSL sia disabilitata sull'host ESX. Per risolvere il problema, utilizzare uno dei metodi seguenti:

Utilizzo del client vSphere

1. Accedere al server vCenter/ESX.
2. Accedere alle impostazioni del server ESX:

   Configurazione, Impostazioni avanzate, Configurazione, Impostazioni predefinite della protezione

3. Abilitare l'opzione seguente:

   config.defaults.security.host.ruissl

Utilizzo della riga di comando

1. Connettersi all'host ESX di mediante SSH.
2. Aprire il seguente file:

   /etc/vmware/config

3. Impostare la voce security.host.ruissl su TRUE.
4. Salvare il file e riavviare gli agenti di gestione.

Problemi causati da UUID duplicati del computer virtuale

Sintomo 1

Il nodo del computer virtuale viene sovrascritto dopo l'importazione di un altro nodo del computer virtuale nella console.

Ad esempio, si dispone di due computer virtuali VM1 e VM2 con lo stesso UUID (denominato UUID istanza per VMware e UUID computer virtuale per Hyper-V) negli host ESXi gestiti da diversi vCenter, VC1 e VC2. VM1 viene importato nella console e visualizzato nella visualizzazione dell'elenco nodi della console. In un secondo momento, viene importato VM2 nella console. Nella visualizzazione dell'elenco nodi, VM1 viene sovrascritto dal VM2 (in altre parole, viene aggiunto VM2 ed eliminato VM1).

Sintomo 2

Le informazioni sul nodo del computer virtuale nella colonna dell'hypervisor cambiano continuamente durante l'esecuzione del rilevamento automatico.

Ad esempio, si dispone di due computer virtuali VM1 e VM2 con lo stesso UUID (denominato UUID istanza per VMware e UUID computer virtuale per Hyper-V) negli host ESXi gestiti da diversi vCenter, VC1 e VC2. Nella console vengono importati VM1 e almeno uno dei computer virtuali dal vCenter VC2. In questo modo sia VC1 che VC2 vengono aggiunti all'elenco di rilevamento dei nodi (è possibile verificare l'elenco nella pagina Configurazione rilevamento nodi della scheda Impostazioni). Durante l'esecuzione, il rilevamento del nodo si connette innanzitutto a VC1 e rileva VM1 in base al GUID corrispondente; quindi, la colonna dell'hypervisor viene aggiornata con le informazioni relative a VC1. In seguito, quando si connette a VC2, rileva VM2 tramite lo stesso GUID e la colonna dell'hypervisor viene aggiornata con le informazioni relative a VC2.

Soluzione

Arcserve UDP utilizza l'UUID del computer virtuale (denominato UUID istanza per VMware e UUID computer virtuale per Hyper-V) per identificare il nodo di un computer virtuale. Sebbene sia poco frequente che i computer virtuali possiedano UUID uguali, in casi simili è possibile che Arcserve UDP presenti problemi.

Per risolvere tali problemi, attenersi alla procedura seguente per modificare manualmente l'UUID del computer virtuale (solo per computer virtuali VMware). Una volta modificato manualmente l'UUID del computer virtuale, eliminare il computer virtuale originale dalla console Arcserve UDP e importare nuovamente il computer virtuale.

1. Aprire il seguente URL:

   https://<nome host vCenter>/mob/

2. Accedere come amministratore.
3. Cercare "content" nella colonna NAME e fare clic sul collegamento nella colonna VALUE nella stessa riga.
4. Cercare "rootFolder" nella colonna NAME e fare clic sul collegamento nella colonna VALUE nella stessa riga.
5. Cercare "childEntity" nella colonna NAME. Nella colonna VALUE della stessa riga, individuare il centro dati in cui risiede il computer virtuale e fare clic sul collegamento corrispondente.
6. Cercare "vmFolder" nella colonna NAME e fare clic sul collegamento nella colonna VALUE nella stessa riga.
7. Cercare "childEntity" nella colonna NAME. Nella colonna VALUE della stessa riga, fare clic su "more..." per espandere l'elenco di computer virtuali. Individuare il computer virtuale interessato e fare clic sul collegamento corrispondente.
8. Cercare ReconfigVM_Task nella tabella Methods (Metodi) e fare clic sul collegamento.
9. Nel browser nuovo aperto, rimuovere tutti i contenuti nel campo VALUE e immettere il codice seguente:

   ```
   <spec>
   <instanceUuid>2499952a-6c85-480e-b7df-4cb-
   d2137eb69</instanceUuid>
   </spec>
   ```

   Nota: La stringa di 2499952a-6c85-480e-b7df-4cbd2137eb69 sopra riportata è un esempio di UUID. È necessario sostituirla con l'UUID che si desidera applicare.
10. Fare clic sul collegamento Invoke Method (Richiama metodo) per applicare il nuovo UUID.
11. Per verificare che il nuovo UUID sia applicato, chiudere il browser appena aperto e tornare alla pagina indicata nel passaggio 8.
12. Cercare "config" nella colonna NAME e fare clic sul collegamento nella colonna VALUE nella stessa riga.
13. Cercare "instanceUuid" nella colonna NAME. L'UUID del computer virtuale viene visualizzato nella colonna VALUE della stessa riga.

Errore del processo di catalogo file system o della verifica del punto di ripristino per il backup senza agente basato su host

Valido per piattaforme Windows. Valido solo per il computer virtuale VMware.

Sintomo

- Errore del processo di catalogo file system per i punti di ripristino di backup senza agente basato su host
- La verifica del punto di ripristino non riesce durante il processo di backup senza agente basato su host e il backup incrementale successivo viene convertito in backup di verifica.

Soluzione

Questo errore può essere causato da un problema noto di VMware (consultare l'articolo della Knowledge Base di VMware). Quando si disattiva un computer virtuale VMware, la snapshot contiene dati corrotti. Il backup legge i dati dalla snapshot, quindi anche i dati su cui è stato eseguito il backup diventano corrotti.

Nota: questo problema si verifica con tutte le versioni di VMware ESXi e sui computer virtuali con sistema operativo guest Windows 2008 R2 SP1 e Windows 2012. Arcserve UDP non è in grado di rilevare il problema di corruzione dei dati perché in questi casi VMware non restituisce un errore. Si potrebbe rimanere all'oscuro del problema finché non si tenta di ripristinare i dati.

Consultare l'articolo della Knowledge Base di Arcserve per verificare se l'errore è causato da questo problema noto di VMware. Per risolvere il problema, VMware consiglia di disabilitare i writer VSS, come il writer del servizio MSSearch (ignorarlo se non è installato) e il writer di ottimizzazione delle copie shadow (in genere presente in ogni computer virtuale Windows), nel sistema operativo guest del computer virtuale. Per disabilitare manualmente i writer, seguire le istruzioni dell'articolo della Knowledge Base di VMware.

Arcserve UDP offre inoltre un semplice metodo per disabilitare i writer se si utilizza il metodo di disattivazione snapshot degli strumenti VMware. Per disabilitare i writer, attenersi alla procedura seguente:

A livello di server proxy (adatto per computer virtuali protetti dal server proxy)

1. Accedere al server proxy.
2. Aprire la chiave del Registro di sistema dal percorso seguente:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data
Protection\Engine\AFBackupDll]
```

3. Creare un valore a stringa multipla denominato *DisableSpecificVSSwriters*.
4. Immettere i nomi del writer VSS che dovrebbe essere disabilitato (il nome di ogni writer occupa una riga).
5. Salvare la chiave del Registro di sistema.

A livello di computer virtuale

1. Accedere al server proxy.
2. Aprire la chiave del Registro di sistema dal percorso seguente:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data
Protection\Engine\AFBackupDll\<vm instance uuid>]
```

3. Creare un valore a stringa multipla denominato *DisableSpecificVSSwriters*.
4. Immettere i nomi del writer VSS che dovrebbe essere disabilitato (il nome di ogni writer occupa una riga).
5. Salvare la chiave del Registro di sistema.

Note:

- Se si aggiunge la chiave del Registro di sistema nel Registro di sistema a entrambi i livelli (computer virtuale e proxy), l'impostazione nel Registro di sistema a livello del computer virtuale avrà la priorità su quella nel Registro di sistema a livello del proxy.
- Questa impostazione del Registro di sistema funziona solo quando si utilizza il metodo di disattivazione snapshot degli strumenti VMware nel piano di backup.
- In caso di configurazione manuale dei writer nel sistema operativo guest del computer virtuale in base alle istruzioni dell'articolo della Knowledge Base di VMware, tale configurazione verrà sovrascritta.
- Rispettare la distinzione tra maiuscole e minuscole per il nome del writer, che deve corrispondere esattamente a quanto mostrato nell'output del comando "vssadmin list writers".
- Se si desidera abilitare nuovamente tutti i writer, non eliminare il valore del Registro di sistema *DisableSpecificVSSwriters*. Conservare il valore del Registro di sistema, ma rimuovere il contenuto al suo interno. Se *DisableSpecificVSSwriters* non esiste, Arcserve UDP presuppone che non sono richieste modifiche in termini di abilitazione o disabilitazione dei writer VSS.

Conversione del backup incrementale per verificare il backup o aumento delle dimensioni di backup in Hyper-V

Valido su computer virtuali Hyper-V

Sintomo

- È stata apportata una modifica incrementale in un computer virtuale Hyper-V. Quando viene eseguito un backup incrementale, viene sottoposto a backup l'intero computer virtuale, non soltanto i dati modificati.
- Si dispone di un server proxy con Arcserve UDP versione 7.0 che esegue il backup di un computer virtuale da un host Hyper-V (ad esempio, HOST1). Si dispone di un altro server proxy con una versione precedente di Arcserve UDP che esegue il backup di un computer virtuale dallo stesso host Hyper-V (HOST1). In tali casi, la funzionalità CBT non è attiva e i processi incrementali non vengono eseguiti. Il backup incrementale viene convertito in backup di verifica.

Soluzione

I comportamenti sopra descritti possono essere causati da uno dei seguenti motivi:

- Perdita dei dati relativi alla funzionalità di traccia dei blocchi modificati (CBT). Le seguenti circostanze comportano la perdita dei dati CBT:
  - L'host Hyper-V ha subito un arresto o è stato interrotto in modo anomalo
  - Il servizio CBT viene interrotto o il servizio viene chiuso in modo anomalo.
  - Il servizio CBT non ha completato il proprio lavoro durante lo spegnimento dell'host Hyper-V.
- Diverse versioni CBT nel server Hyper-V e nel server proxy.

  Esempio: si supponga di avere a disposizione due ambienti Arcserve UDP, di cui uno è Arcserve UDP versione 6.0 e l'altro è Arcserve UDP versione 7.0. Questi due ambienti Arcserve UDP eseguono il backup di computer virtuali diversi nello stesso server Hyper-V. L'ambiente Arcserve UDP versione 7.0 rileva automaticamente la versione meno recente di CBT nel server Hyper-V e la aggiorna all'ultima versione. In tali casi, l'ambiente Arcserve UDP versione 5 converte il backup incrementale pianificato restante in un backup completo.

  Se Arcserve UDP rileva versioni diverse di CBT, il registro attività mostra un messaggio di avviso.

Per risolvere il problema, aggiornare alla stessa versione di Arcserve UDP tutti i server proxy che proteggono i computer virtuali da un host Hyper-V.

Il backup basato su host non riesce per un computer virtuale Hyper-V con una speciale configurazione del disco di differenziazione

Valido per il computer virtuale Hyper-V

Sintomo

Se in un computer virtuale Hyper-V è configurato un disco di differenziazione, il processo di backup per quel computer virtuale non riuscirà. Viene visualizzato il seguente messaggio di errore nel registro attività:

Failed to prepare for backup of the virtual machine (Impossibile preparare il backup del computer virtuale)

Nel file di log del processo di backup in C:\Programmi\Arcserve\Unified Data Protection\Engine\Logs, viene visualizzato il seguente messaggio di errore:

The virtual disk file \\?\UNC\<IP_Address_VM>\HYPERV_HBBU_SNAPSHOT@<snapshot_name>\WIN12-SQL\VIRTUAL HARD DISKS\WIN12-SQL-1.VHDX was not exposed. (Il file del disco virtuale \\?\UNC\<IP_Address_VM>\HYPERV_HBBU_SNAPSHOT@<snapshot_name>\WIN12-SQL\VIRTUAL HARD DISKS\WIN12-SQL-1.VHDX non è stato esposto.)

Il problema si verifica solo quando il computer virtuale presenta le seguenti configurazioni di disco di differenziazione. È necessario applicare tutte le configurazioni.

- Il computer virtuale ha un normale disco rigido virtuale (dimensione fissa o a espansione dinamica) (Disk1) collegato a un controller IDE o SCSI del computer virtuale.
- Il computer virtuale ha un disco rigido virtuale di differenziazione (Disk2) anch'esso collegato a un controller IDE o SCSI del computer virtuale.
- Il disco padre di Disk2 è specificato in Disk1.

Soluzione

Questo errore si verifica a causa di una configurazione anomala o errata. Per risolvere questo errore, staccare il disco di differenziazione o quello principale dal computer virtuale. Arcserve UDP non supporta tale configurazione del disco di differenziazione.

Backup Job Fails for a VMware Virtual Machine (Il processo di backup non riesce per un computer virtuale VMware)

Valido per il computer virtuale VMware

Sintomo

Quando si esegue il backup di un computer virtuale, il processo di backup non riesce con uno dei seguenti messaggi di errore nel registro attività:

Abort backup because backup job has been configured to use the "Microsoft VSS inside VM" snapshot method. However, only the "VMware Tools" snapshot method is applicable because Host-based VM Backup failed to deploy the necessary tools into the VM. (Interrompere il backup perché il processo di backup è stato configurato sull'utilizzo del metodo snapshot "Microsoft VSS all'interno del computer virtuale". Tuttavia, solo il metodo snapshot "Strumenti VMware" è applicabile perché il backup del computer virtuale basato su host non è riuscito a distribuire gli strumenti necessari nel computer virtuale.)

Oppure

Abort backup because backup job has been configured to use the "VMware Tools" snapshot method. However, only the "Microsoft VSS inside the VM" snapshot method is applicable because Host-based VM Backup failed to undeploy tools from inside VM (Interrompere il backup perché il processo di backup è stato configurato per utilizzare il metodo snapshot "Strumenti VMware. Tuttavia, solo il metodo snapshot "Microsoft VSS dentro il computer virtuale" è applicabile perché il backup del computer virtuale basato su host non è riuscito ad annullare la distribuzione degli strumenti all'interno del computer virtuale.)

Soluzione

Il primo errore può verificarsi a causa di diversi motivi. È stata selezionata l'opzione **Microsoft VSS inside VM** (Microsoft VSS all'interno del computer virtuale) ma:

- Il computer virtuale non è stato aggiornato con le credenziali necessarie.
- Le credenziali non sono corrette.
- Gli Strumenti VMware non sono stati installati o aggiornati.

In questo caso, Arcserve UDP non è in grado di distribuire gli strumenti necessari al computer virtuale per utilizzare il nuovo metodo snapshot.

Per risolvere questo errore, aggiornare il computer virtuale con le credenziali corrette. Verificare che gli Strumenti VMware siano aggiornati e in esecuzione nel computer virtuale. Dopo la verifica, avviare di nuovo il processo di backup.

Soluzione

Il secondo errore si può verificare nello scenario seguente. È stata utilizzata l'opzione **Microsoft VSS inside VM** (Microsoft VSS all'interno del computer virtuale) nei processi di backup precedenti. Ora, si intende usare l'opzione **Strumenti VMware**, ma le credenziali del computer virtuale sono cambiate (ad esempio, è stata modificata la password del sistema operativo guest ma non è stato aggiornato il nodo del computer virtuale nella Console) oppure, per qualche motivo, Strumenti VMware non è in esecuzione. In tali casi, Arcserve UDP non può annullare la distribuzione degli strumenti (che sono stati distribuiti dal processo di backup precedente) dal computer virtuale per utilizzare il nuovo metodo snapshot.

Per risolvere il problema, completare una delle seguenti fasi:

- Aggiornare il computer virtuale con le credenziali corrette. Verificare che gli Strumenti VMware siano aggiornati e in esecuzione nel sistema operativo guest del computer virtuale. Dopo la verifica, avviare di nuovo il processo di backup.
- Annullare manualmente la distribuzione degli strumenti dal computer virtuale:
    a. Accedere al computer virtuale.
    b. Navigare alla seguente cartella:

        C:\Programmi\ARCServe\ASVMOperationTools\custom-freeze-vmware-snapshot\auto-deploy

    c. Fare clic con il tasto destro del mouse sul file batch auto-undeploy.bat e selezionare Esegui come amministratore.
    d. Eliminare le seguenti cartelle:

        C:\Programmi\ARCServe\as-hbbu-vmwarebackup

        C:\Programmi\ARCServe\ASVMOperationTools

    e. Inoltrare nuovamente il processo di backup.

Disabilitazione della ripetizione della scansione delle schede HBA durante il backup incrementale

Applicabile a VMware ESX

Applicabile solo a UDP v6.5, non agli aggiornamenti v6.5.

Sintomo

Quando il nodo di origine e il server proxy si trovano su server ESX VMware diversi e si esegue un backup incrementale, il backup richiede più tempo per l'esecuzione. Inoltre, si ricevono più messaggi di ripetizione della scansione. Si desidera disabilitare la ripetizione della scansione di tutti gli adattatori bus host (hba) di altri server ESX VMware durante i backup incrementali.

Soluzione

È possibile disabilitare la scansione creando una chiave del registro di sistema nel server proxy e assegnandole un valore.

Effettuare le operazioni seguenti:

1. Accedere al computer.
2. Navigare alla seguente cartella:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
   ```

3. Creare la seguente chiave del Registro di sistema (DWORD), se non è stata già creata

   ```
   DisableAllESXNodeRescan
   ```

4. Impostare il valore della chiave del Registro di sistema su 1.

Creazione di snapshot consecutive disabilitata in un computer virtuale VMware per il backup

Nella versione precedente di Arcserve UDP, in caso di avvio simultaneo di più processi di backup per computer virtuali VMware, vengono create snapshot sull'host ESX parallelamente ai processi. A volte le operazioni di creazione delle snapshot in parallelo aumentano l'attività di I/O del disco sull'host ESX. Per evitare tale situazione, per impostazione predefinita Arcserve UDP versione 7.0 serializza l'operazione di creazione delle snapshot durante l'esecuzione dei processi sullo stesso server proxy, se tale operazione interessa lo stesso host ESX. In altre parole, le operazioni di creazione delle snapshot si verificano una dopo l'altra, creando una sola snapshot alla volta. Questa soluzione non è applicabile se i processi di backup sono in esecuzione su server proxy diversi o se interessano host ESX diversi.

Per evitare che la creazione di snapshot per un processo si blocchi o richieda molto tempo, bloccando gli altri processi, il processo successivo attende circa **cinque minuti** per consentire il completamento dell'operazione precedente. Trascorsi i cinque minuti, viene avviato il processo successivo di creazione delle snapshot.

Per disabilitare questa attesa di cinque minuti, procedere come segue:

1. Accedere al server proxy.
2. Aprire la chiave del Registro di sistema dal percorso seguente:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

3. Creare un valore DWORD con il nome **CreateSnapshotSequentially**.
4. Impostare il valore su 0.

Invece, per modificare il valore di timeout predefinito (5 minuti), procedere come segue:

1. Accedere al server proxy.
2. Aprire la chiave del Registro di sistema dal percorso seguente:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

3. Creare un valore DWORD con il nome **CreateSnapshotTimeout**.
4. Impostare un valore numerico.

   L'unità di misura è il secondo.

Blocco in fase di avvio del computer virtuale in seguito al ripristino da una versione successiva dell'host ESXi a una versione precedente dell'host ESXi

Dopo il ripristino da una versione successiva dell'host ESXi a una versione precedente dell'host ESXi, il computer virtuale viene interrotto durante l'avvio in seguito all'accensione.

Valido per piattaforme Windows. Valido solo per il computer virtuale VMware.

Sintomo

Ripristinare un computer virtuale da una versione successiva dell'host ESXi a una versione precedente dell'host ESXi, quindi attivare il computer virtuale. Il computer virtuale si blocca durante la fase di avvio.

Soluzione

La versione del sistema operativo guest del computer virtuale potrebbe non essere supportata dalla versione precedente di ESXi. Per risolvere il problema, è possibile utilizzare una delle seguenti opzioni:

- Ripristinare il computer virtuale su un ESXi che supporta tale versione del sistema operativo guest oppure
- Eseguire l'aggiornamento dell'host ESXi esistente alla versione appropriata.

Ad esempio, è stato eseguito il backup di un computer virtuale con Windows Server 2012 R2 da ESXi 5.5 con il ripristino su ESXi 5.0 Aggiornamento 1. Poiché ESXi 5.0 ha avviato il supporto del sistema operativo guest Windows Server 2012 R2 in seguito all'Aggiornamento 2, è possibile che si verifichi questo problema.

È necessario eseguire l'aggiornamento da ESXi 5.0 aggiornamento 1 all'aggiornamento 2 in modo che il sistema operativo guest Windows Server 2012 R2 sia supportato. Per risolvere il problema, è possibile modificare la versione del sistema operativo guest del computer virtuale ripristinato alla versione supportata dalla versione corrente di ESXi (nell'esempio riportato precedentemente, modificarlo in Windows Server 2008 R2).

Nota: Questa soluzione alternativa potrebbe non risolvere il problema.

RAM utilizzata al 99% durante l'inoltro dei processi di backup al computer virtuale

La RAM viene utilizzata al 99% quando si inoltrano i processi di backup ai computer virtuali su un volume CSV di Windows 2012 Hyper-V.

Sintomo

Durante il backup dei computer virtuali inclusi nel cluster Hyper-V 2012, l'utilizzo della RAM aumenta gradualmente fino a raggiungere il 99% sull'host Hyper-V proprietario del volume CSV. Di conseguenza, i computer virtuali e l'host Hyper-V si arrestano durante il backup.

Soluzione

Questo problema è dovuto a errori noti nel codice di Microsoft.

Per risolverlo, scaricare e applicare l'aggiornamento rapido fornito da Microsoft su tutti gli host Hyper-V dal collegamento seguente:

https://support.microsoft.com/en-in/kb/2878635

Errore del processo di ripristino Hyper-V. Errore di connessione dell'utilità sull'host

Il processo di ripristino del computer virtuale Hyper-V produce non riesce e viene visualizzato un messaggio di errore.

Sintomo

L'esecuzione del ripristino di un computer virtuale Hyper-V non riesce e viene visualizzato un messaggio di errore nel registro attività:

Impossibile stabilire la connessione all'utilità di ripristino Hyper-V sull'host xxxxx

Nel registro di debug del processo di ripristino viene visualizzato il seguente messaggio di errore:

Impossibile stabilire la connessione a xxxxx:10218. Errore: Tentativo di connessione scaduto senza aver stabilito una connessione ((rc=-536805332)

Impossibile stabilire la connessione a xxxxx:10218, errore-536805332

Soluzione

In genere, il problema si verifica poiché la connessione tra il proxy di backup e l'host Hyper-V è bloccata dal firewall. Se possibile, disattivare il firewall ed eseguire nuovamente il ripristino. Se non è possibile disattivare il firewall, registrare la porta (o l'intervallo di porte) utilizzato dal processo di ripristino nell'eccezione firewall.

Per impostazione predefinita, il processo di ripristino sceglie casualmente una porta disponibile nell'intervallo compreso tra 1024 e 65535. È possibile specificare manualmente l'intervallo in base ai valori del registro di sistema impostati nell'host Hyper-V.

Effettuare le operazioni seguenti:

1. Accedere all'host Hyper-V.
2. Eseguire il comando *regedit* per aprire l'editor del registro di sistema.
3. Accedere alla seguente chiave del registro di sistema (le chiavi vengono create nel caso in cui non esistano):

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\HyperVRestoreStub
4. Creare i seguenti due valori di registro (DWORD):

   PortMin

   PortMax

5. Specificare i valori corrispondenti al numero iniziale e finale dell'intervallo di porte.

   Note:

   - Intervallo obbligatorio dei valori specificati: 1024-65535
   - È possibile specificare lo stesso numero per entrambi i valori del registro di sistema. In questo caso, il numero di porta fisso viene utilizzato per il processo di ripristino. Se vengono eseguiti processi di ripristino simultanei e la porta è occupata di un processo di ripristino, gli altri processi di ripristino produrranno un errore.

Errore della protezione automatica durante il rilevamento e la protezione del computer virtuale

Il computer virtuale non viene rilevato e pertanto non viene protetto in modo automatico.

Sintomo

Sebbene un computer virtuale possa essere visualizzato in un hypervisor ((vCenter/ESX o Hyper-V) da un'applicazione client nativa (ad esempio, vSphere Client o Hyper-V Manager), la protezione automatica non viene rilevata, pertanto il computer virtuale non può essere protetto automaticamente.

Motivi

- Il computer virtuale non dispone di uno stato valido nell'hypervisor. Ad esempio, la protezione automatica ignora i computer virtuali con stato Disconnesso, Orfano o Non accessibile in vCenter/ESX.
- Il computer virtuale viene creato da attività Arcserve UDP come Virtual Standby (VSB), Computer virtuale istantaneo o Assured Recovery (AR) (oppure con clonazione da computer virtuali VSB/IVM/AR). Arcserve UDP ignora intenzionalmente tali computer virtuali a causa delle seguenti considerazioni:
  - Il backup di computer virtuali Arcserve UDP da parte di VSB/IVM/AR senza l'imposizione di alcun limite potrebbe comportare una situazione *in loop di backup infinito*. Ad esempio, utilizzare la protezione automatica per proteggere lintero ambiente ESX. Nel piano di backup, dopo aver aggiunto l'attività di backup, aggiungere un'attività VSB in grado di creare un computer virtuale VSB nello stesso ambiente ESX. Pertanto, dopo il primo backup una nuova VM VSB viene creata nell'archiviazione ESX. Il nuovo computer virtuale VSB viene rilevato automaticamente dalla protezione automatica e viene aggiunto al piano di backup. Durante l'esecuzione del backup successivo, viene creato un nuovo computer virtuale VSB, il quale viene aggiunto al piano di backup. Il processo continua finché l'archiviazione ESX esaurisce lo spazio libero.
  - Per i computer virtuali IVM/AR di Linux, a meno che la migrazione dell'archiviazione esegua la conversione in un computer virtuale normale, Arcserve UDP non è in grado di eseguire il backup del computer virtuale. Il backup del processo verrà completato, tuttavia non sarà possibile eseguire il ripristino del punto di ripristino sottoposto a backup.

Questa situazione si verifica a causa di una limitazione tecnica dell'implementazione IVM di Linux.

Soluzione

Se si desidera eseguire il backup di computer virtuali VSB/IVM/AR, oppure i computer virtuali sono stati convertiti in computer virtuali indipendenti da una migrazione di clonazione o di archiviazione, attenersi alla procedura riportata di seguito per i computer virtuali vSphere e Hyper-V in modo da consentire alla protezione automatica di rilevare e proteggere i computer virtuali.

Per il computer virtuale vSphere

1. Accedere al client Web vSphere e individuare il computer virtuale.
2. Disattivare il computer virtuale.
3. Fare clic con il tasto destro del mouse sul computer virtuale e selezionare Modifica impostazioni dal menu.
4. Selezionare la scheda **Opzioni computer virtuale** ed espandere la sezione Avanzate.
5. Fare clic su **Modifica configurazione**.
6. Nella finestra di dialogo Parametri di configurazione, individuare il parametro contenente uno dei seguenti nomi:
   - VCM
   - UDP_IVM
   - UDP_ARVM
   - UDP_IVM_LINUX
   - UDP_VSBVM
   - UDP_ARVM_LINUX
   - UDP_ARIVM_LINUX
7. Cancellare i valori del parametro e fare clic su **OK** per salvare.

Per il computer virtuale Hyper-V

1. Accedere all'host Hyper-V e aprire Gestione Hyper-V.
2. Individuare il computer virtuale.
3. Fare clic con il tasto destro del mouse sul computer virtuale e selezionare Impostazioni dal menu.

4. Nella finestra di dialogo Impostazioni, selezionare Nome nel riquadro sinistro.
5. Rimuovere tutte le righe che iniziano con le stringhe seguenti:
   - VCM
   - UDP_IVM
   - UDP_ARVM
   - UDP_IVM_LINUX
   - UDP_VSBVM
   - UDP_ARVM_LINUX
   - UDP_ARIVM_LINUX
6. Fare clic su **OK** per salvare.

Impostazione della dimensione del blocco di lettura durante il backup del file VMDK

Sintomo

In un determinato ambiente, la velocità effettiva di backup del computer virtuale VMware è compromessa dalla dimensione del blocco di lettura durante il backup del file VMDK.

Soluzione

Per impostazione predefinita, la dimensione del blocco di lettura VMDK corrisponde a 2 MB. È possibile modificare le dimensioni.

Effettuare le operazioni seguenti:

1. Accedere al proxy di backup senza agente.
2. Eseguire il comando *regedit* per aprire l'editor del registro di sistema.
3. Accedere alla chiave di registro seguente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll
4. Creare i valori del registro di sistema (DWORD) utilizzando il seguente nome:

   ReadVirtualDiskBlockSizeKB
5. Specificare il valore desiderato come dimensione del blocco di lettura (l'unità è KB).

Prenotazione dello spazio LUN acquisita tramite l'esecuzione del clone Lun

Sintomo

Quando viene eseguito il clone Lun durante il backup mediante la snapshot hardware, la prenotazione dello spazio viene ereditata per impostazione predefinita dal Lun di origine.

Soluzione

È necessario utilizzare la chiave di registro fornita da Arcserve UDP per disattivare la protezione di spazio. La chiave di registro è disponibile nel percorso seguente:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

DisableLunSpaceReservation =1

Specifica che le prenotazioni di spazio Lun sono disattivate.

Nota: questa opzione è valida solo quando viene applicata la licenza FlexClone.

Per ulteriori informazioni, consultare la sezione Considerazioni sul supporto per VMware NetApp iSCSI/FC.

Problemi correlati a Virtual Standby

In questa sezione verranno illustrati i seguenti argomenti sulla risoluzione dei problemi relativi a Virtual Standby:

- Sistema operativo non trovato
- Errore dei processi di standby virtuale causato da errori interni
- Errore dei processi Virtual Standby mediante la modalità di trasporto HotAdd
- Errore dei processi Virtual Standby verso sistemi Hyper-V
- Problema relativo alla duplicazione dell'agente UUID
- Opzione Risorse Terminal EC2 non visualizzata[CDATA[ ]]>

Sistema operativo non trovato

Valido per piattaforme Windows.

Sintomo:

Il seguente messaggio viene visualizzato in caso di errore di attivazione del computer virtuale Virtual Standby.

Sistema operativo non trovato.

Soluzione:

Il comportamento descritto può inoltre verificarsi su computer virtuali contenenti periferiche SCSI e IDE. Se il problema si verifica, verificare la configurazione dei dischi sul computer virtuale e accertarsi che la sequenza di avvio del computer virtuale di cui è stato eseguito il recupero corrisponda all'origine del computer virtuale. Se la sequenza di avvio è differente, sarà necessario aggiornare il BIOS del computer virtuale di cui è stato eseguito il recupero corrispondente all'origine.

Nota: utilizzare (0:1) per rappresentare il primo disco IDE.

Errore dei processi di standby virtuale causato da errori interni

Valido per i sistemi operativi Windows.

Sintomo 1:

I processi di standby virtuale producono errori. In Registro attività appare uno dei seguenti messaggi:

Impossibile convertire il disco virtuale

Si è verificato un errore interno. Contattare il Supporto tecnico di CA.

Inoltre, VDDK riporta il seguente messaggio di errore:

Errore sconosciuto.

Soluzione 1:

Per risolvere il problema, considerare quanto segue:

- Le operazioni di conversione potrebbero avere esito negativo se non si dispone di spazio su disco sufficiente nell'archivio dati specificato nel criterio Virtual Standby. VDDK restituisce questo messaggio in quanto l'API di VDDK non supporta la funzionalità che consente di rilevare la quantità di spazio disponibile sul disco dell'archivio dati. Per risolvere il problema, liberare lo spazio su disco dell'archivio dati originale necessario per il completamento dell'operazione, quindi inoltrare nuovamente il processo.
- I disturbi di rete ed un traffico di rete elevato possono comportare un errore dei processi di conversione. Per risolvere il problema, verificare che il nodo di origine e il sistema server ESX o vCenter siano in grado di comunicare attraverso la rete, quindi inviare nuovamente il processo.
- Possono verificarsi errori dovuti a connessioni multiple simultanee di processi di backup o recupero di computer virtuali verso sistemi server ESX o vCenter, comprese le connessioni vSphere SDK mediante il client VMware vSphere. Per correggere il problema, chiudere le connessioni non necessarie e inviare nuovamente il processo.

  Il problema è causato da una limitazione della connessione di VMware VDDK. I seguenti limiti del protocollo NFC (Network File Copy) si applicano:

  ESXi 5: limitato da un buffer di trasferimento per tutte le connessioni NFC e applicato dall'host. La somma di tutti i buffer di connessione NFC a un host ESXi non può superare i 32 MB. 52 connessioni mediante il server vCenter, compreso il limite per host.

Nota: le connessioni non possono essere condivise tra dischi. I valori massimi non sono applicabili a connessioni HotAdd o SAN. Se il client NFC non si chiude correttamente, le connessioni possono rimanere aperte per dieci minuti.

- Esaminare le sezioni Attività ed Eventi del log client VMware vSphere per rilevare errori interni per un computer virtuale specifico. Correggere gli errori interni e inviare nuovamente il processo.

  Esempio: il file VMDK è utilizzato da un'altra applicazione o un'altra operazione. Per risolvere il problema, rilasciare il file e inviare nuovamente il processo.

Sintomo 2:

I processi di standby virtuale producono errori. In Registro attività appare uno dei seguenti messaggi:

Impossibile convertire il disco virtuale

Si è verificato un errore interno. Contattare il Supporto tecnico di CA.

Inoltre, VDDK riporta il seguente messaggio di errore:

L'apertura di vmdk ha prodotto un errore. File non trovato.

Soluzione 2:

Questo problema può verificarsi quando:

- VDDK non ha elaborato una snapshot correttamente.
- VDDK non ha eliminato una snapshot manualmente o interna al computer virtuale.

Per risolvere il problema, inviare nuovamente il processo. Se il processo produce nuovamente un errore, eliminare il computer virtuale di cui è stato eseguito il recupero e inviare nuovamente il processo.

Sintomo 3:

I processi di standby virtuale producono errori. In Registro attività appare uno dei seguenti messaggi:

Impossibile applicare <Plan Name> al nodo <Node Name>'. Il servizio Web dell'agente Arcserve UDP sul convertitore <Converter Name> è occupato. Riprovare in un secondo momento.

Inoltre, il file di registro della Console UDP (ARCApp.log) riporta il seguente messaggio di errore:

[ERROR] deployVsbTask: Failed to invoke D2D web service API - timeout. javax.xml.ws.WebServiceException: java.net.SocketTimeoutException: Read timed out

Soluzione 3:

Questo problema può verificarsi a causa del timeout. Per risolvere il problema, attenersi alla seguente procedura:

1. Accedere alla **Console UDP** con le credenziali appropriate.
2. Aprire l'interfaccia della riga di comando ed eseguire il seguente comando:

   regedit

   Viene visualizzato il Registro di sistema.
3. Accedere a ***\SOFTWARE\Arcserve\Unified Data Protection\Engine\WebService***.
4. Verificare l'esistenza della chiave **timeoutValue**. Se la chiave non esiste, crearla manualmente.

   Aggiungere/modificare una nuova chiave come indicato di seguito:

   - **Nome chiave:** timeoutValue
   - **Valore:** <immettere il valore in minuti>. Ad esempio, se si desidera impostare il valore di timeout su 20 minuti, specificare 20 come valore.
5. Uscire da **regedit**.
6. Accedere alla cartella di installazione della **Console UDP**. Ad esempio, *C:\Programmi\Arcserve\Unified Data Protection\Management\Configuration*.
7. Aprire il file **ConsoleConfiguration.xml** tramite il Blocco note.
8. Individuare il testo sottostante nella sezione **<TimeoutConf>**:

   <webServiceRequestTimeout>600</webServiceRequestTimeout>
9. Modificare il valore di **webServiceRequestTimeout** in secondi. Ad esempio, se si desidera impostare il valore di timeout su 20 minuti, specificare 1200 come valore.
10. **Salvare** il file e uscire.
11. **Riavviare** il **servizio di gestione della Console UDP** per rendere effettive le impostazioni.
12. Ridistribuire il piano e verificarne il risultato.

Errore dei processi Virtual Standby mediante la modalità di trasporto HotAdd

Valido per piattaforme Windows.

Sintomo:

Si verifica un errore delle operazioni di recupero durante il recupero dei dati mediante la modalità di trasporto HotAdd. Il seguente messaggio viene visualizzato nel Registro attività:

Si è verificato un errore sconosciuto. Contattare il supporto tecnico.

Inoltre, VDDK riporta il seguente messaggio di errore:

Errore sconosciuto.

Soluzione:

Le operazioni di ripristino hanno esito negativo con la modalità di trasporto HotAdd quando le impostazioni del disco non sono configurate correttamente.

Per configurare il disco, attenersi alla procedura seguente:

1. Accedere al sistema proxy di backup mediante un account con privilegi di amministratore.

   Aprire la riga di comando di Windows.

2. Dalla riga di comando, immettere il seguente comando:

   diskpart

   Premere Invio.

   Digitare SAN, quindi premere Invio.

   Vengono visualizzati i criteri SAN correnti.

3. Digitare il seguente comando:

   SAN POLICY = OnlineAll

   Premere Invio.

   Il criterio SAN viene configurato in modo da non eseguire il montaggio automatico dei volumi SAN.

4. Per cancellare l'attributo di sola lettura di un determinato disco SAN, selezionare il disco dall'elenco, quindi immettere il seguente comando:

   attribute disk clear readonly

   Premere Invio.

5. Digitare exit, quindi premere Invio.

Il disco viene configurato e sarà possibile inoltrare nuovamente il processo. Se il processo riporta ancora errori, montare i dischi HotAdd manualmente utilizzando la gestione disco sul sistema proxy.

Per montare i dischi manualmente, attenersi alla procedura seguente:

1. Accedere al sistema proxy di backup mediante un account con privilegi di amministratore.

   Aprire il Pannello di controllo di Windows e fare doppio clic su Strumenti di amministrazione.

   Viene visualizzata la finestra di dialogo degli strumenti di amministrazione.

2. Dall'elenco Preferiti, fare doppio clic su Gestione computer.

   Viene visualizzata la finestra della Gestione computer.

3. Espandere Archiviazione, quindi fare clic sulla Gestione disco.

   Vengono visualizzati i dischi.

4. Fare clic con il tasto destro del mouse sul disco che si desidera montare, quindi fare clic su In linea.

   Il disco viene montato e sarà possibile inoltrare nuovamente il processo.

Errore dei processi Virtual Standby verso sistemi Hyper-V

Valido per i sistemi operativi Windows.

Sintomo:

Il seguente messaggio viene visualizzato nel Registro attività:

Impossibile acquisire il computer virtuale Hyper-V durante il processo Virtual Standby.

Soluzione:

I processi Virtual Standby non riescono quando:

- Il servizio Web Virtual Standby non è in grado di recuperare informazioni relative al computer virtuale dal sistema Hyper-V. Si verificano problemi di comunicazione tra il server Arcserve UDP e il sistema Hyper-V quando i server Hyper-V richiesti non vengono eseguiti sul sistema Hyper-V.

  Soluzione: Verificare che tutti i servizi Hyper-V siano in esecuzione sul sistema Hyper-V.

- Il sistema Hyper-V non dispone di spazio su disco sufficiente per la creazione del computer virtuale Virtual Standby o per la creazione di una snapshot del computer virtuale Virtual Standby.

  Soluzione: Riconfigurare il sistema Hyper-V per liberare spazio su disco nel volume di sistema.

Nota: Se vengono rilevate altre possibili cause, contattare il Supporto tecnico di Arcserve.

Problema relativo alla duplicazione dell'agente UUID

Sintomo:

Un monitor presente nella Console con lo stesso agente UUID deve sovrascrivere l'agente UUID.

Soluzione:

1. Dal computer, eseguire *regedit*.
2. Visualizzare il percorso: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine*
3. Eliminare i dati valore di NodeID.
4. Riavviare il servizio dell'agente Arcserve UDP.

Le modifiche apportate a Virtual Private Cloud nell'attività Virtual Standby non vengono riportate in Amazon EC2

Sintomo:

Dopo l'esecuzione di un'attività Virtual Standby, se si modifica Virtual Private Cloud (VPC) nelle Impostazioni di rete dell'attività Virtual Standby per l'utilizzo di un VPC Amazon differente per le attività successive, le modifiche non vengono aggiornate in Amazon EC2.

Soluzione

Amazon EC2 non consente la modifica di VPC dalla Console UDP dopo l'esecuzione di un'attività Virtual Standby almeno una volta. Come soluzione alternativa, ora Arcserve UDP consente di terminare l'istanza precedente e creare una nuova istanza con i dati esistenti delle sessioni precedenti.

Effettuare le operazioni seguenti:

1. Configurare un piano di backup in EC2 tramite VSB come attività secondaria.
2. Eseguire correttamente alcune attività VSB in AWS.
3. Modificare l'impostazione VPC nell'attività VSB [impostazioni di rete].

   Le impostazioni VPC aggiornate vengono visualizzate nell'istanza dopo la successiva attività VSB completata.

Note:

- L'istanza precedente creata in EC2 viene ignorata e in EC2 viene creata la nuova istanza con le impostazioni VPC aggiornate per riflettere le modifiche alla rete.
- Le nuove impostazioni di vengono applicate anche alle snapshot precedenti.

Opzione Risorse Terminal EC2 non visualizzata

Sintomo:

Quando i nodi vengono configurati con un piano dotato di Virtual Standby sull'attività EC2 in UDP 7.0 U1, UDP 7.0 o UDP 6.5 U4 e si esegue l'aggiornamento della console a UDP 7.0 U2, l'opzione **Risorse Terminal EC2** non viene visualizzata per quei nodi specifici.

Soluzione:

Fare clic sull'opzione **Modifica** per il piano corrispondente e salvarlo.

Problemi correlati alla copia del punto di ripristino

In questa sezione verranno illustrati i seguenti argomenti sulla risoluzione dei problemi relativi alla copia dei punti di ripristino (CRP):

- Congestione della larghezza di banda con i processi di copia del punto di ripristino su cloud
- Configurazione del registro per il processo di copia del punto di ripristino
- Processo di unione ignorato

Configurazione del registro per il processo di copia del punto di ripristino

Sintomo

Il processo Copia punto di ripristino (CRP) non viene eseguito.

Soluzione

È possibile controllare il numero di ripetizioni e il relativo intervallo di tempo per l'attività Copia punto di ripristino utilizzando le seguenti chiavi del Registro di sistema. La chiave del Registro di sistema è disponibile nel computer in cui è stato installato l'agente UDP.

Ripetere il processo CRP.

La chiave del Registro di sistema è disponibile nell'agente Arcserve UDP al percorso seguente:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession\nodename1

Aggiungere una nuova chiave come indicato di seguito:

Nome chiave: MaxRetryCount

Tipo di chiave: REG_DWORD

Valore: 1 come predefinito e massimo (10)

Nota: Questo aggiornamento è applicabile a un solo nodo "nodename1".

Per i processi di copia del punto di ripristino su cloud, Arcserve UDP utilizza un percorso temporaneo, che può essere configurato con le chiavi del Registro di sistema per il percorso Temp.

Configurare il percorso temporaneo.

La chiave del Registro di sistema si trova nel server Arcserve Backup al percorso seguente:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession

Nome chiave: LocalTempPath

Tipo di chiave: REG_SZ

Nota: Per impostazione predefinita, è archiviata nel percorso della directory principale del prodotto Arcserve.

Congestione della larghezza di banda con i processi di copia del punto di ripristino su cloud

Sintomo

I processi di copia dei punti di ripristino (CRP) in esecuzione provocano spesso il rallentamento del computer dell'agente a causa della congestione della larghezza di banda.

Soluzione

Arcserve consente di definire una larghezza di banda specifica per i processi CRP. Di conseguenza, anche se il computer presenta più processi in esecuzione, la larghezza di banda è controllata automaticamente sul computer dell'agente solo per i processi CRP. Mediante un processo distinto AFCRPBackend.exe per i processi CRP, è possibile configurare la QoS basata su criteri per AFCRPBackend.exe e limitare la velocità della larghezza di banda in uscita.

Effettuare le operazioni seguenti:

1. Digitare MMC nella casella Inizia ricerca e premere Invio.

   Viene aperta la Microsoft Management Console.

2. Dalla console MMC, premere CTRL+M.

   Viene visualizzata la finestra di dialogo Aggiungi o rimuovi snap-in.

3. Dalla finestra di dialogo Aggiungi o rimuovi snap-in, selezionare Editor oggetti Criteri di gruppo in Snap-in disponibili, quindi fare clic su Aggiungi.

4. Nella finestra di dialogo Selezione oggetto Criteri di gruppo, lasciare l'impostazione predefinita Computer locale e fare clic su Fine.

5. Fare clic su OK.

   La finestra di dialogo Aggiungi o rimuovi snap-in viene chiusa.

6. Dal riquadro sinistro della finestra della console MMC, espandere Computer locale, Configurazione computer, Impostazioni di Windows, fare clic con il pulsante destro del mouse su QoS basata su criteri e selezionare Crea nuovo criterio dal menu.

7. Nelle finestre relative alla QoS basata su criteri, selezionare le opzioni seguenti e fare clic su Avanti:

   - Immettere il nome del nuovo criterio.

   - Impostare il valore DSCP su 0.

   - Selezionare la casella di controllo Specifica velocità in uscita.

Nota: Si consiglia di selezionare l'opzione MBps.

8. Per l'opzione Questo criterio QoS viene applicato a, selezionare la casella di controllo Solo le applicazioni con questo nome di eseguibile, quindi immettere il seguente percorso exe e fare clic su Avanti:

   C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN\AFCRPBackend.exe

   Nota: AFCRPBackend.exe garantisce che la limitazione della larghezza di banda sia applicabile solo ai processi CRP, anche se sono in esecuzione più processi sul computer dell'agente.

9. Mantenere le impostazioni predefinite fino all'ultima schermata e fare clic su Fine.

Processo di unione ignorato

Sintomo

- Il processo di unione è stato ignorato perché la sessione è attualmente bloccata dal processo Copia punto di ripristino. Verificare se dei processi Copia punto di ripristino sono in sospeso.
- Il processo di unione è stato ignorato perché la sessione è attualmente bloccata dal processo Copia punto di ripristino su richiesta. Il processo Copia punto di ripristino su richiesta è in esecuzione o in attesa di esecuzione.

Soluzione

Per continuare il processo di unione è necessario rimuovere i file di blocco dalla destinazione di backup del nodo.

Eseguire lo strumento di blocco Elimina da *C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN\AFDeleteLockTool.exe*.

Nota: Questo strumento elimina tutti i blocchi relativi al processo CRP (CRP pianificato e CRP ad hoc) e l'unione inizia immediatamente. Le sessioni unite non saranno disponibili per essere copiate nella destinazione dal processo CRP.

Uso:

AFDeleteLockTool.exe -path <BackupDestinationPath> -user <USERNAME> -password <PASSWORD> -type <crp/adhoccrp>

Note:

-path: -specificare il percorso di destinazione di backup

-type: -specificare tipo di attività per eliminare il blocco

crp: elimina il blocco relativo ai processi CRP pianificati.

adhoccrp: elimina il blocco relativo ai processi CRP ad hoc.

-user: -specifica nome utente per la destinazione di backup

-password: -specificare la password per la destinazione di backup

-path e -type sono obbligatori

-user e -password sono facoltativi. (Fornirli o ignorarli entrambi).

Esempi:

- Se si desidera rimuovere solo i blocchi di attività CRP pianificate, eseguire lo strumento come indicato di seguito:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -type crp

- Se si desidera rimuovere solo i blocchi del processo CRP ad-hoc, eseguire lo strumento come indicato di seguito:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -user User123 -password "**********" -type crp

- Se si desidera rimuovere tutti i blocchi CRP, eseguire lo strumento come indicato di seguito:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -user User123 -password "**********" -type crp -type adhoccrp

Problemi correlati ai rapporti Arcserve UDP

In questa sezione verranno illustrati i seguenti argomenti sulla risoluzione dei problemi relativi ad Arcserve UDP:

Visualizzazione dei grafici a barre per i rapporti Arcserve UDP

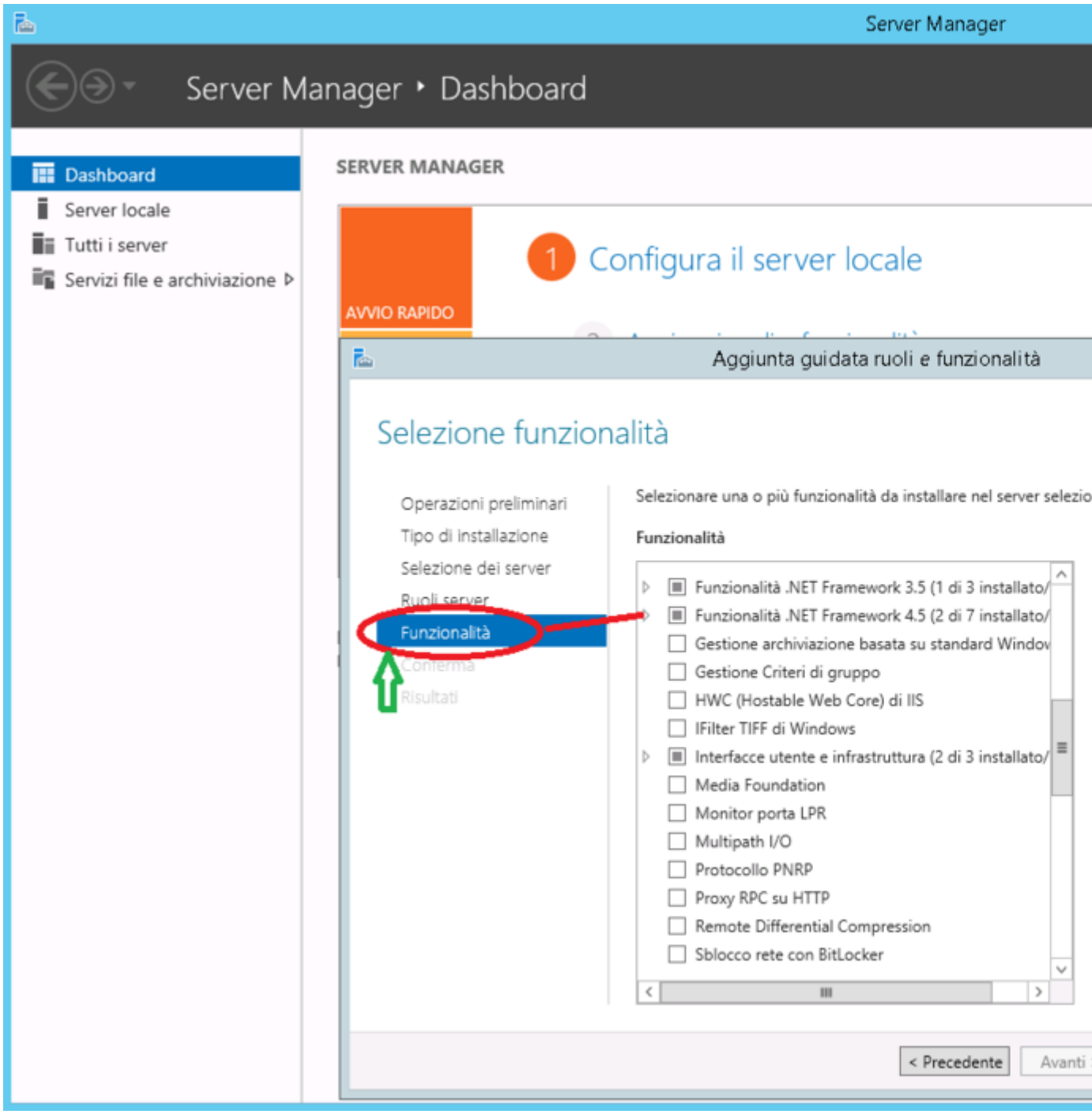
Visualizzazione dei grafici a barre per visualizzare i rapporti Arcserve UDP

In alcuni casi i grafici potrebbero non essere visualizzati durante la visualizzazione dei rapporti. Completare i prerequisiti seguenti per risolvere il problema per Windows 2012/2012r2.

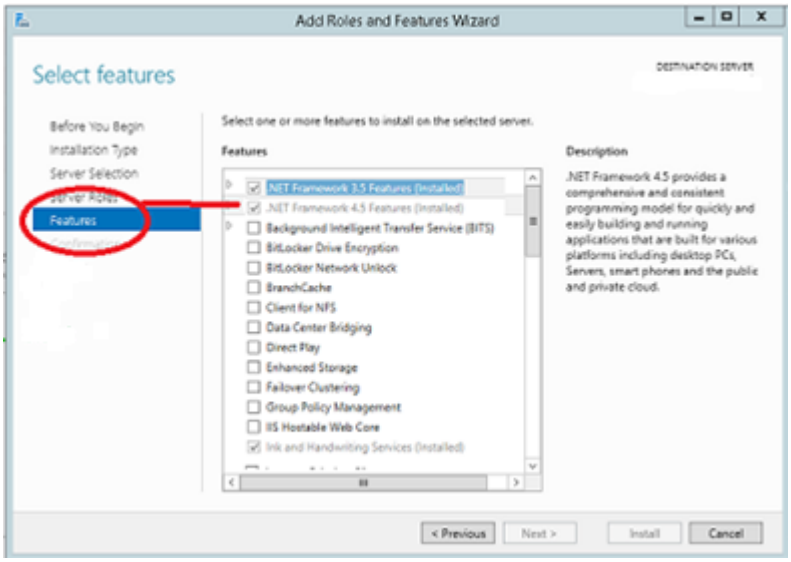
Per visualizzare i grafici, è necessario installare .NET 3.5 Framework (o versioni successive).

Per installare .NET Framework, procedere come segue:

1. Aprire Server Manager.
2. Nel Dashboard, dall'angolo superiore destro fare clic su **Gestisci**, quindi selezionare l'opzione **Aggiungi ruoli e funzionalità**.



3. Nella finestra di dialogo Procedura guidata di aggiunta ruoli o funzionalità, procedere come segue:
   a. Dal riquadro sinistro, fare clic su **Funzionalità**.
   b. Nella scheda **Funzionalità**, selezionare la casella di controllo **Funzionalità .NET Framework 3.5 (Installate)**.
   c. Fare clic su **Avanti**.



4. Dalla schermata Conferma selezioni per l'installazione, fare clic su **Installa**.

   L'installazione di .NET Framework è stata completata correttamente.

   Importante: Se, anche dopo aver completato questi tre prerequisiti, i grafici non vengono visualizzati utilizzando le opzioni di **stampa/invio tramite posta elettronica/salvataggio**, verificare che l'editor del Registro di sistema contenga il file FCImgExportDll. Per verificare la DLL, accedere al percorso seguente:

   C:\Programmi\Arcserve\Unified Data Protection\Management\BIN

   Per annullare la registrazione e registrare FCImgExportDLL.dll, procedere come segue:

   1. Accedere al seguente percorso nel prompt dei comandi:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319

   2. Per annullare la registrazione della DLL, eseguire il seguente comando:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319>Regasm.exe /u "C:\Programmi\Arcserve\Unified Data Protection\Management\BIN\FCImgExportDLL.dll"

   3. Per registrare la DLL, eseguire il comando seguente:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319>Regasm.exe "C:\Programmi\Arcserve\Unified Data Protection\Management\BIN\FCImgExportDLL.dll" /codebase

Problemi correlati a Microsoft Exchange Online Office 365

Questa sezione include i seguenti argomenti di risoluzione dei problemi relativi a Microsoft Office 365 Exchange Online:

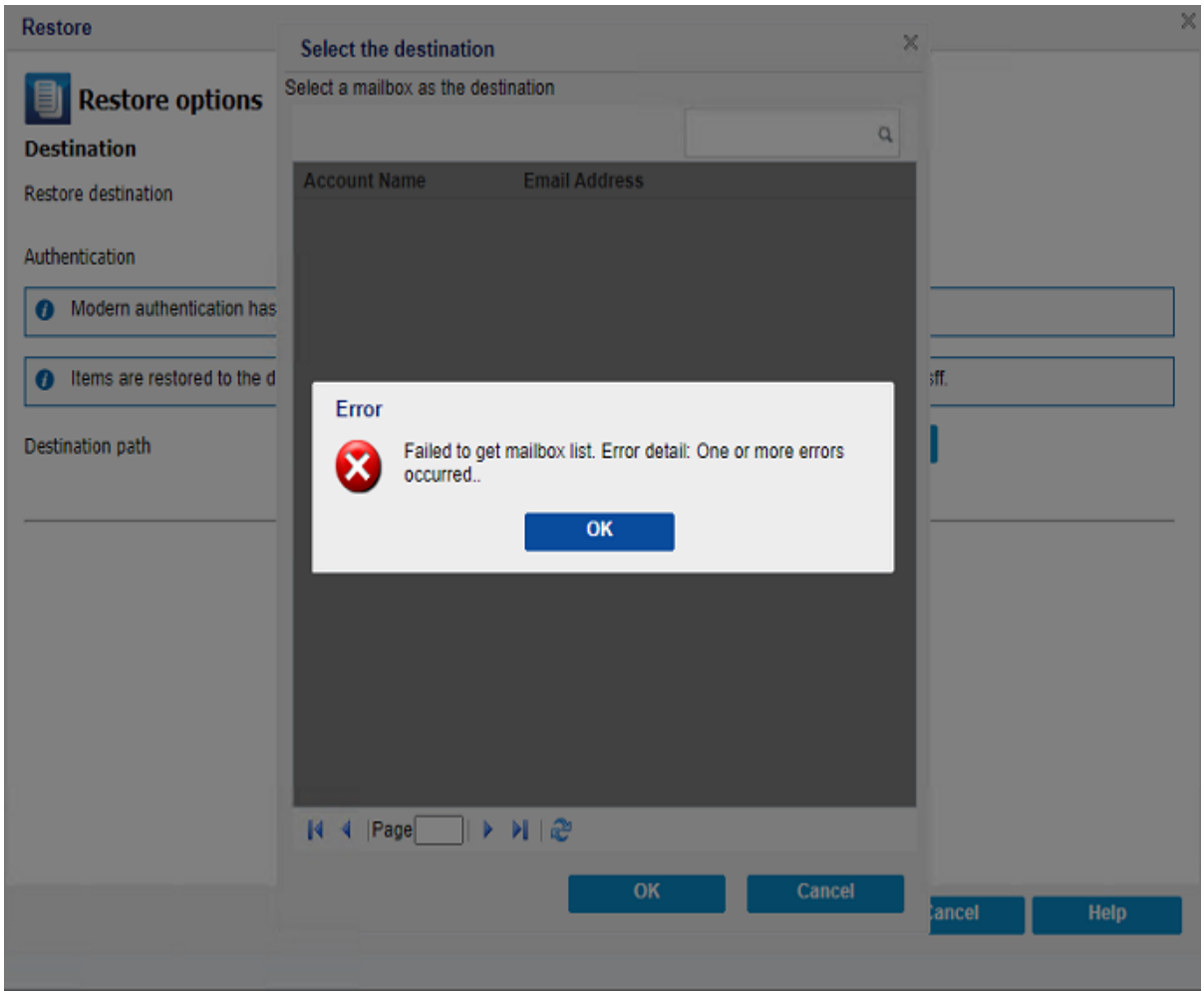
- Errore di visualizzazione dell'elenco delle caselle di posta nella finestra di dialogo *Seleziona destinazione*
- Accesso o autorizzazione negata per il gruppo Exchange Online

Errore di visualizzazione dell'elenco delle caselle di posta nella finestra di dialogo *Seleziona destinazione*

Sintomo:

Durante la definizione delle opzioni di ripristino, nella finestra di dialogo Seleziona destinazione non viene visualizzato l'elenco delle caselle di posta. Quando si ripristinano i dati di posta elettronica in una posizione alternativa utilizzando l'autenticazione esistente e si fa clic sul pulsante Sfoglia per selezionare una destinazione, viene visualizzato il seguente messaggio di errore:

Impossibile ottenere l'elenco delle caselle di posta. Dettagli errore: si sono verificati uno o più errori.



Soluzione:

Per risolvere questo errore, caricare un certificato valido nel portale Azure sotto l'ID applicazione specificato. Per ulteriori informazioni, consultare la sezione Utilizzo del certificato autofirmato.

Accesso o autorizzazione negata per il gruppo Exchange Online

Sintomo:

Quando non è presente alcuna casella postale associata al gruppo privato Teams, viene visualizzato il seguente messaggio di errore:

Backup della casella di posta [abcd-pvt-group] non riuscito: Accesso negato

Soluzione:

Per risolvere il problema, attenersi alla procedura seguente:

1. Creare una casella di posta condivisa:
    a. Accedere alla pagina di accesso di Microsoft, quindi accedere all'account di amministrazione di Microsoft Office 365.
    b. Accedere alla pagina dell'interfaccia di amministrazione di Exchange Online.
    c. In Dashboard, accedere a **destinatari** > **condivisi**.
    d. Fare clic su **+** per aggiungere o creare una casella di posta condivisa.
2. Impostare una password e assegnare la licenza di Office 365 per la casella di posta condivisa:
    a. Tornare all'account di amministratore di Office 365.
    b. Accedere a **Utenti** > **Utenti attivi**, quindi selezionare la casella di posta condivisa.
    c. Impostare la password e assegnare la licenza di Office 365.
3. Aggiungere la casella di posta condivisa come membro del gruppo privato:
    a. Accedere alla pagina dell'interfaccia di amministrazione di Exchange Online, quindi fare clic su **Gruppi** da Dashboard.
    b. Selezionare la casella di posta privata, quindi fare clic su **Modifica**.
    c. Nella pagina Modifica impostazioni, aggiungere la casella di posta condivisa come membro del gruppo, quindi fare clic su **Salva**.
4. Aggiungere la casella di posta condivisa per l'amministratore globale:
    a. Accedere al portale Azure.
    b. Accedere alla sezione Ruoli, quindi selezionare il ruolo di amministratore globale.
    c. Fare clic su **Aggiungi assegnazioni**, selezionare la casella di posta condivisa, quindi fare clic su **Salva**.
5. Sulla console UDP, aggiornare il nodo con l'indirizzo di posta elettronica della casella di posta condivisa, quindi eseguire nuovamente il processo di backup.
6. Verificare che il processo di backup sia stato eseguito correttamente.

Chapter 13: Appendice

La presente sezione descrive i seguenti argomenti:

Strumento della riga di comando per l'archivio dati di deduplicazione

Lo strumento della riga di comando (as_gddmgr.exe) consente di controllare l'integrità dei dati a livello del punto di ripristino e dell'archivio dati per gli archivi dati di deduplicazione.

È possibile utilizzare questo strumento per rigenerare un database hash in caso di errore. È possibile utilizzare questo strumento anche per eseguire una query e gestire l'eliminazione back-end e il recupero del disco per gli archivi dati di deduplicazione.

L'output del comando viene visualizzato nella console del comando di Windows. Inoltre, lo strumento genera un file di registro nella cartella Logs. Ad esempio, as_gddmgr_2014-9-4_11-14-22-655.log è un file di registro che contiene tutti i dettagli.

Nota: tutti i comandi dello strumento della riga di comando (as_gddmgr.exe) supportano anche l'archivio dati del volume GUID. Ad esempio, *-scan VerifyAll <archivio dati volume GUID> [-Password <password archivio dati>]*.

Posizione:

È possibile trovare as_gddmgr.exe nella cartella Bin del percorso di installazione UDP.

Sintassi:

as_gddmgr.exe

-Scan CheckRecoveryPoint <data store name> -Node [<All> |<UDP agent node name>] -RecoveryPoint [<Latest>|<recovery point number>] [-LogLevel <n>]

-Scan VerifyRefCount <data store name> [-LogLevel <n>]

-Scan VerifyData <data store name> [-Password <data store password>] [-LogLevel <n>]

-Scan VerifyAll <data store name > [-Password < data store password >] [-LogLevel <n>]

-Scan RebuildHash <data store name> [-NewHashPath <new hash path>] [-LogLevel <n>]

-Scan RebuildHashWithIndexPath <index path> -NewHashPath <new hash path> [-LogLevel <n>]

-Purge Start <data store name>

-Purge Stop <data store name>

-Purge Status <data store name>

-Purge StartToReclaim <data store name>

-Purge StartToIdentifyObsoletedData <data store name>

Opzioni:

CheckRecoveryPoint

Ridefinisce i punti di ripristino specificati come completi, quindi verifica l'integrità dei dati.

Node <All> | <UDP agent node name>

Specifica il nome del nodo dell'agente.

RecoveryPoint <All> | <recovery point number>

Specifica il punto di ripristino di cui controllare l'integrità.

Password <data store password>

Specifica la password dell'archivio dati.

LogLevel <n>

Specifica il numero di livelli del registro.

VerifyRefCount

Analizza i file di indice e i file di riferimento per verificare il numero di riferimenti registrati nel database hash. Prima di specificare questa opzione, arrestare manualmente l'archivio dati di deduplicazione.

VerifyData

Analizza i file di dati per poi rigenerare le chiavi hash tramite confronto con il file di riferimento. Prima di specificare questa opzione, arrestare manualmente l'archivio dati di deduplicazione.

VerifyAll

Esegue entrambe le operazioni VerifyRefCount e VerifyData. Prima di specificare questa opzione, arrestare manualmente l'archivio dati di deduplicazione.

RebuildHash

Consente di specificare il nome dell'archivio dati e di rigenerare il database hash mediante la scansione dei file di indice e di riferimento. Prima di specificare questa opzione, arrestare manualmente l'archivio dati di deduplicazione.

RebuildHashWithIndexPath

Consente di specificare il percorso dell'indice di deduplicazione e di rigenerare il database hash mediante la scansione dei file di indice e di riferimento. L'opzione viene utilizzata soltanto quando l'archivio dati non è presente su nessuno dei Recovery Point Server.

Avvia

Attiva l'esecuzione dell'eliminazione e del recupero del disco in contemporanea con altri processi standard di Arcserve UDP. L'esecuzione in contemporanea dell'eliminazione potrebbe ridurre la velocità effettiva dei processi standard di Arcserve UDP.

Interrompi

Disattiva l'esecuzione dell'eliminazione e del recupero del disco in contemporanea con altri processi standard di Arcserve UDP.

Stato

Consente di eseguire una query sullo stato dell'eliminazione o del recupero del disco.

StartToReclaim

Attiva l'esecuzione dell'eliminazione e del recupero del disco in contemporanea con altri processi standard di Arcserve UDP. Questa opzione ignora la fase di identificazione dei dati obsoleti, che consente di individuare il blocco di dati obsoleti, e avvia direttamente la fase di recupero del disco, che consente di liberare spazio su disco. Come effetto collaterale, questa opzione potrebbe compromettere l'efficienza del recupero del disco poiché potrebbero essere individuati più blocchi di dati obsoleti nei file di dati, ma il recupero del disco non attende il completamento della fase di identificazione dei dati obsoleti. Inoltre, l'esecuzione in contemporanea dell'eliminazione potrebbe ridurre la velocità effettiva dei processi standard di Arcserve UDP.

StartToIdentifyObsoletedData

Attiva l'esecuzione dell'eliminazione e del recupero del disco in contemporanea con altri processi standard di Arcserve UDP. Questa opzione avvia la fase di identificazione dei dati obsoleti. L'opzione è utile se si desidera ignorare la fase di recupero del disco in corso.

Nota: L'esecuzione delle opzioni seguenti potrebbero durare a lungo a causa del numero elevato di file analizzati nell'archivio dati di deduplicazione.

- VerifyRefCount
- VerifyData
- VerifyAll

- RebuildHash
- RebuildHashWithIndexPath

Esempi:

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

Visualizzazione dell'opzione di verifica del punto di ripristino

A partire dalla versione 7.0 di Arcserve UDP, la funzione di verifica del punto di ripristino è nascosta per impostazione predefinita nella procedura guidata di creazione del piano. Si consiglia di utilizzare l'attività Assured Recovery per rilevare eventuali problemi relativi ai dati. Si consiglia di utilizzare l'attività Assured Recovery per rilevare eventuali problemi relativi ai dati. Per ulteriori informazioni, consultare la sezione Configurazione di Assure Recovery. Se necessario, è ancora possibile utilizzare tale opzione per eseguire la verifica dei dati e visualizzarla durante la procedura guidata di creazione del piano.

Effettuare le operazioni seguenti:

1. Accedere alla console UDP.
2. Accedere alla cartella di installazione della Console UDP. Ad esempio, *C:\Programmi\Arcserve\Unified Data Protection\Management\Configuration*.
3. Aprire il file ConsoleConfiguration.xml in un editor di testi.
4. Individuare il testo sottostante nella sezione <TimeoutConf>:

   <recoveryPointCheck>false</recoveryPointCheck>
5. Modificare il valore da False a True.
6. Salvare il file e uscire.
7. Riavviare il servizio di gestione della console UDP per rendere effettiva l'impostazione.

   Nota: la versione di Arcserve UDP viene aggiornata dalla versione precedente e questa opzione è già stata selezionata in un piano, pertanto non è nascosta per impostazione predefinita.

   Questa opzione consente di rilevare problemi di danneggiamento dei dati verificando il file system dei volumi. Al completamento del processo di backup, Arcserve UDP monta il punto di ripristino ed esegue il comando Windows chkdsk. Se il comando chkdsk rileva un errore, il processo di backup successivo viene convertito in un processo di backup di verifica. Questa opzione è applicabile per i computer virtuali Hyper-V e VMware con sistema operativo guest di Windows. Rivedere le considerazioni seguenti prima di abilitare questa opzione:

   - I seguenti tipi di volume non sono supportati e vengono ignorati dalla **verifica del punto di ripristino**:

- Il volume il cui tipo di file system non è NTFS
- Il volume il cui tipo è Striping con parità
- Il volume che si trova in quel pool di archiviazione

- Il comando chkdsk non riesce a rilevare tutti i problemi di file system. La verifica del punto di ripristino può avere esito positivo, ma il punto di ripristino può essere comunque danneggiato.
- A seconda delle dimensioni del file system del sistema operativo guest, il comando chkdsk può richiedere molto tempo per la sua esecuzione. Il chkdsk utilizza una grande quantità di memoria di sistema sul server proxy di backup e influisce sulle sue prestazioni. La conseguenza di ciò è che il processo di backup richiederà più tempo per il suo completamento. *Nel caso peggiore è possibile che la memoria di sistema del server proxy di backup si esaurisca e che il server non risponda, specialmente se sono presenti numerosi processi di backup simultanei o è in corso la verifica di volumi di grandi dimensioni.* La verifica del punto di ripristino può monitorare l'utilizzo della memoria di sistema e, se l'utilizzo della memoria raggiunge una soglia, verificare che il punto di ripristino verrà sospeso per alcuni minuti rilasciando alcune memorie di sistema. Come procedura ottimale, disabilitare questa opzione, a meno che non sia necessaria o non si disponga di un server proxy di backup potente. In alternativa, è possibile distribuire il carico su più server proxy creando più piani e specificando server proxy diversi in ciascun piano.
- Se il backup è coerente con l'arresto anomalo, vi sono tante probabilità che chkdsk rilevi problemi (a causa della natura di un backup coerente con l'arresto anomalo). Come pratica ottimale, non abilitare questa opzione per un backup coerente con l'arresto anomalo.
- Se si desidera abilitare l'opzione di verifica del punto di ripristino ma non si desidera che il successivo processo di backup venga convertito in un processo di backup di verifica, creare un valore DWORD denominato CheckRecoveryPointIgnoreError nel Registro di sistema del server proxy e impostare il valore DWORD su 1. Creare il valore DWORD nel percorso seguente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

  Il valore DWORD è applicabile a tutti i processi di backup in esecuzione sul server proxy attuale. Se si desidera controllare il comportamento di un computer virtuale specifico, è possibile impostare il valore nel percorso seguente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM GUID>

Nota: Se si aggiunge la chiave del Registro di sistema nel Registro di sistema a livello del computer virtuale e del proxy, l'impostazione nel Registro di sistema a livello del computer virtuale avrà la priorità sull'impostazione nel Registro di sistema a livello del proxy.

- Se si desidera interrompere il processo di backup dopo il rilevamento di un problema da parte della verifica del punto di ripristino (in modo che sia possibile rilevare tempestivamente il problema), creare un valore DWORD denominato CheckRecoveryPointDontFailJob nel Registro di sistema del server proxy e impostare il valore DWORD su 0. Creare il valore DWORD nel percorso seguente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

  Il valore DWORD è applicabile a tutti i processi di backup in esecuzione sul server proxy attuale. Se si desidera controllare il comportamento di un computer virtuale specifico, è possibile impostare il valore nel percorso seguente:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM GUID>.

  Nota: Se si aggiunge la chiave del Registro di sistema nel Registro di sistema a livello del computer virtuale e del proxy, l'impostazione nel Registro di sistema a livello del computer virtuale avrà la priorità sull'impostazione nel Registro di sistema a livello del proxy.

Applicazione di una versione differente di VDDK rispetto alla versione integrata in Arcserve UDP

VMware Virtual Disk Development Kit (VDDK) 6.7.1 è integrato con Arcserve UDP 7.0. Allo stesso tempo, Arcserve UDP 7.0 è compatibile con VDDK 5.5. Se si desidera eseguire VSB/Computer virtuale istantaneo/Assured Recovery su VMware 5.0 o 5.1, utilizzare VDDK 5.5 invece di VDDK 6.7.1.

Importante: Arcserve certifica solo VDDK 6.7.1 e 5.5. Il funzionamento delle altre versione di VDDK non è garantito con Arcserve UDP versione 7.0.

Per modificare manualmente VDDK, attenersi alla procedura seguente:

- Modifica di VDDK per il backup di Virtual Standby (VSB)
- Modifica di VDDK per il backup basato su host (HBBU)

Modifica manuale di VDDK per il backup di Virtual Standby (VSB)

È possibile modificare VDDK manualmente oppure utilizzando un file batch di Windows. In questa sessione vengono illustrate le procedure per entrambe le opzioni.

Considerazioni:

- Per la verifica computer virtuale istantaneo e Assured Recovery è necessario eseguire questa operazione sul server di ripristino/server proxy.
- Da VSB a VMware, utilizzare un server agente dedicato come VSB Monitor e configurare l'attività VSB in modalità proxy. Passare quindi manualmente a VDDK versione 5.5 sul server di monitoraggio VSB.
- Se l'attività VSB è configurata in un piano MSP o uno switch di piano tra siti, VDDK sul server RPS come server di monitoraggio non è presente. Di conseguenza, il server RPS non è disponibile per poter essere utilizzato come server proxy per attività di backup senza agente basato su host.

Per modificare manualmente VDDK, attenersi alla procedura seguente:

1. Accedere al computer di installazione dell'agente Arcserve UDP utilizzando un account amministrativo o un account con privilegi di amministratore.
2. Rinominare la cartella *VDDK* in VDDK6.7.
3. Rinominare la cartella *VDDK5.5* in VDDK dal seguente percorso predefinito:

   C:\Programmi\Arcserve\Unified Data Protection\engine\BIN

Nota: La posizione della cartella BIN può variare in base a percorso di installazione dell'agente di Arcserve UDP.

4. Eseguire il comando riportato di seguito per verificare lo stato del servizio:

   Nota: È necessario eliminare il servizio solo quando non è in stato di esecuzione.

   sc query vstor2-mntapi20-shared

   Se il servizio non esiste, eseguire l'eliminazione utilizzando il passaggio successivo. Se il servizio è in esecuzione, prima di eseguire l'eliminazione mediante il passaggio successivo, eseguire il comando seguente per eseguire l'arresto:

   sc stop vstor2-mntapi20-shared

5. Eseguire il comando riportato di seguito per eliminare il servizio:

   sc delete vstor2-mntapi20-shared

6. Eseguire il comando riportato di seguito per verificare che il servizio sia stato eliminato correttamente:

   sc query vstor2-mntapi20-shared

   Nota: Se lo stato del servizio è STOP_PENDING, riavviare il computer.

   Per modificare VDDK utilizzando un file batch di Windows, attenersi alla seguente procedura:

1. Accedere al computer di installazione dell'agente Arcserve UDP utilizzando un account amministrativo o un account con privilegi di amministratore.
2. Avviare l'utilità *ChangeToVDDK55.bat* dalla seguente posizione predefinita:

   C:\Programmi\Arcserve\Unified Data Protection\engine\BIN

   Nota: La posizione della cartella BIN può variare in base a percorso di installazione dell'agente di Arcserve UDP.

   VDDK 5.5 viene installato dopo l'avvio di un nuovo processo.

Modifica manuale di VDDK per il backup basato su host (HBBU)

È possibile modificare manualmente VDDK per il backup basato su host (HBBU).

Modificare VDDK 6.7 per il backup di vSphere 5.5 (o versioni successive):

Effettuare le operazioni seguenti:

1. Scaricare VDDK dal sito Web di VMware.
2. Estrarre tutti i file in una cartella temporanea.

3. Individuare la cartella denominata ***bin*** disponibile nel percorso sottostante e rinominare la cartella (ad esempio, *bin_old*):

   <Arcserve UDP installation path>\Engine\BIN\VDDK\BIN\VDDK64\

   Esempio: C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN\VDDK\BIN\VDDK64\

4. Individuare la cartella denominata ***bin*** dai file estratti nella cartella temporanea e copiarli nel percorso seguente:

   <Arcserve UDP installation path>\Engine\BIN\VDDK\BIN\VDDK64\.

   VDDK è stato modificato correttamente.

Modificare VDDK 5.5 per il backup di vSphere 5.0 e 5.1:

Effettuare le operazioni seguenti:

1. Scaricare VDDK dal sito Web di VMware.
2. Estrarre tutti i file in una cartella temporanea.
3. Individuare la cartella denominata ***bin*** disponibile nel percorso sottostante e rinominare la cartella (ad esempio, *bin_old*):

   <Arcserve UDP installation path>\Engine\BIN\VDDK5.5\BIN\VDDK64\

   Esempio: C:\Programmi\Arcserve\Unified Data Protection\Engine\BIN\VDDK5.5\BIN\VDDK64\

4. Individuare la cartella denominata ***bin*** dai file estratti nella cartella temporanea e copiarli nel percorso seguente:

   <Arcserve UDP installation path>\Engine\BIN\VDDK5.5\BIN\VDDK64\.

   VDDK è stato modificato correttamente.

Migrazione dei dati di backup di Arcserve D2D r16.5 per due server con nome host identico nell'archivio dati RPS

Sono presenti due server con nome host identico e nome FQDN DNS diverso, protetti mediante Arcserve D2D r16.5. In tal caso, procedere come riportato di seguito per eseguire la migrazione dei dati nell'archivio dati RPS di Arcserve UDP:

1. Arrestare il servizio Arcserve D2D sul Server 1.
2. Utilizzando il processo Arcserve UDP Jumpstart, eseguire la migrazione dei dati del Server 1 nell'archivio dati RPS.
3. Aggiornare l'agente Arcserve UDP nel Server 1.
4. Creare un piano o usarne uno esistente per proteggere il Server 1, quindi scegliere lo stesso archivio dati RPS come destinazione di backup.
5. Distribuire il piano.
6. Arrestare il servizio Arcserve D2D sul Server 2.
7. Utilizzando il processo Arcserve UDP Jumpstart, eseguire la migrazione dei dati del Server 2 nell'archivio dati RPS.
8. Sul server RPS, accedere alla cartella di destinazione del backup per l'archivio dati e individuare la cartella del Server 2 utilizzando il relativo nome host per trovarla.

   Ad esempio, se il nome host del Server 2 è "MyServer2", il nome della cartella sarà "MyServer2".
9. Aggiornare l'agente Arcserve UDP nel Server 2.
10. Avviare l'agente UDP sul Server 2, se non risulta avviato.
11. Aprire il Registro di sistema (su un server specifico) e individuare la seguente chiave:

    HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
12. Annotare il valore di "NodeID".

    Si tratta di un ID univoco in formato di GUID, ad esempio "e856e0ba-66d7-4da5-8b98-2250173e349a".
13. Sul server RPS, individuare la cartella di destinazione del backup per il Server 2 e aggiornare l'ID di nodo come **<folder_name> [NodeID value]**.

    Esempio: MyServer2[e856e0ba-66d7-4da5-8b98-2250173e349a]

14. Creare un piano o usarne uno esistente per proteggere il Server 2, quindi scegliere lo stesso archivio dati RPS come destinazione di backup.
15. Distribuire il piano.

Distribuzione di Arcserve UDP in Microsoft Azure

È possibile distribuire Arcserve UDP in Microsoft Azure quando si utilizza Arcserve Unified Data Protection v6.5, Aggiornamento 2 o versioni successive. La funzionalità consente di distribuire i computer Virtual Standby in Microsoft Azure e proteggere i dati. Un computer Virtual Standby viene creato su Microsoft Azure e i dati corrispondenti si basano sui punti di ripristino del backup on premise.

Lo standby virtuale converte i punti di ripristino in formati di computer virtuale su Microsoft Azure e prepara una snapshot per recuperare facilmente i dati qualora necessario.

Questa funzionalità fornisce anche la capacità High Availability e garantisce che il computer virtuale possa intervenire immediatamente quando si verifica un errore nel computer di origine. Il computer Virtual Standby viene creato tramite la conversione dei punti di ripristino in un formato Virtual Standby di Azure.

Come procedere?

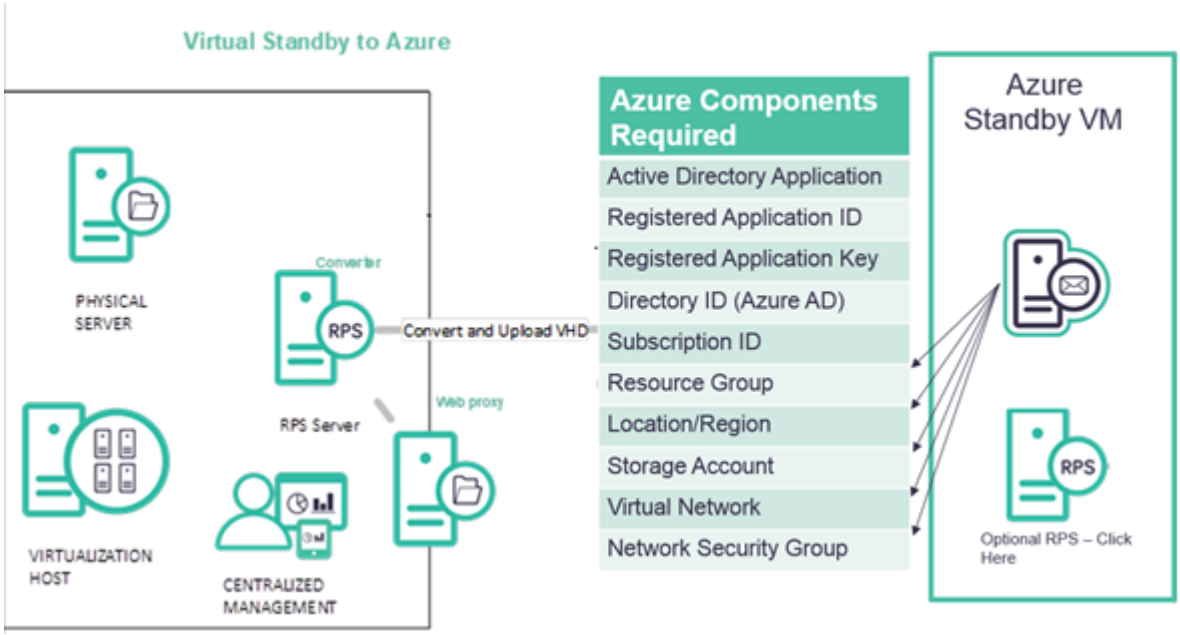
1. Informazioni sul flusso di processo
2. Procedure consigliate
3. Considerazioni
4. Pianificazione della distribuzione
5. Distribuzione di Arcserve UDP in Microsoft Azure

Informazioni sul flusso di processo

Arcserve UDP supporta i computer virtuali Virtual Standby in Microsoft Azure. Se la soluzione di protezione dei dati è già stata distribuita in modalità on premise, è possibile distribuire Arcserve UDP in Microsoft Azure.

La soluzione on premise è composta dalla Console Arcserve UDP e da Arcserve UDP Recovery Point Server (RPS). È possibile eseguire il backup dei sistemi Windows su un server RPS locale. È possibile creare un piano nella Console Arcserve UDP per il backup dei dati nel server RPS locale, quindi eseguire l'attività Virtual Standby. La funzionalità Virtual Standby monitora l'heartbeat del nodo di origine. Se il nodo di origine non è disponibile, viene sostituito dal computer virtuale su Azure.

La seguente immagine mostra il flusso di processo di Arcserve UDP per Microsoft Azure:



Considerazioni

Rivedere le considerazioni seguenti prima di effettuare la distribuzione di Arcserve UDP in Microsoft Azure:

Nota: per ulteriori informazioni sulle procedure consigliate, consultare la sezione Distribuzione di Arcserve UDP su Microsoft Azure.

- In Microsoft Azure qualsiasi file VHD non può contenere un disco di sistema con dimensioni superiori a 2048 GB e un disco dei dati con dimensioni superiori a 4095 GB. In Arcserve UDP Virtual Standby, l'origine non può disporre di un disco di sistema con dimensioni superiori a 2048 GB e il disco dei dati non può avere dimensioni superiori a 4095 GB.
- Il computer virtuale Microsoft Azure e Arcserve UDP Virtual Standby supportano solo il sistema operativo Windows 2008 R2 o versioni successive.
- Arcserve UDP non supporta la creazione del computer virtuale classico come computer virtuale di standby.
- Il computer virtuale Microsoft Azure richiede il volume di sistema e il volume di avvio sullo stesso disco.
- Microsoft Azure non supporta l'avvio del computer dal sistema UEFI.
- Microsoft Azure non supporta il computer di origine come server Hyper-V.
- Arcserve UDP Virtual Standby non supporta il disco di sistema dinamico per il computer di origine.
- Arcserve UDP in Microsoft Azure supporta solo i nodi Windows.

Pianificazione della distribuzione di Arcserve UDP in Microsoft Azure

È necessario completare le attività seguenti prima di distribuire Arcserve UDP in Microsoft Azure:

1. Verifica dei prerequisiti
2. Preparazione di un account Cloud in Microsoft Azure
3. Preparazione delle risorse Microsoft Azure

Prerequisiti

Verificare i prerequisiti seguenti per Arcserve UDP e Recovery Point Server prima di distribuire Arcserve UDP in Microsoft Azure:

- Verificare la matrice di compatibilità per i sistemi operativi, i database e i browser supportati.
- Preparare i server in precedenza per effettuare la distribuzione della Console Arcserve UDP e del Recovery Point Server.
- I server per ogni componente devono soddisfare i seguenti requisiti di sistema:
  - **Server:** Server Windows 2008 R2 o versioni successive
  - **CPU:** minimo 4 Core 2.7 GHz
  - **Spazio su disco:** 40 GB per l'installazione del sistema operativo
  - **RAM:** minimo 8 GB
  - **Archiviazione di backup per il Recovery Point Server:** in base alle dimensioni dei dati di origine

Preparazione di un account Cloud in Microsoft Azure

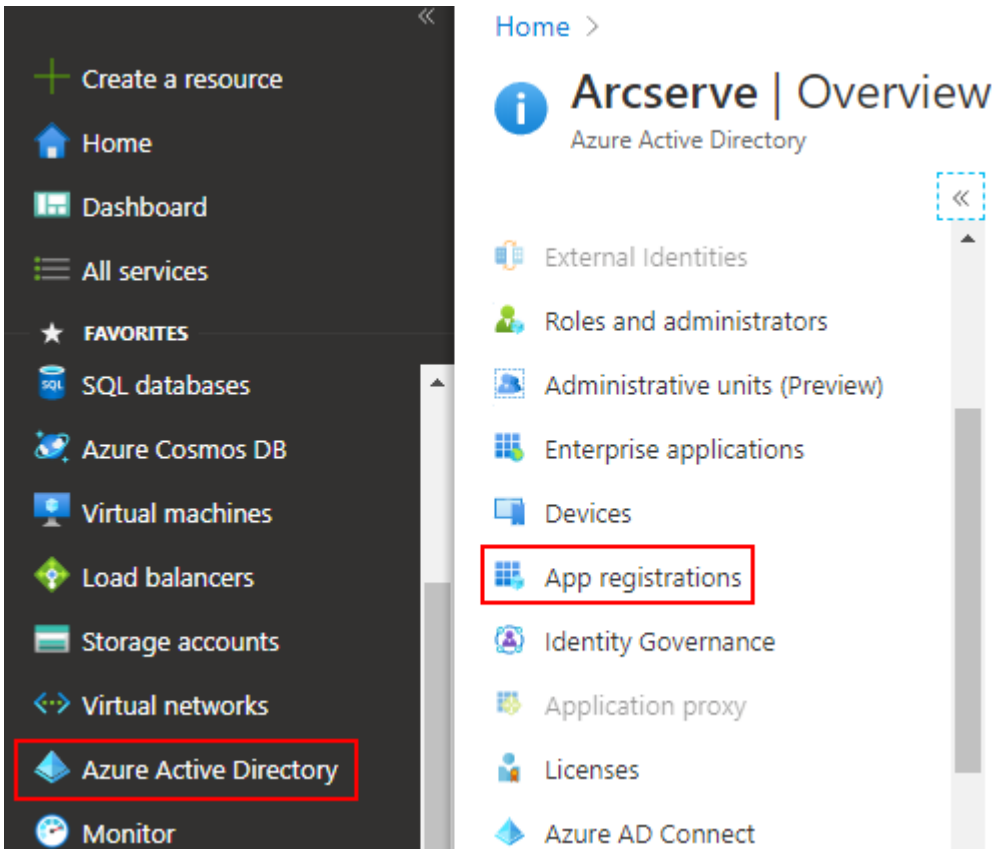
Questa sezione fornisce informazioni su come creare un account cloud in Microsoft Azure.

Effettuare le operazioni seguenti:

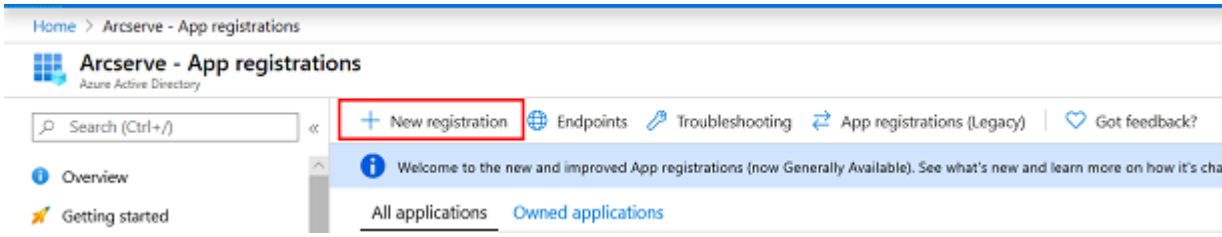
1. Eseguire i passaggi seguenti per registrare l'applicazione Azure Active Directory utilizzata da Arcserve UDP per comunicare con Microsoft Azure:

a. Accedere al portale Azure.

b. Dal riquadro sinistro, selezionare **Azure Active Directory** e nel riquadro destro fare clic su **Registrazioni app**.



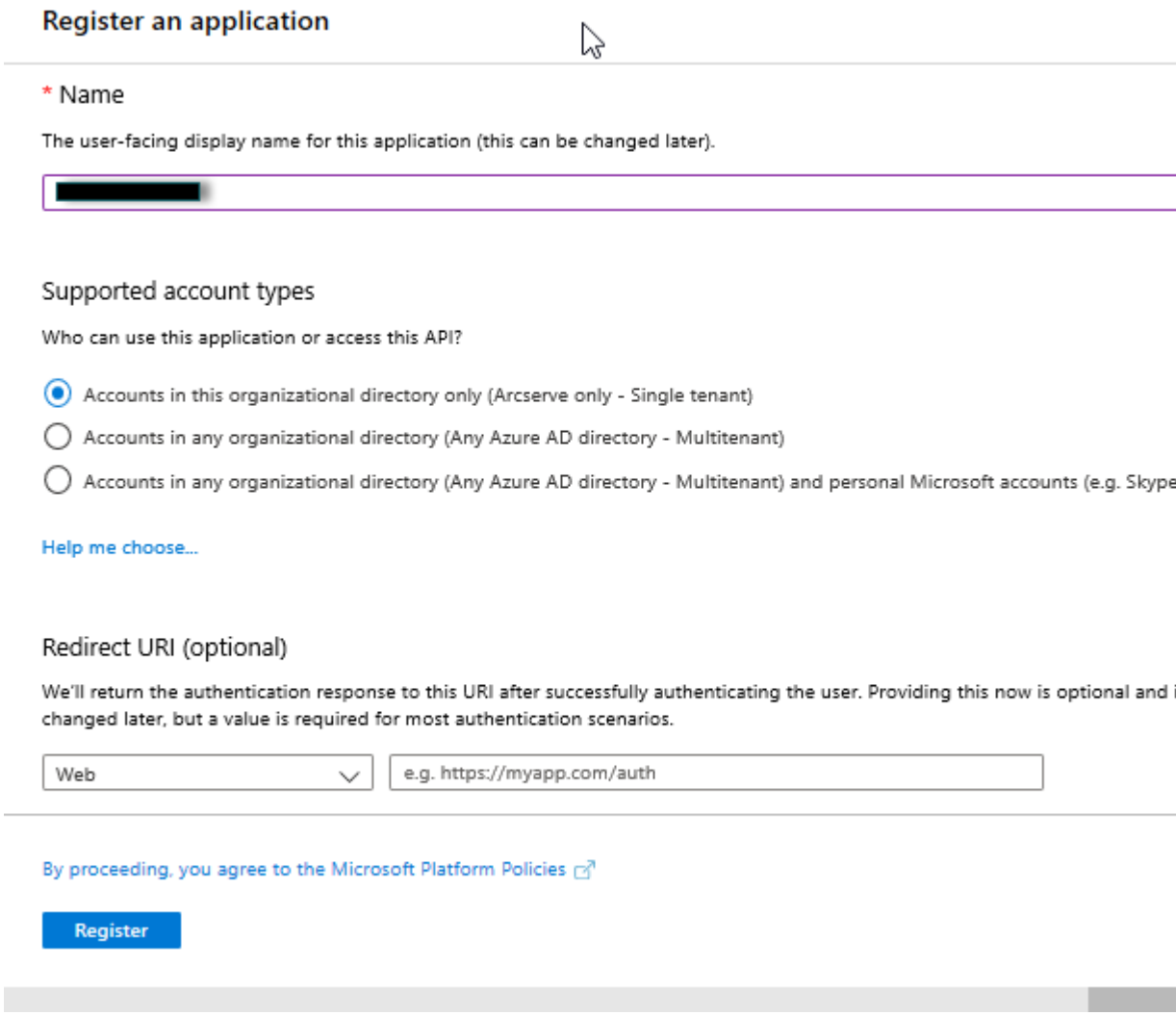
c. Nella pagina Registrazioni applicazione Arcserve, fare clic su **Nuova registrazione**.



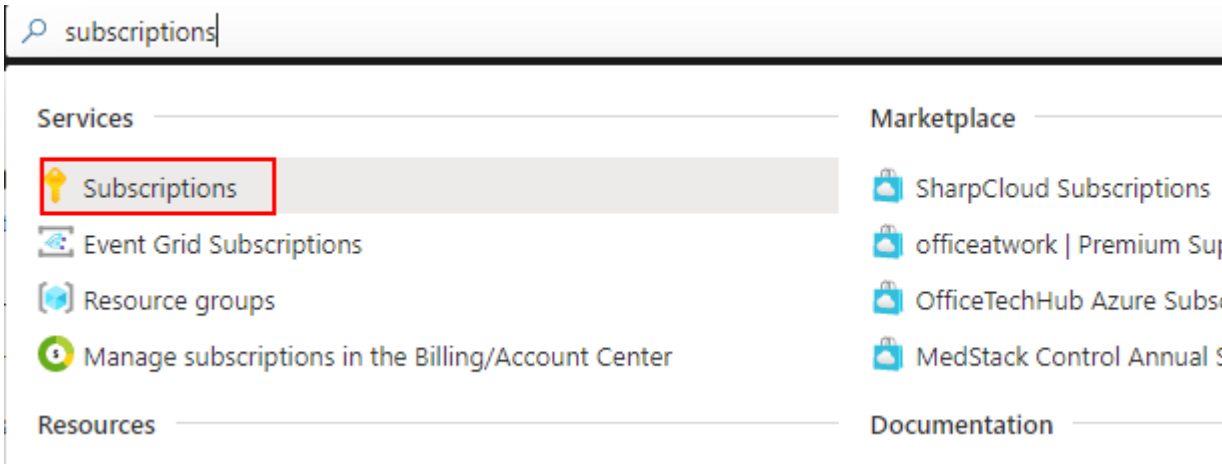
d. Nella pagina Registrazione di un'applicazione, effettuare le operazioni descritte di seguito, quindi fare clic su **Registra**.

- Nome: immettere il nome dell'applicazione.
- Tipi di account supportati: selezionare un tipo di account supportato per definire quali utenti potranno usare l'applicazione.

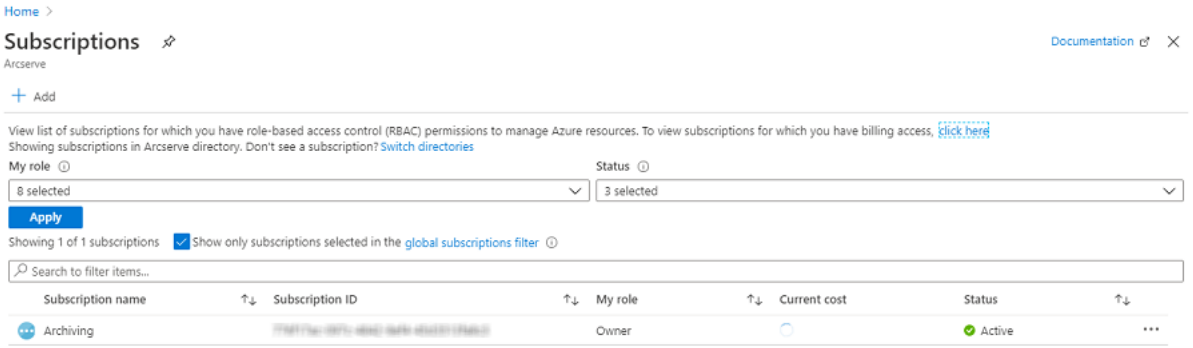
- URI di reindirizzamento (facoltativo): selezionare **Client Web o Pubblico (versione mobile o desktop)** per il tipo di applicazione da creare, quindi immettere l'URI di reindirizzamento per l'applicazione.



e. Sulla barra di ricerca, digitare sottoscrizioni, quindi dall'elenco fare clic su **Sottoscrizioni**.

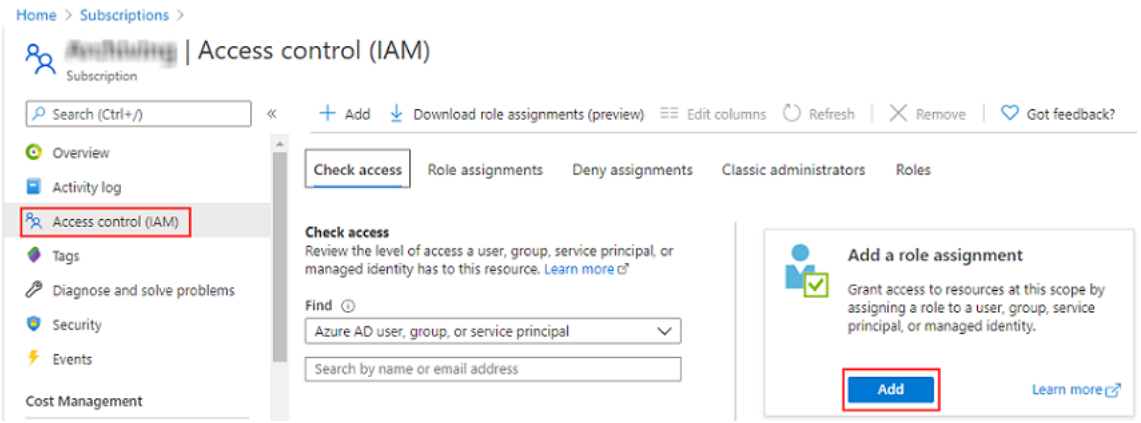


f. Nelle pagine Sottoscrizioni selezionare la sottoscrizione per l'applicazione.



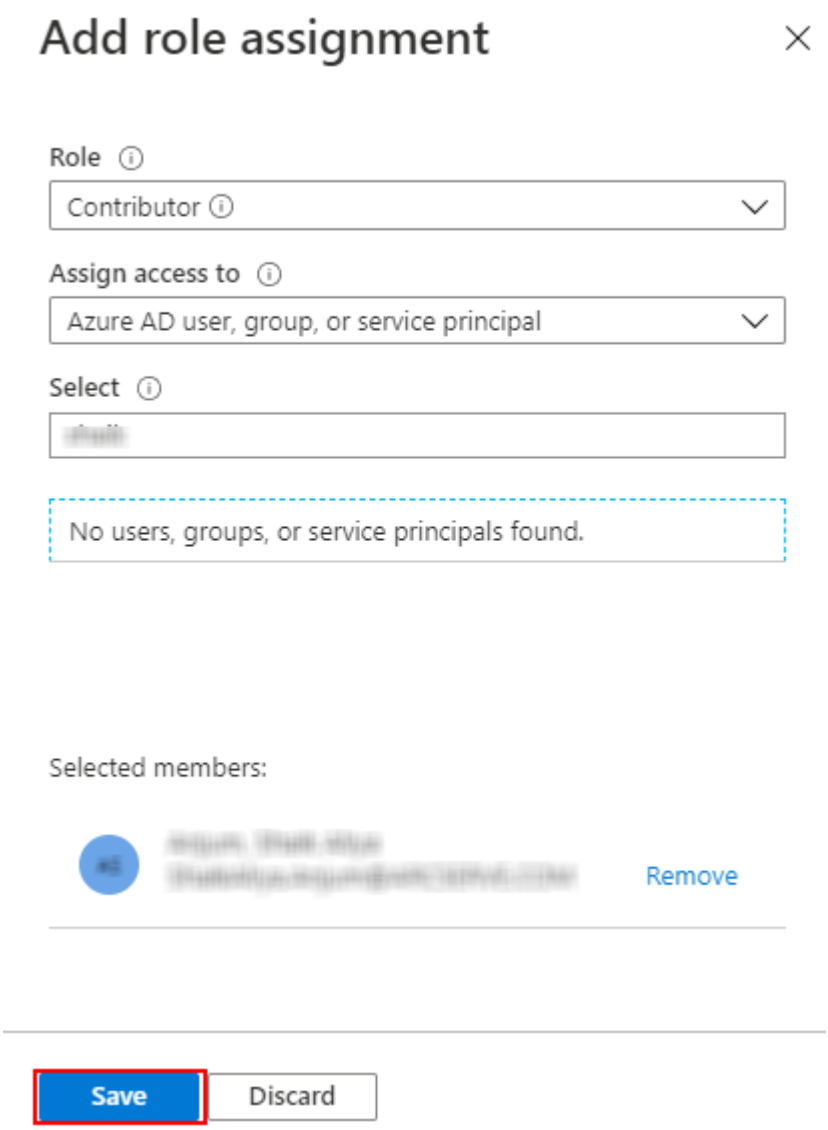
Nota: se l'elenco delle sottoscrizioni non visualizza la sottoscrizione richiesta, selezionare il filtro **sottoscrizioni globali**. Assicurarsi che la sottoscrizione desiderata sia selezionata per il portale.

g. Da Sottoscrizioni, accedere a **Controllo di accesso (IAM)> Verifica accesso**, quindi fare clic su **Aggiungi** dalla casella Aggiungi assegnazione ruolo.



h. Nella pagina Aggiungi assegnazione ruolo, effettuare le operazioni seguenti, quindi fare clic su **Salva**.

- Ruolo: selezionare il ruolo da assegnare all'applicazione.
- Assegna accesso a: utilizzare l'impostazione predefinita.
- Seleziona: per impostazione predefinita, le applicazioni AD Azure non vengono visualizzate nelle opzioni disponibili. Per individuare l'applicazione, cercare il nome dell'applicazione e selezionarlo.



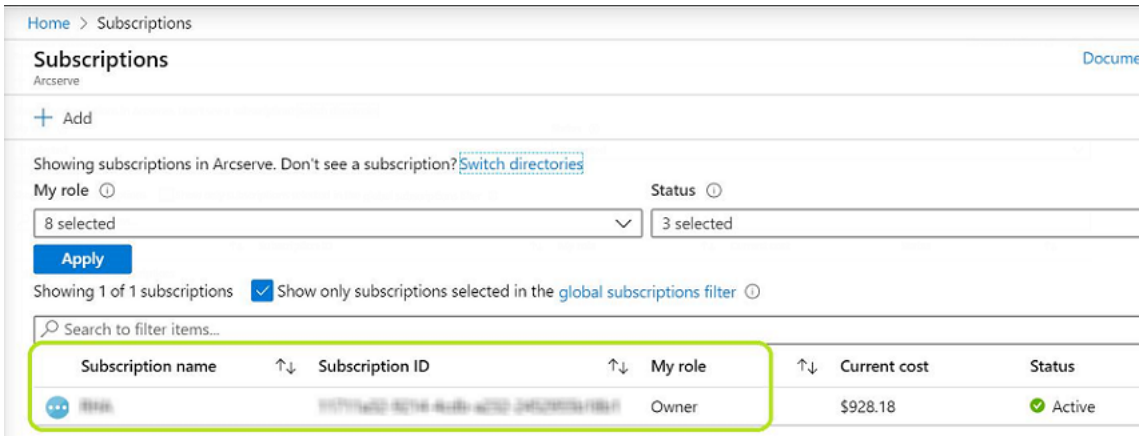
L'applicazione Azure Active Directory viene registrata e il ruolo viene assegnato correttamente.

È ora possibile effettuare i passaggi successivi utilizzando l'applicazione registrata per ottenere gli ID e le chiavi necessarie.

2. Come ottenere l' ID sottoscrizione[1]Procedere come segue:

   a. Dal pannello di navigazione a sinistra nel portale Azure, fare clic su **Sottoscrizioni**.

      L'elenco delle sottoscrizioni viene visualizzato con l'ID di sottoscrizione.

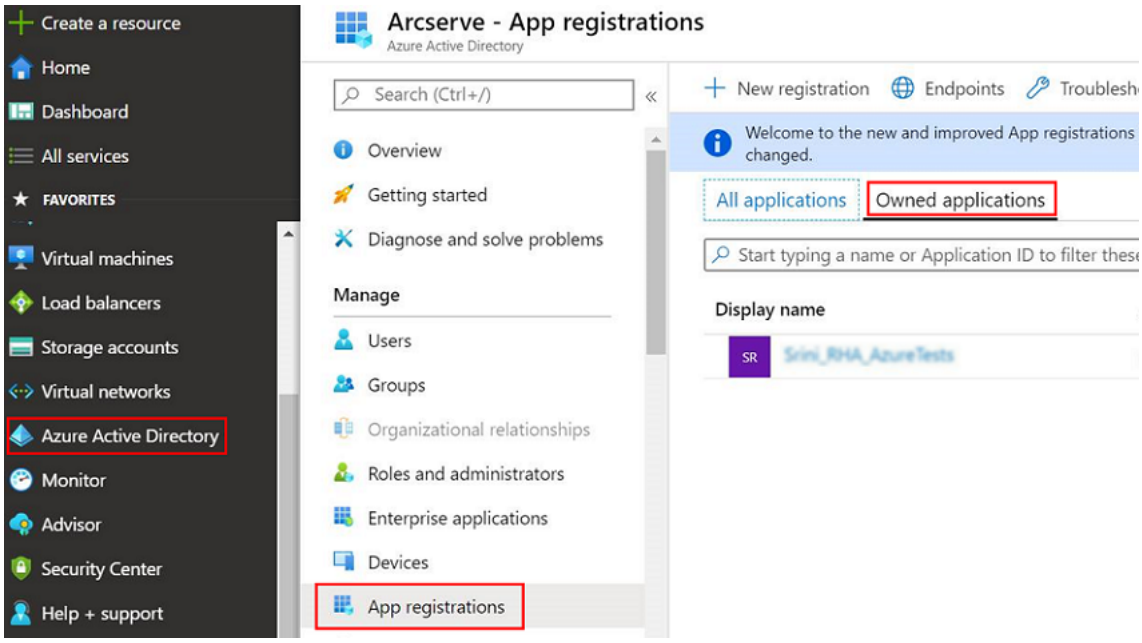


   b. Copiare e salvare l'ID di sottoscrizione, che viene utilizzato durante l'aggiunta dell'account Microsoft Azure Cloud in Arcserve UDP.

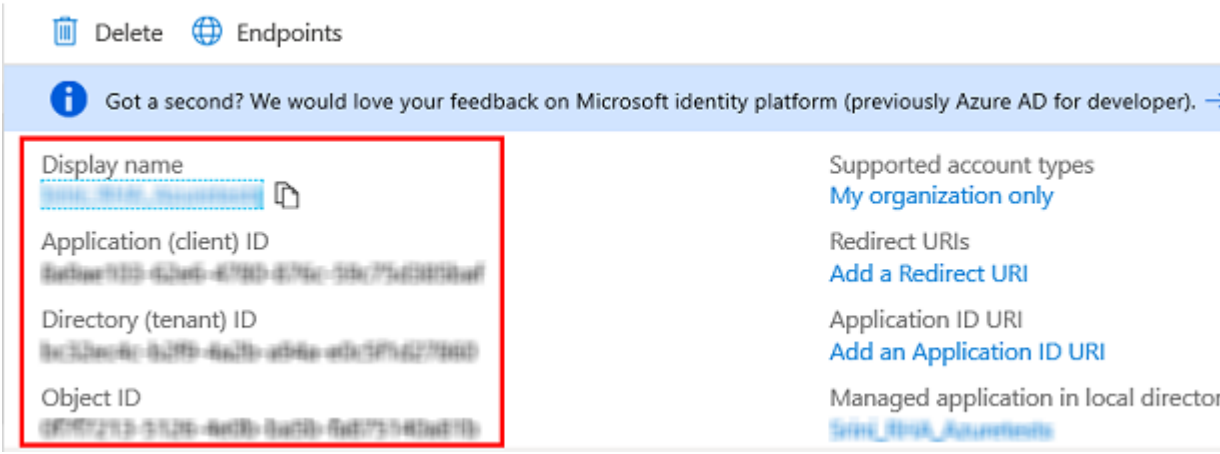
3. Come ottenere l' ID tenant[2] e ID applicazione[3]Procedere come segue:

   a. Accedere a **Azure Active Directory** > **Registrazioni applicazioni** > **Applicazioni di proprietà dell'utente**, quindi selezionare l'applicazione.

[1]L'ID di sottoscrizione fa riferimento a un ID univoco globale che identifica in modo univoco la sottoscrizione per l'utilizzo del servizi Azure.
[2]L'ID tenant è l'ID della directory Azure Active Directory in cui è stata creata la registrazione dell'applicazione. L'ID tenant viene definito ID directory nelle proprietà di Azure Active Directory.
[3]Un ID applicazione fa riferimento a un ID dell'interfaccia utente grafica che identifica esclusivamente la registrazione dell'applicazione nel tenant di Active Directory di Azure. A volte viene definito come ID client.



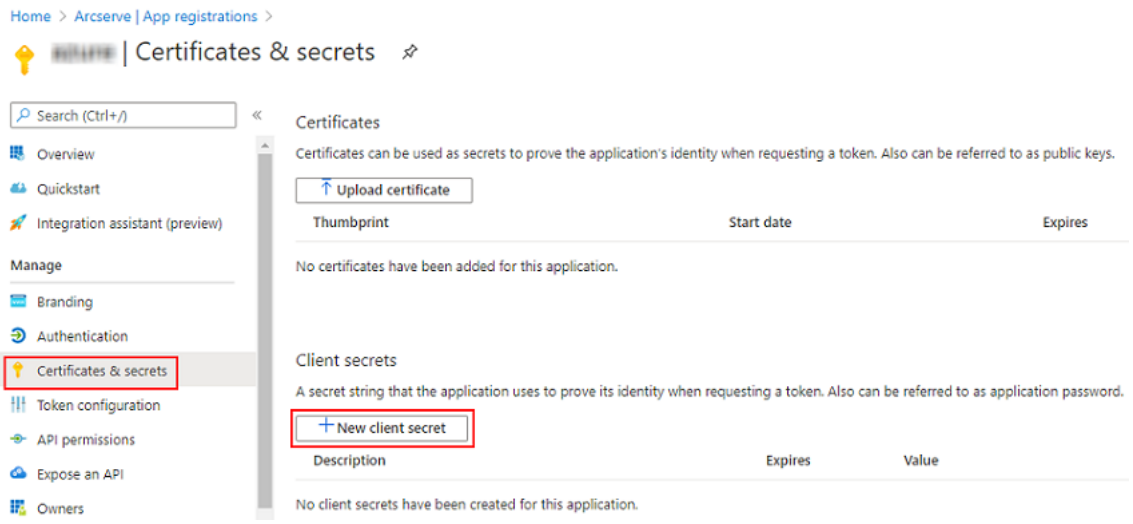
b. Copiare e salvare l'ID dell'applicazione (client) e l'ID directory (tenant) in una posizione sicura.



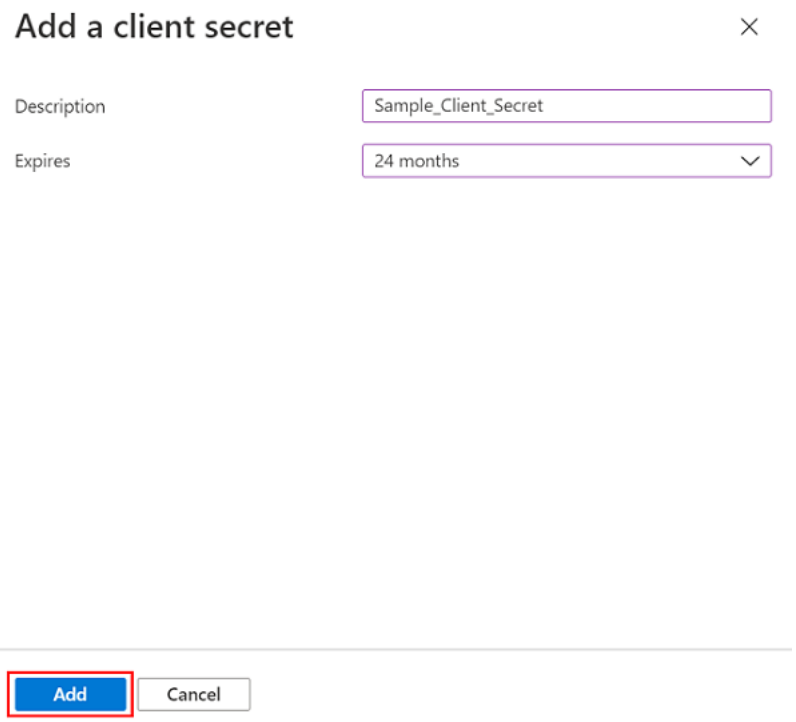
4. Come ottenere il Segreto client[1]Procedere come segue:

   a. Nella schermata Registrazioni app, selezionare l'applicazione, accedere a **Certificati e segreti** nel riquadro sinistro, quindi fare clic su **Nuovo segreto client** per aggiungere un segreto client.

[1]Il segreto client è definito chiave di autenticazione in Azure.

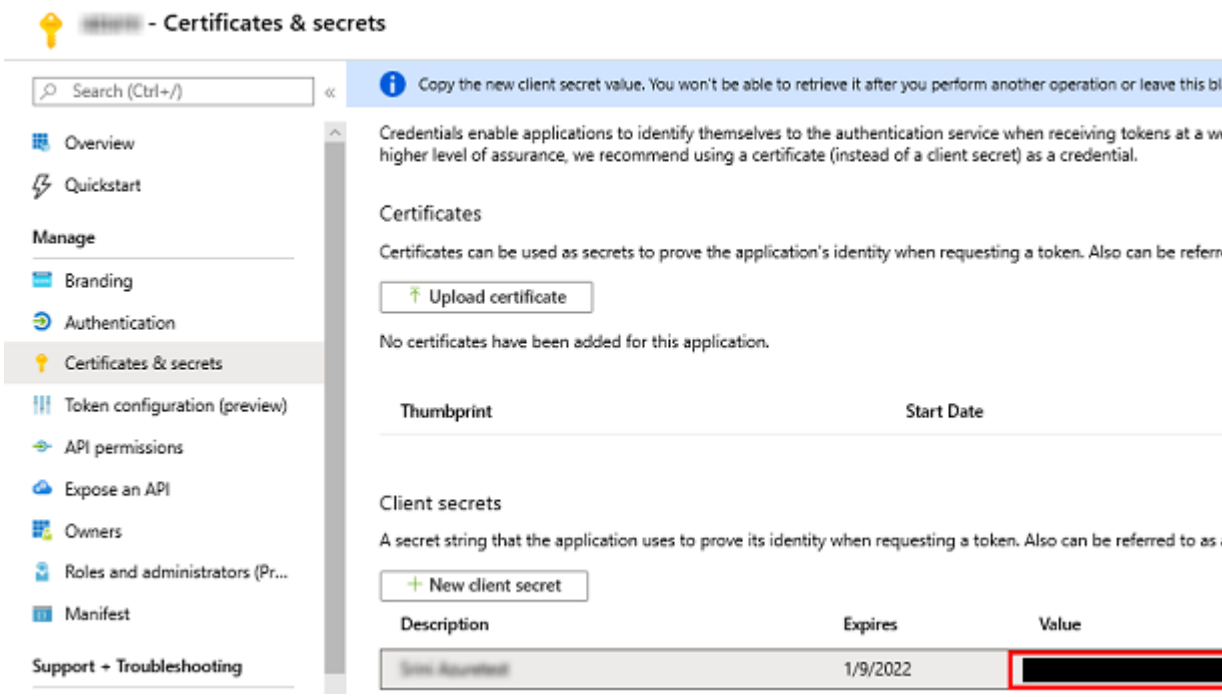


b. Nella pagina Aggiungi un segreto client, immettere una descrizione, selezionare l'intervallo di scadenza desiderato dall'elenco a discesa, quindi fare clic su **Aggiungi**.



Nota: si consiglia di selezionare l'opzione**24 mesi** come intervallo di scadenza per evitare di generare ripetutamente il segreto client.

Viene visualizzato il valore del segreto client.



Importante: Copiare e salvare il valore del segreto client in quanto non sarà possibile recuperarlo in seguito. Se si dimentica di salvare il valore, eliminare il segreto client esistente e crearne uno nuovo, come illustrato nel passaggio 4.

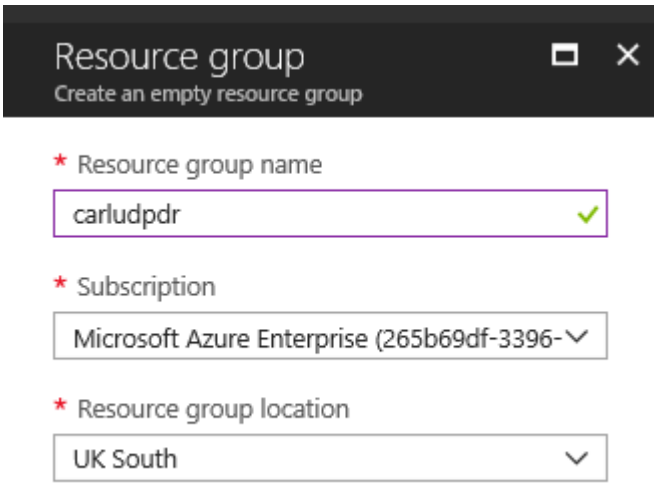
L'account cloud è stato creato correttamente in Microsoft Azure.

Prepare Microsoft Azure Resources

Before you can create a cloud account for Microsoft Azure, you must create the following Microsoft Azure resources:

1. Perform the following steps to create a Resource group:
    a. Log into the Azure portal using valid credentials.
    b. Click **Add** to create an empty resource group.
    c. Enter a name and location for the new resource group and click

Create.



2. Perform the following steps to create a storage account:
    a. Navigate to **Storage accounts** and click **Add**.
    b. Specify the following:

    Note: Ensure that your storage account, virtual network and network security group of the standby VM are at the same location.

    Name

    Specifies name of the storage account.

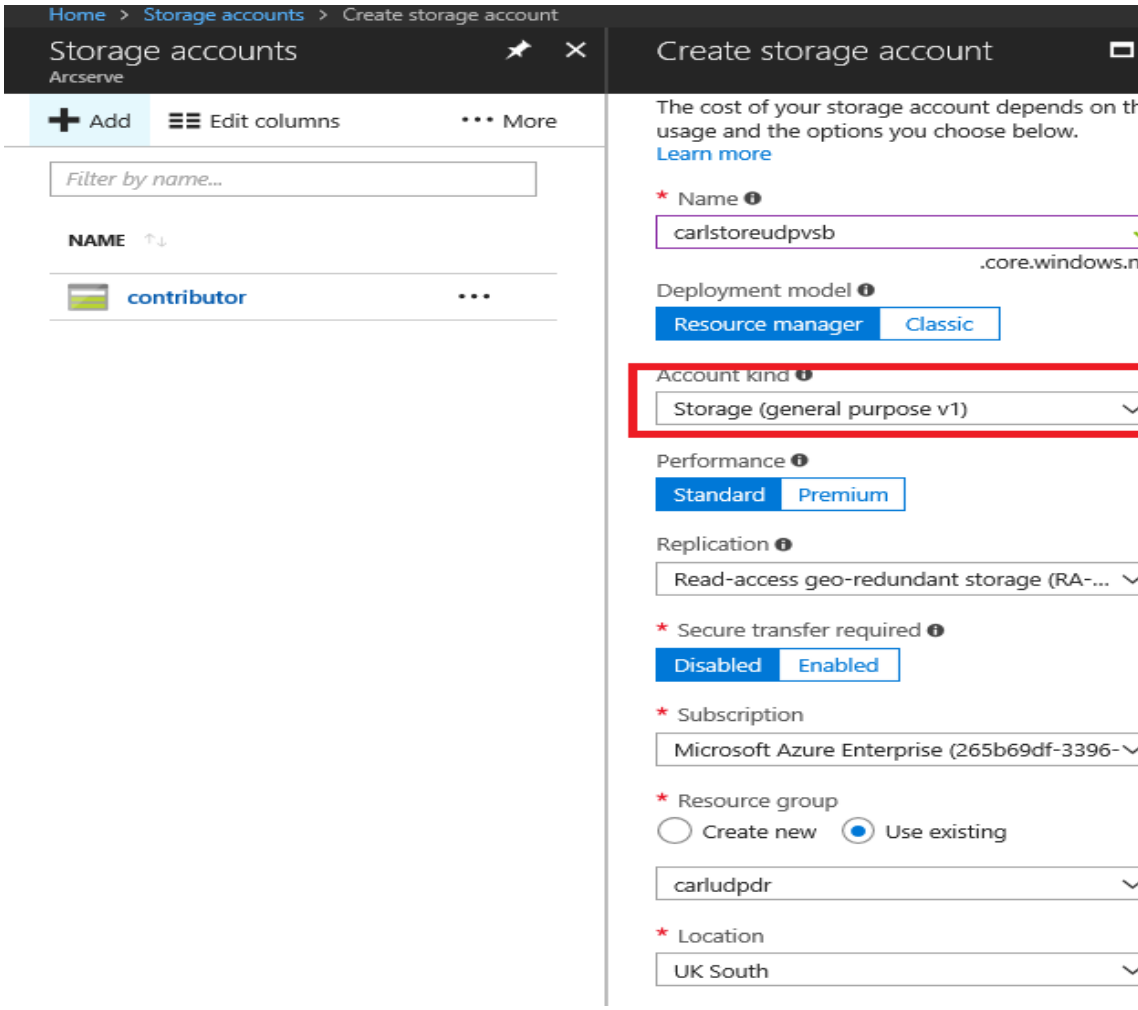
    Deployment model

    Select deployment model based on your requirement.

    Account kind

    Specify **Storage (general purpose v1)** or **StorageV2 (general purpose v2)** as Account kind.

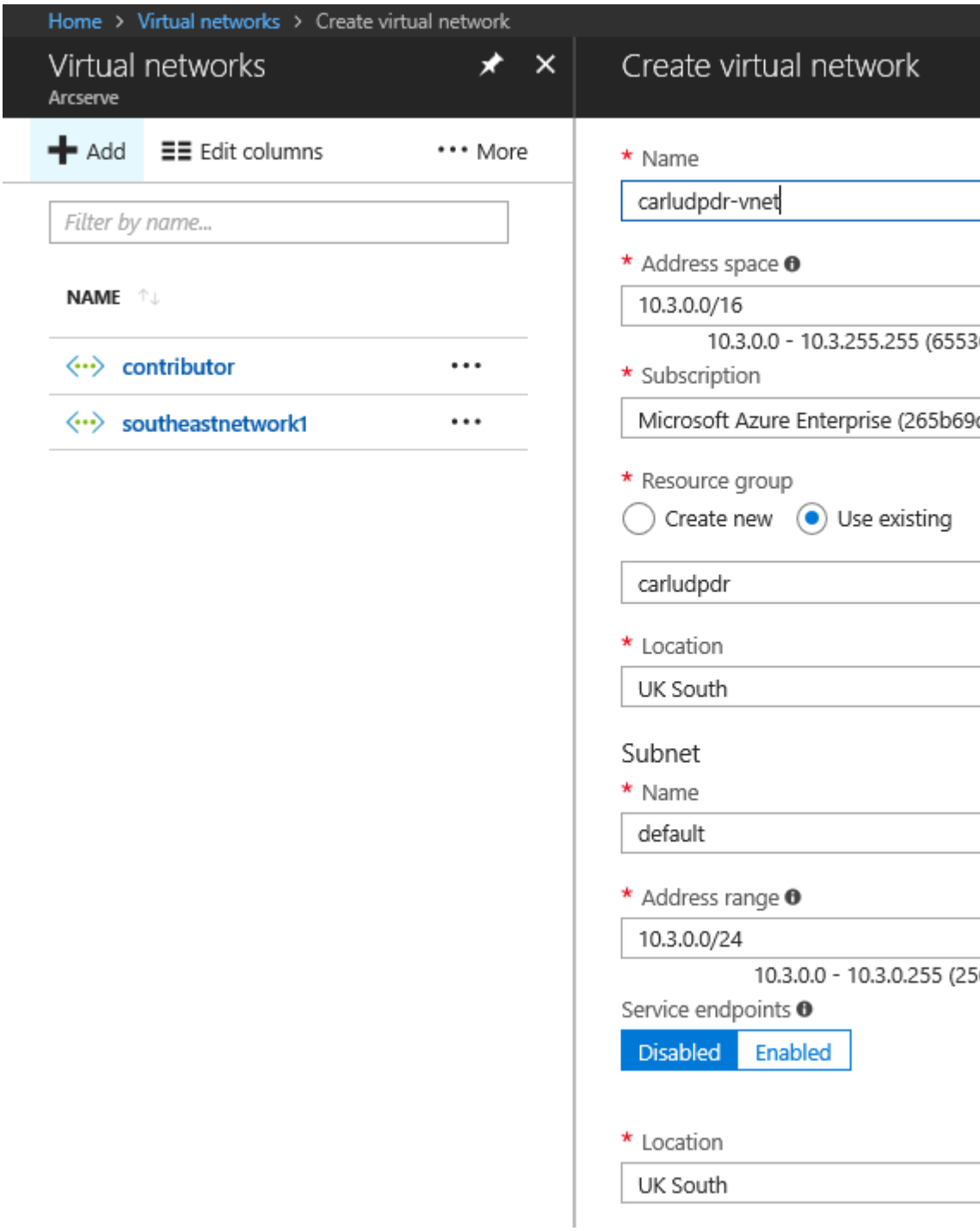
c. Specify other details as required and click **Create**:



3. Perform the following steps to create a Virtual Network and Subnet:

   a. Navigate to Microsoft Azure home, **Virtual networks**, and click **Add**.

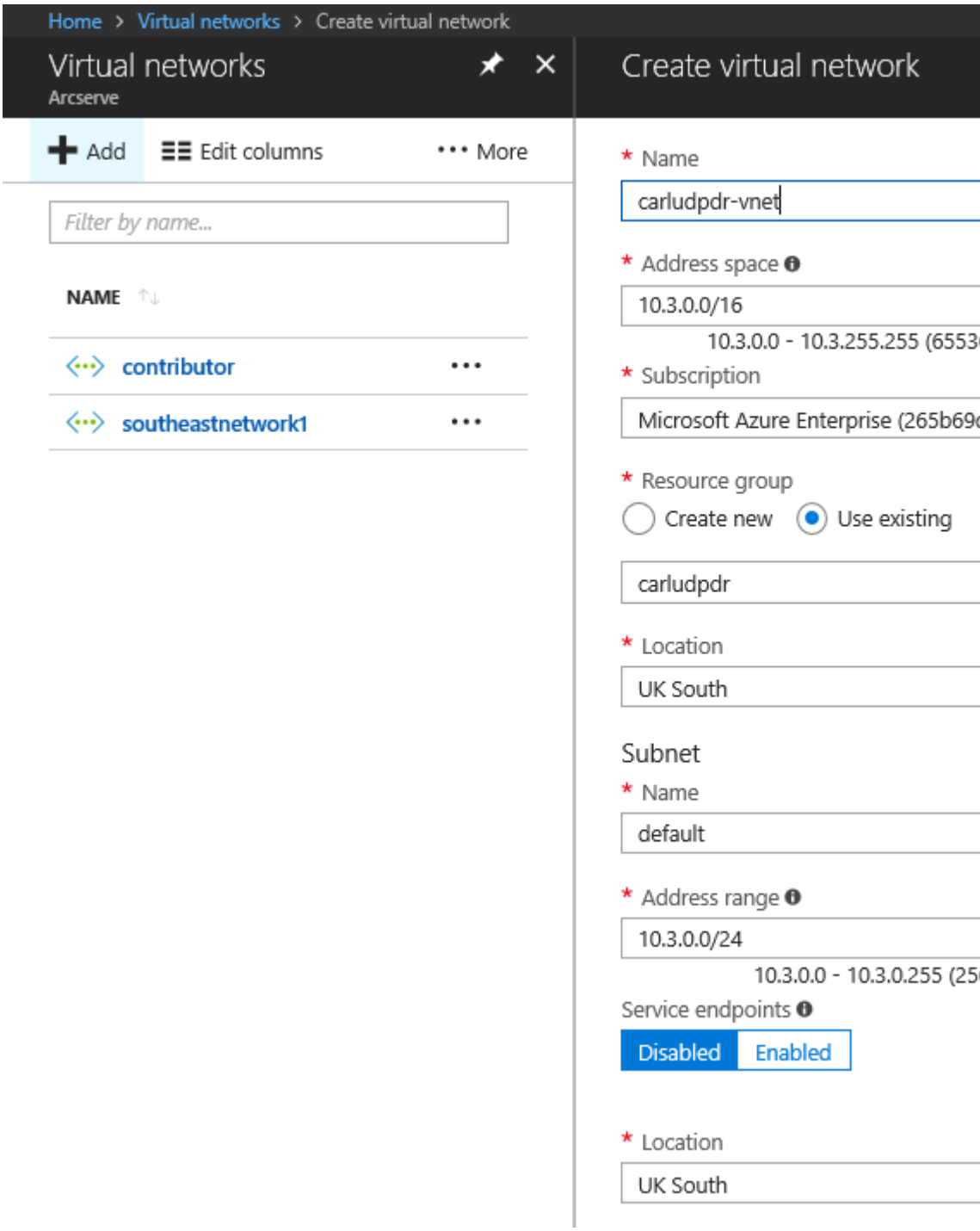
b. Enter the required details and click **Create**.



4. Perform the following steps to create a Network Security group:

   a. Navigate to Microsoft Azure home, **Network security groups**, and click **Add**.

b. Enter the required details and click **Create**.



Microsoft Azure resources are successfully created.

Distribuzione di Arcserve UDP in Microsoft Azure

Dopo aver completato i prerequisiti, è possibile avviare la distribuzione di Arcserve UDP in Microsoft Azure.

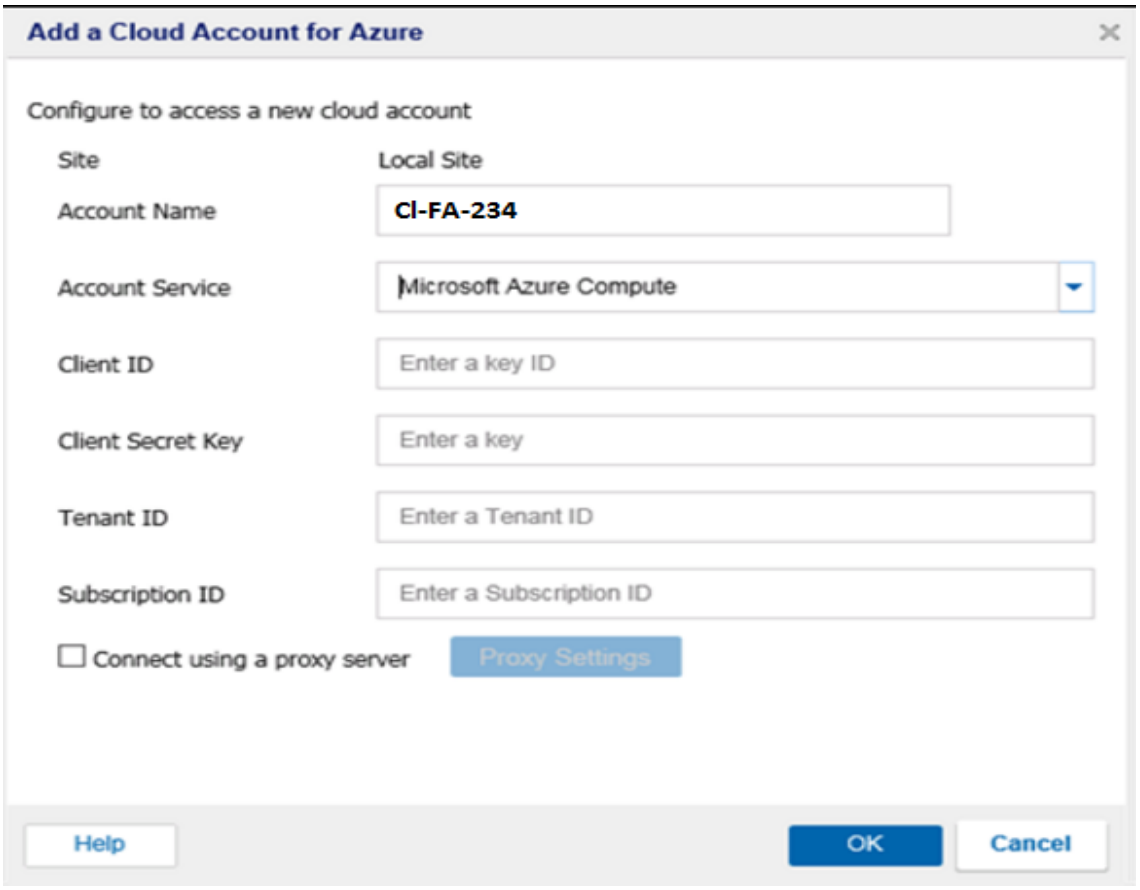
Come procedere?

1. Aggiunta di un account Azure Cloud in Arcserve UDP
2. Creazione di un piano con un'attività di
3. Aggiunta al piano di un'attività Virtual Standby
4. Esecuzione manuale del processo Virtual Standby
5. Accensione del computer virtuale Virtual Standby in Azure
6. Verifica dello stato del computer virtuale Virtual Standby

Aggiunta di un account Azure Cloud in Arcserve UDP

Aggiungere un account cloud Microsoft Azure Compute per copiare i file o i punti di ripristino nell'archiviazione cloud. È possibile utilizzare questo account durante la creazione di attività per i piani Virtual Standby su Cloud o Computer virtuale istantaneo su Microsoft Azure.

Nota: per aggiungere un account cloud per Microsoft Azure, è necessario che vengano soddisfatti i prerequisiti. Per ulteriori informazioni, consultare la sezione Prerequisiti.



Effettuare le operazioni seguenti:

1. Accedere ad Arcserve Unified Data Protection, quindi fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Destinazioni**, quindi fare clic su **Account cloud**.

   Nel riquadro centrale viene visualizzata la pagina **Destinazioni: account cloud**.
3. Fare clic su **Aggiungi account cloud**.

   Viene visualizzata la pagina **Aggiungi account cloud**.
4. Per il campo **Nome account**, specificare un nome univoco.

   Il campo Nome account specifica il nome dell'archiviazione cloud. Questo nome viene aggiunto alla console per identificare l'account cloud. Ciascun account cloud deve avere un nome di archiviazione univoco.
5. Selezionare l'opzione dall'elenco a discesa **Servizio account**.

   Vengono visualizzati più campi per la configurazione.
6. Immettere i dettagli nei campi seguenti per eseguire la configurazione e fare clic su **OK**:

   ID client

   Fa riferimento all'ID applicazione dell'applicazione Azure Active Directory. Copiare l'ID client preparato nell'editor di testo.

   Chiave segreta client

   Fa riferimento alla chiave di autenticazione generata per l'applicazione Azure Active Directory immessa come ID client. Copiare la chiave segreta client preparata nell'editor di testo.

   Importante! La chiave privata è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere la chiave privata in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

   ID tenant

   Fa riferimento all'ID di Azure Active Directory in cui è stata creata l'applicazione Azure Active Directory. Copiare l'ID tenant preparato nell'editor di testo.

   ID sottoscrizione

   Fa riferimento a un ID univoco globale (GUID) che identifica in modo univoco la sottoscrizione per l'utilizzo del servizi Azure. Copiare l'ID di sottoscrizione nell'editor di testo.

   Impostazioni proxy

Specifica le impostazioni del server proxy fornite. Selezionare **Connetti tramite server proxy** per abilitare questa opzione. Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. È quindi necessario fornire le informazioni di autenticazione corrispondenti richieste per l'utilizzo del server proxy.

L'account cloud viene aggiunto alla console.

Creazione di un piano con un'attività di backup

Un piano include diversi tipi di attività da eseguire. Per creare un computer Virtual Standby, creare un piano che include un'attività di backup e un'attività Virtual Standby. Un'attività di backup esegue un backup dei nodi di origine e archivia i dati nella destinazione specificata. La funzionalità Virtual Standby utilizza i dati di backup e li converte in un formato del computer virtuale.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse** della Console.
2. Dal riquadro sinistro, accedere a **Piani**, e fare clic su **Tutti i piani**.

   Se sono stati creati altri piani in precedenza, tali piani verranno visualizzati nel riquadro centrale.
3. Nel riquadro centrale, fare clic su **Aggiungi un piano**.

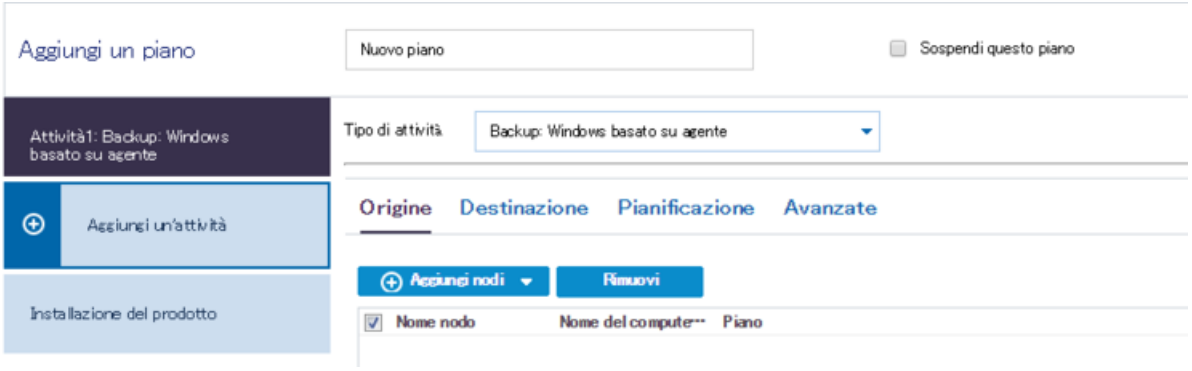
   Viene visualizzata la finestra di dialogo **Aggiungi un piano**.
4. Immettere un nome per il piano.
5. (Facoltativo) Selezionare la casella di controllo **Sospendi questo piano**.

   Il piano non verrà eseguito fino alla deselezione della casella di controllo per la ripresa del piano.

   Nota: se un piano viene sospeso, i processi in corso non vengono interrotti, mentre vengono interrotti tutti i processi pianificati associati al piano. Tuttavia, è possibile eseguire manualmente un processo. Ad esempio, è possibile eseguire manualmente il processo di backup e il processo di replica per un nodo anche se il piano corrispondente viene sospeso. In tal caso, la seguente attività sul processo on demand (manuale) non verrà eseguita. Ad esempio, se è presente un'attività di replica in seguito a un processo di backup on-demand, il processo di replica non verrà eseguito per il processo di backup on-demand. È necessario eseguire manualmente il processo di replica. Quando il piano viene ripreso, i processi in sospeso

non verranno ripresi immediatamente. Dopo aver ripreso un piano, i processi in sospeso verranno eseguiti all'ora di pianificazione successiva.

6. Dall'elenco a discesa **Tipo di attività**, selezionare **Backup, Windows basato su agente**.



Specificare quindi i dettagli per i campi Origine, Destinazione, Pianificazione e Avanzate.

Aggiunta al piano di un'attività Virtual Standby

Creare un server Virtual Standby su un'attività Azure in modo che i dati di backup vengano convertiti in un formato di computer virtuale e venga creato un computer virtuale. La funzionalità Virtual Standby controlla anche l'heartbeat del nodo di origine in modo che quando il nodo di origine è inattivo, il computer virtuale assume immediatamente il controllo come nodo di origine.

Note:

- Virtual Standby non è in grado di attivare automaticamente le snapshot del punto di ripristino acquisite dai nodi del computer virtuale basato su host e dai nodi replicati da un Recovery Point Server remoto. Soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso. Per tali nodi è necessario alimentare manualmente le snapshot del punto di ripristino.
- Quando il piano viene ripreso, il processo Virtual Standby non viene ripreso automaticamente. Per avviare il processo Virtual Standby è necessario eseguire un altro processo di backup manualmente. Inoltre, quando il piano viene sospeso, l'opzione Sospendi/Riprendi Virtual Standby non è disponibile. Se non si desidera che il computer virtuale venga avviato automaticamente dopo l'interruzione del piano, sarà necessario interrompere manualmente l'heartbeat per i nodi.

Effettuare le operazioni seguenti:

1. Fare clic su **Aggiungi un'attività** dal riquadro sinistro.

   Viene aggiunta una nuova attività al riquadro sinistro.

2. Dal menu a discesa **Tipo di attività**, selezionare **Virtual Standby**.

   Viene aggiunta l'attività Virtual Standby.

3. Dalla scheda **Origine**, selezionare un'origine per l'attività Virtual Standby.

4. Fare clic sulla scheda **Server di virtualizzazione** e immettere i dettagli del server di virtualizzazione e del server di monitoraggio.

   Tipo di virtualizzazione

   Specificare Azure come tipo di virtualizzazione.

   Nome account

   Selezionare un account Azure esistente o fare clic su **Aggiungi** per creare un account.

   Per ulteriori informazioni, consultare la sezione Aggiunta di un account cloud.

   Gruppo di risorse

   Selezionare un gruppo di risorse esistente oppure fare clic su **Aggiungi** per creare un gruppo di risorse.

   Per ulteriori informazioni, consultare la sezione Gruppi di risorse in Azure.

   Area

   Selezionare l'area in cui si desidera utilizzare il computer virtuale di standby per Azure. Per ulteriori informazioni, consultare la sezione Aree in Azure.

   Monitoraggio

   Specificare il nome host del server che dovrà monitorare lo stato del server di origine.

   Note:

   - È possibile utilizzare qualsiasi computer fisico o virtuale come server di monitoraggio.
   - Non è possibile utilizzare il server di origine di backup come server di monitoraggio.
   - Se i nodi vengono replicati da un Recovery Point Server remoto o se soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso, non è necessario configurare il server di monitoraggio.

- La configurazione del server di monitoraggio non è richiesta se l'origine di Virtual Standby corrisponde all'attività di replica e il server RPS di destinazione di replica è contenuto in Azure.

Nome utente

Specificare il nome utente per accedere al sistema di monitoraggio.

Password

Specificare la password del nome utente per accedere al sistema di monitoraggio.

Protocollo

Specificare HTTP o HTTPS come protocollo da utilizzare per la comunicazione tra Arcserve UDP e il server di monitoraggio.

Porta

Specificare la porta che si desidera utilizzare per il trasferimento dei dati tra Arcserve UDP e il server di monitoraggio.

5. Fare clic sulla scheda **Computer virtuale** e immettere i dettagli relativi alle impostazioni di base del computer virtuale, all'archivio dati del computer virtuale per VMware, al percorso al computer virtuale per Hyper-V e alla rete del computer virtuale.

Prefisso nome del computer virtuale

Specificare il prefisso che si desidera aggiungere al nome visualizzato per il computer virtuale su Azure.

Valore predefinito: UDPVM_

Snapshot del punto di ripristino

Specificare il numero di snapshot del punto di ripristino (punti di ripristino) per il computer virtuale di standby. Il numero massimo consentito di snapshot del punto di ripristino corrisponde a 29.

Valore predefinito: 5

Combina tutte le sessioni non convertite in una snapshot del singolo punto di ripristino

Selezionare l'opzione se si desidera combinare tutte le sessioni non convertite in una singola snapshot del punto di ripristino con l’esecuzione pianificata del processo VSB successivo.

Impostazione predefinita: opzione selezionata

Dimensioni del computer virtuale

Microsoft Azure fornisce un'ampia scelta di dimensioni ottimizzate per il computer virtuale adatte ai diversi casi di utilizzo. Dispongono di diverse combinazioni di CPU, memoria, archiviazione e capacità di rete. Per ulteriori informazioni sulle dimensioni del computer virtuale e il soddisfacimento dei requisiti di calcolo, consultare la sezione Dimensioni del computer virtuale Windows in Azure.

Nome account di archiviazione

Selezionare un Nome account di archiviazione esistente o creare un Account di archiviazione in Azure. Quando si crea l'account di archiviazione in Azure, è necessario specificare una delle opzioni seguenti come Tipo di account

- Archiviazione (scopo generale v1)
- ArchiviazioneV2 (scopo generale v2)

Per ulteriori informazioni, consultare la sezione Account di archiviazione in Azure.

Rete virtuale

Selezionare una rete virtuale esistente o creare una rete virtuale in Azure. Per ulteriori informazioni, consultare la sezione Rete virtuale in Azure.

Subnet

Selezionare una subnet della rete virtuale esistente in base alla rete virtuale selezionata oppure aggiungere una subnet nel Azure. Per ulteriori informazioni, consultare la sezione Aggiunta di una subnet in Azure.

Gruppo di protezione di rete

Selezionare un gruppo di protezione di rete esistente o creare un gruppo di protezione di rete in Azure. Configurare le regole del gruppo di protezione per aprire le porte correlate, comprese la porta 3389 per il desktop remoto e la porta 8014 e 8015 per la comunicazione con Arcserve UDP. Per ulteriori informazioni, consultare la sezione Gruppo di protezione di rete.

Attivazione dell'assegnazione automatica dell'IP pubblico

Selezionare questa opzione per assegnare automaticamente l'indirizzo IP pubblico al computer virtuale di standby con l'avvio del computer virtuale in Azure.

6. Fare clic sulla scheda **Avanzate** e fornire i dettagli seguenti:

Avvia il computer virtuale automaticamente

Specificare se si desidera avviare il computer virtuale automaticamente.

Nota: questa opzione non è disponibile per i nodi del computer virtuale basati su host e per i nodi replicati da un Recovery Point Server remoto. Soltanto

l'origine dell'attività Virtual Standby viene replicata su un sito diverso. L'origine di Virtual Standby è un'attività di replica e il server RPS di destinazione della replica è compreso in Azure.

Timeout

Specificare il tempo di attesa di un heartbeat da parte del server di monitoraggio prima di attivare la snapshot di un punto di ripristino.

Frequenza

Specificare la frequenza con cui il server di origine comunica gli heartbeat al server di monitoraggio.

Esempio: Il valore di timeout specificato è 60. Il valore di frequenza specificato è 10. Il server di origine comunicherà gli heartbeat a intervalli di 10 secondi. Se il server di monitoraggio non rileva un heartbeat entro 60 secondi dell'ultimo heartbeat rilevato, attiva un computer virtuale utilizzando la snapshot del punto di ripristino più recente.

Personalizzazione dei parametri del processo

È possibile personalizzare i parametri del processo per le seguenti opzioni:

- *Numero di thread in caricamento per ogni processo*: valore predefinito: 4
- *Dimensione di buffer per ciascun thread*: valore predefinito: 4096 KB

Abilitazione degli avvisi di posta elettronica

Selezionare questa opzione per abilitare gli avvisi di posta elettronica. Consente di ricevere avvisi di posta elettronica a seconda delle impostazioni fornite.

- **Heartbeat mancante per il computer di origine** - Virtual Standby invia notifiche di avviso quando il server di monitoraggio non rileva un heartbeat nel server di origine.

  Nota: questa opzione non è disponibile per i nodi associati a Esegui replica da un Recovery Point Server remoto o se l'origine dell'attività Virtual Standby viene replicata su un sito diverso.

- **Computer virtuale attivo per il computer di origine configurato con attivazione automatica** - Virtual Standby invia notifiche di avviso quando viene attivato un computer virtuale configurato per l'attivazione automatica nel caso in cui l'heartbeat non venga rilevato.

  Nota: questa opzione non è disponibile per i nodi del computer virtuale basati su host e per i nodi replicati da un Recovery Point Server remoto. Soltanto l'origine dell'attività Virtual Standby viene replicata su un sito diverso.

- **Computer virtuale attivo per il computer di origine configurato con attivazione manuale** - Virtual Standby invia notifiche di avviso quando viene attivato un computer virtuale.
- **Errori o arresto anomalo di Virtual Standby** - Virtual Standby invia notifiche di avviso quando si verifica un errore durante il processo di conversione.
- **Virtual Standby eseguito correttamente** - Virtual Standby invia notifiche di avviso quando un computer virtuale è stato attivato correttamente.
- **Errore di avvio di Virtual Standby dalla snapshot del punto di ripristino** - se è stata specificata l'opzione Avvia il computer virtuale automaticamente, Virtual Standby invia notifiche di avviso in caso di rilevamento di computer virtuali non avviati automaticamente.

7. Fare clic su **Salva**.

   Le modifiche vengono salvate e l'attività Virtual Standby viene distribuita automaticamente al server Virtual Standby.

   Nota: una volta completata l'attività Virtual Standby, viee creato il volume di standby del computer virtuale. Il computer virtuale di standby viene creato solo dopo l'attivazione del computer virtuale da Arcserve UDP.

   Virtual Standby è stato creato e distribuito correttamente nel piano Azure.

Esecuzione manuale del processo Virtual Standby

Per eseguire manualmente un processo Virtual Standby, occorre prima eseguire un backup manuale. L'attività Virtual Standby è associata a un'attività di backup. Se un piano include un'attività di backup e un'attività Virtual Standby, quando si esegue manualmente il processo di backup, il processo Virtual Standby viene eseguito automaticamente dopo il completamento del processo di backup.

Effettuare le operazioni seguenti:

1. Fare clic sulla scheda **Risorse**.
2. Dal riquadro sinistro, accedere a **Nodi**, quindi fare clic su **Tutti i nodi**.

   Consente di visualizzare i piani aggiunti.
3. Selezionare i nodi di cui si desidera eseguire il backup. Il nodo selezionato deve avere un piano assegnato.
4. Nel riquadro centrale, fare clic su **Azioni**, **Esegui backup**.

   Verrà visualizzata la finestra di dialogo **Esegui un backup immediato**.
5. Selezionare il tipo di backup e fornire un nome al processo di backup.
6. Fare clic su **OK**.

Il processo di backup viene eseguito.

Il processo Virtual Standby viene eseguito immediatamente dopo la conclusione del processo di backup.

Il processo Virtual Standby viene eseguito manualmente.

Accensione del computer virtuale Virtual Standby in Azure

I volumi del computer virtuale di standby vengono creati in Azure in seguito al completamento del processo Virtual Standby. Il computer virtuale di standby viene creato soltanto con l'attivazione da Arcserve UDP.

Virtual Standby può essere configurato in modo tale da attivare computer Virtual Standby a partire da snapshot del punto di ripristino quando il server di monitoraggio non rileva heartbeat dal server di origine. In alternativa, è possibile attivare manualmente i computer Virtual Standby dalle snapshot del punto di ripristino in caso di errore del server di origine, di emergenza o per utilizzare un nodo di origine in modalità non in linea per la manutenzione.

Effettuare le operazioni seguenti:

1. Dalla scheda **Risorse**, accedere al gruppo nodi **Virtual Standby**.

   I nodi Virtual Standby vengono mostrati nel riquadro centrale.

2. Nel riquadro centrale, selezionare il nodo e fare clic su **Computer virtuale di standby**.

   Viene visualizzata la finestra di dialogo **Computer virtuale di standby**.

3. Nella finestra di dialogo **Computer virtuale di standby**, completare le attività seguenti:

   - Selezionare un intervallo di tempo della snapshot del punto di ripristino per l'attivazione del computer virtuale.
   - Fare clic su **Attiva computer virtuale**.

     Il computer virtuale viene attivato utilizzando i dati contenuti nella snapshot del punto di ripristino.

   È ora possibile verificare lo stato o arrestare il computer virtuale Virtual Standby. Per ulteriori informazioni, consultare le seguenti sezioni:

   - Verifica dello stato del computer virtuale Virtual Standby
   - Interruzione del computer virtuale Virtual Standby in Azure

Interruzione del computer virtuale Virtual Standby in Azure

È possibile arrestare il computer virtuale Virtual Standby in Azure mediante la Console Arcserve UDP.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Accedere a **Virtual Standby**.
3. Selezionare e fare clic con il tasto destro sul **computer virtuale Virtual Standby** dal riquadro centrale.

   Viene visualizzata la finestra di dialogo del computer virtuale di standby contenente le snapshot attive.
4. Selezionare una snapshot attiva e fare clic su **Arresta computer virtuale**.
5. Fare clic su **Elimina**.

   Viene visualizzata una finestra di dialogo di conferma.
6. Se si desidera eliminare i dischi collegati al computer virtuale Virtual Standby, selezionare l'opzione **Elimina i dischi collegati**.
7. Fare clic su **OK**.

   Il computer virtuale Virtual Standby viene arrestato correttamente.

Verifica dello stato del computer virtuale Virtual Standby

È possibile verificare lo stato del computer virtuale Virtual Standby tramite la Console Arcserve UDP.

Effettuare le operazioni seguenti:

1. Dalla Console, fare clic su **Risorse**.
2. Accedere a **Virtual Standby**.
3. Selezionare il **computer virtuale Virtual Standby** dal riquadro centrale.
4. Viene visualizzato il riquadro della procedura guidata di configurazione, contenente lo stato del computer virtuale Virtual Standby per il gruppo **Stato Virtual Standby**.

   Lo stato corrisponde a **In esecuzione** se il computer virtual Virtual Standby è attivato. Se il computer non è attivato, lo stato corrisponde a **N/D** o **Disattivato**.

Termini e definizioni relativi ad Arcserve UDP

Backup basato su agente

Il backup basato sull'agente è un metodo per l'esecuzione del backup dei dati mediante un componente dell'agente. L'agente è installato sul nodo di origine.

Compressione

La compressione viene utilizzata per i backup. La compressione consente solitamente di ridurre l'utilizzo dello spazio su disco. Tuttavia, può avere un effetto inverso e ridurre la velocità di backup a causa dell'aumento dell'utilizzo della CPU.

Le opzioni disponibili sono:

Nessuna compressione

L'opzione determina un utilizzo minimo della CPU (velocità massima) e un utilizzo massimo dello spazio su disco per la creazione dell'immagine di backup.

Compressione standard

Verrà eseguito un certo livello di compressione. Questa opzione fornisce un buon bilanciamento tra l'utilizzo della CPU e dello spazio su disco. Si tratta dell'impostazione predefinita.

Compressione massima

Verrà eseguita la compressione massima. L'opzione implica un utilizzo massimo di CPU (velocità minima) ma utilizza anche una quantità minore di spazio su disco per l'immagine di backup.

Note:

- Se l'immagine di backup contiene dati non comprimibili quali immagini JPG, file ZIP, ecc., potrebbe essere necessario allocare ulteriore spazio per la gestione di tali dati. Di conseguenza, se si seleziona una qualsiasi opzione di compressione e il backup contiene dati non comprimibili, l'utilizzo di spazio su disco potrebbe aumentare.
- Se il livello di compressione viene modificato da Nessuna compressione a Compressione standard o Compressione massima, oppure se viene modificato da Compressione standard o Compressione massima a Nessuna compressione, il primo backup eseguito dopo le modifiche apportate al livello di compressione sarà impostato automaticamente come backup completo. Dopo l'esecuzione del primo backup completo, tutti i backup successivi (completo, incrementale o

di verifica) vengono eseguiti come pianificati.

Questa opzione è disponibile solo per le destinazioni di condivisione locali o remote. Non è possibile modificare l'impostazione di compressione se si esegue il backup dell'agente Arcserve Unified Data Protection nell'archivio dati.

- Se la destinazione non dispone di sufficiente spazio libero, è possibile aumentare il livello di compressione del backup. Questa opzione è disponibile solo per le destinazioni di condivisione locali o remote. Non è possibile modificare l'impostazione di compressione se si esegue il backup dell'agente Arcserve Unified Data Protection nell'archivio dati.

configurazione

La scheda accessibile dalla Console di Arcserve UDP consente di definire parametri di configurazione come avvisi di posta elettronica, impostazioni del database e preferenze di installazione.

Dashboard

Una scheda sulla console di Arcserve UDP che consente di visualizzare l'ultimo stato di backup e lo stato di archiviazione. È possibile visualizzare l'archiviazione più recente di dati effettivi, raw e ripristinabili.

Archivio dati

Un archivio dati è un'area fisica di archiviazione su un disco. È possibile creare un archivio dati su tutti i sistemi Windows in cui è installato il Recovery Point Server. Gli archivi dati possono essere locali oppure possono trovarsi in una condivisione remota a cui il sistema Windows può accedere.

Destinazione

La destinazione è un computer o un server in cui vengono archiviati i dati di backup. Una destinazione può essere una cartella locale sul nodo protetto, una cartella remota condivisa o un Recovery Point Server (RPS).

Nodi rilevati

I nodi rilevati sono sistemi fisici o virtuali che vengono aggiunti alla Console di Arcserve UDP dopo essere stati rilevati da Active Directory o da un server vCenter/ESX, oppure importati da un file, o aggiunti manualmente mediante l'indirizzo IP.

Crittografia

La soluzione Arcserve Unified Data Protection fornisce la crittografia per i dati.

Quando la destinazione di backup è un Recovery Point Server, le crittografie disponibili sono Nessuna crittografia e Crittografa dati con AES-256. È possibile impostare questo valore per creare un archivio dati. Se la destinazione di backup è la condivisione locale o remota, le opzioni del formato di crittografia disponibili sono Nessuna crittografia, AES-128, AES-192 e AES-256. È possibile impostare l'opzione per la creazione di un piano per eseguire il backup nella cartella locale o condivisa, oppure impostare il valore dalle impostazioni di backup per l'agente Arcserve Unified Data Protection standalone.

Funzionalità principali della crittografia

1. Il metodo di crittografia AES256 si applica a:
   - Archivio dati
   - Password salvate (nel piano di protezione, nel registro di sistema, nel file di configurazione e così via)
2. *Per il processo di backup*: se la crittografia è abilitata, i dati vengono crittografati prima dell'invio al di fuori del server.
3. *Per il processo di replica*: se la destinazione di replica è abilitata per la crittografia, i dati vengono crittografati prima dell'invio al di fuori del server.

Impostazioni di crittografia

a. Selezionare il tipo di algoritmo di crittografia da utilizzare per i backup.

   La crittografia dei dati corrisponde alla conversione di dati in un modulo incomprensibile senza un meccanismo di decifratura. La soluzione Arcserve Unified Data Protection utilizza algoritmi protetti di crittografia AES (Advanced Encryption Standard) per ottenere la massima protezione e riservatezza dei dati specificati.

b. Nel caso in cui venga selezionato un algoritmo di crittografia, è necessario specificare e confermare una password di crittografia.
   - La password di crittografia può contenere un massimo di 23 caratteri.
   - Il backup completo e i relativi backup incrementali e di verifica devono utilizzare la stessa password di crittografia.
   - Se la password di crittografia di un backup incrementale o di verifica viene modificata, è necessario eseguire il backup completo. In seguito alla modifica della password di crittografia, la prima esecuzione del backup sarà di tipo completo, indipendentemente dal tipo di backup impostato.

Ad esempio, se si modifica la password di crittografia e si procede all'invio manuale di un backup incrementale o di verifica personalizzato, il backup si converte automaticamente un backup completo.

Nota: Questa opzione è disponibile solo per le destinazioni di condivisione locali o remote. Non è possibile disabilitare l'impostazione di crittografia se si esegue il backup dell'agente di Arcserve Unified Data Protection nell'archivio dati.

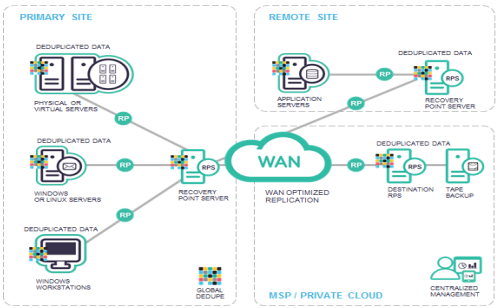
c. La soluzione Arcserve Unified Data Protection presenta una password di crittografia e una password di sessione.

- La password di crittografia è richiesta per l'archivio dati.
- La password di sessione è richiesta per il nodo.
- Se l'archivio dati è crittografato, la password di sessione è obbligatoria. Se l'archivio dati non è crittografato, la password di sessione è facoltativa.

Se il ripristino viene eseguito sullo stesso computer su cui è stato eseguito il backup, non è necessario immettere la password. La password viene richiesta in caso di ripristino su un computer diverso. Per impostazione predefinita, la password viene richiesta soltanto per il primo accesso. Per immettere la password anche in seguito al primo accesso, l'amministratore dovrà arrestare manualmente il servizio di estensione Explorer dell'agente Arcserve UDP.

Deduplicazione globale

La deduplicazione globale di Arcserve UDP consente di ridurre notevolmente la quantità di dati effettivamente trasferiti durante i cicli di backup. La capacità di deduplicazione su tutti i client nell'ambiente limita l'archiviazione e il trasferimento non necessari dei dati esistenti, rendendoli globali dal momento che verranno deduplicati nei nodi, nei processi e nei siti.



Backup senza agente basato su host

Un backup senza agente basato su host è un metodo per l'esecuzione del backup dei dati senza utilizzare un componente dell'agente sul computer di origine.

Modalità di trasporto HOTADD

La modalità di trasporto HOTADD è un metodo di trasporto dei dati che consente di eseguire il backup dei computer virtuali configurati con dischi SCSI. Per ulteriori informazioni, consultare la guida alla programmazione Virtual Disk API Programming Guide disponibile sulla pagina Web di VMware.

Processo

Un processo è un'azione di Arcserve UDP per l'esecuzione di backup e ripristino e per la creazione di Virtual Standby o la replica dei nodi.

Processi

Una scheda della console di Arcserve UDP che consente di monitorare lo stato di tutti i processi di backup, replica e ripristino. I dettagli includono processi, tipi di attività, ID di nodi, punti di ripristino e nomi di piano.

Modalità di trasporto NBD

La modalità di trasporto Network Block Device (NBD), denominata anche modalità di trasporto LAN, utilizza il protocollo NFC (Network File Copy) per la comunicazione. Diverse operazioni VDDK e VCB utilizzano una connessione per ciascun disco virtuale a cui effettuano l'accesso su ciascun server host ESX/ESXi, durante l'utilizzo di NDB.

Modalità di trasporto NBDSSL

La modalità di trasporto NBDSSL (Network Block Device Secure Sockets Layer) utilizza il protocollo di comunicazione NFC (Network File Copy). NBDSSL esegue il trasferimento dei dati crittografati mediante le reti di comunicazione TCP/IP.

Nodi

Un nodo è un sistema fisico o virtuale protetto da Arcserve UDP. Arcserve UDP consente di proteggere i nodi fisici e i computer virtuali in un server vCenter/ESX o Microsoft Hyper-V.

Piano

Un piano è un gruppo di attività per la gestione del backup, della replica e della creazione di computer Virtual Standby. Un piano è composto da un'attività singola o da più attività. Le attività sono un insieme di attività per la definizione dell'origine, della destinazione, della pianificazione e dei parametri avanzati.

Nodi protetti

I nodi protetti sono nodi che dispongono di piani di backup programmati per l'esecuzione regolare del backup dei dati.

Evento recente

Gli eventi recenti sono i processi ancora in esecuzione o recentemente completati.

Punto di ripristino

Un punto di ripristino è una snapshot di backup temporizzato. Un punto di ripristino viene creato quando si esegue il backup di un nodo. I punti di ripristino vengono archiviati nella destinazione di backup.

Recovery Point Server

Un Recovery Point Server è un nodo di destinazione in cui si installa il server. È possibile creare gli archivi dati in un Recovery Point Server. Il Recovery Point Server (RPS) agisce come un repository di backup per le immagini dei dischi e offre un insieme unico di tecnologie che formano le fondamenta della soluzione Arcserve UDP. Tra le funzioni principali del server RPS vi sono la deduplicazione globale basata sull'origine, la replica integrata e testata delle immagini dei dischi, il processo di jumpstart RPS o sincronizzazione non in linea e l'archiviazione multi-tenant.

Replica

La replica è un'attività che duplica i punti di ripristino da un server a un altro.

Risorse

risorse è una scheda della Console di Arcserve UDP. Dalla scheda **risorse** è possibile gestire nodi di origine, destinazioni e piani.

Modalità di trasporto SAN

La modalità di trasporto SAN consente il trasferimento dei dati di backup da sistemi proxy connessi alla rete SAN a periferiche di archiviazione.

Sistemi

Per sistemi si intendono tutti i tipi di nodi, periferiche e computer virtuali che possono essere gestiti da Arcserve Unified Data Protection. Sono inclusi computer fisici, virtuali, Linux e computer virtuali di standby.

Attività

Un'attività è un insieme di attività per la definizione di vari parametri per l'esecuzione di backup, replica e per la creazione di computer Virtual Standby. Questi parametri includono origine, destinazione, pianificazione e alcuni parametri avanzati. Ogni attività è associata a un piano. È possibile disporre di più di un'attività in un piano.

Nodi non protetti

I nodi non protetti sono i nodi aggiunti a Arcserve Unified Data Protection, ma senza l'assegnazione di un piano. Quando un piano non viene assegnato, non è

possibile eseguire il backup dei dati e il nodo rimane non protetto.

Deduplicazione dei dati

La deduplicazione dati è la tecnologia che consente di eliminare copie duplicate degli stessi dati, riducendo lo spazio di archiviazione. In un'organizzazione, ci potrebbero essere varie ragioni per l'esistenza di dati duplicati, come un allegato a messaggio di posta elettronica inoltrato a più utenti. Quando si esegue il backup di questi dati, si finiscono per salvare diverse copie degli stessi dati sul supporto di archiviazione di backup.

La deduplicazione dei dati consente di eliminare dati ridondanti e salvare solamente una istanza dei dati. Tutte le altre istanze vengono sostituite da un riferimento a quell'istanza. Questo metodo consente di ridurre considerevolmente lo spazio di archiviazione richiesto per archiviare dati di backup.

Ad esempio, ci potrebbe essere uno stesso file di 10 MB archiviato da 100 utenti nei loro sistemi locali. Quando si eseguirà il backup di tutti questi sistemi locali o di tutti nodi, si avrà bisogno di 1000 MB di spazio di archiviazione. Con la deduplicazione dei dati sarà possibile ridurre lo spazio di archiviazione a circa 10 MB poiché viene archiviata una sola istanza del file sul disco. Le 99 istanze restanti faranno riferimento a quell'unica istanza.

Benefici della deduplicazione dei dati

- Maggiori dati di backup in uno spazio di archiviazione
- Ridotta quantità di dati inviati sulla rete
- Backup rapido in quanto vengono archiviate le informazioni di riferimento piuttosto che i dati reali
- Costo della larghezza di banda di rete e del supporto di archiviazione ridotto

Tipi di deduplicazione dei dati

Arcserve UDP supporta i due seguenti tipi di deduplicazione dei dati.

Deduplicazione di dati dal lato origine

Solamente i dati univoci dell'agente vengono inviati a un Recovery Point Server per il backup dei dati.

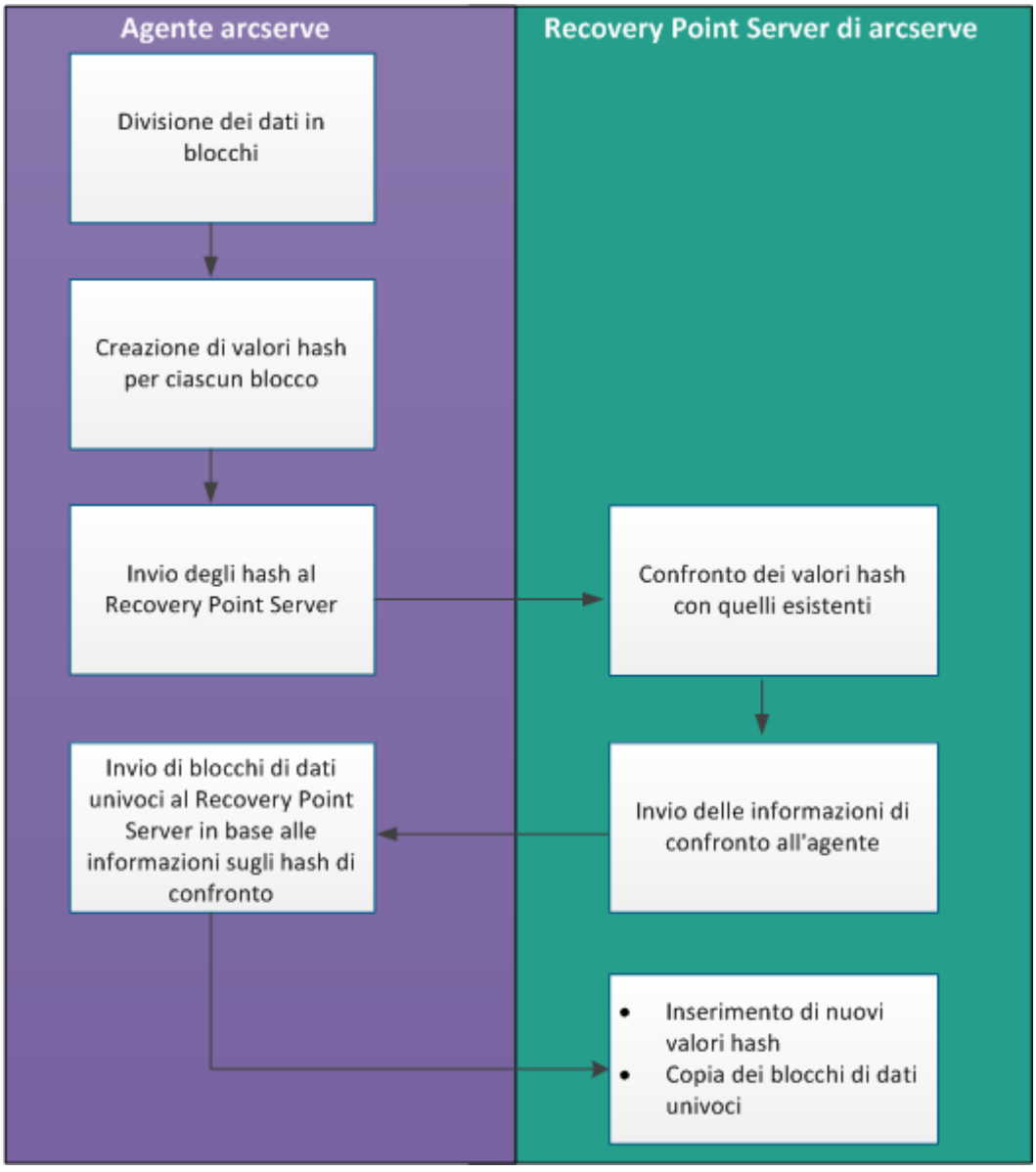
Deduplicazione globale

Viene eseguito il backup in un Recovery Point Server solamente dei dati univoci di più agenti. Se blocchi di dati simili sono presenti su più nodi, verrà eseguito il backup di una sola copia nel Recovery Point Server.

Funzionamento della deduplicazione dei dati

Il processo di deduplicazione dei dati di Arcserve UDP consente di dividere i dati in blocchi, ciascuno dei quali viene assegnato a un identificatore univoco denominato hash. L'hash viene calcolato in base al cluster del volume. La dimensione dei blocchi di deduplicazione predefinita è 4KB (la dimensione dei cluster del volume predefinita è 4KB per la maggior parte dei nodi). Tali valori hash vengono confrontati con i valori hash dei dati di backup esistenti e qualora vengano rilevati riferimenti duplicati, non viene eseguito il backup di quei blocchi di dati. Viene eseguito il backup solamente dei blocchi di dati con riferimenti univoci.

Il diagramma seguente illustra il funzionamento della deduplicazione in Arcserve UDP.



Quando un backup viene attivato, il processo di deduplicazione sull'agente suddivide prima i dati in blocchi e assegna una chiave hash univoca o un valore univoco a ciascun blocco. I valori hash vengono quindi inviati al Recovery Point Server. Nel Recovery Point Server, tali valori hash vengono comparati con i valori hash esistenti e gli hash duplicati vengono eliminati. I risultati della comparazione vengono rimandati all'agente. In base alle informazioni sugli hash duplicati, l'agente invia i blocchi di dati univoci al Recovery Point Server per il backup. I nuovi valori hash di questi blocchi di dati vengono inseriti nell'elenco degli hash esistenti sul Recovery Point Server.

Quando ci sono più agenti, il processo di deduplicazione rimane lo stesso, tuttavia, i dati duplicati dagli agenti vengono eliminati. Ciò consente di eliminare qualsiasi duplicazione di dati da vari agenti.

Di seguito vengono elencati i benefici derivanti dalla deduplicazione di dati in Arcserve UDP:

- **Backup completo più veloce**
- **Processo di unione più veloce**
- **Supporto di deduplicazione globale**
- **Replica ottimizzata**

Scenari in cui è consigliabile l'utilizzo della deduplicazione

Di seguito vengono riportati alcuni degli scenari in cui è possibile trarre grandi benefici dall'utilizzo di un archivio dati di deduplicazione:

- La deduplicazione può essere utilizzata quando si dispone di molti nodi con dati simili. In questo scenario, eseguendo il backup di dati da tutti i nodi a un archivio dati, si ottiene una buona riduzione della quantità di dati che in realtà viene archiviata sul Recovery Point Server. Lo spazio di archiviazione richiesto risulta considerevolmente minore.
- La deduplicazione può inoltre essere utilizzata quando è necessario eseguire frequentemente un backup completo di un nodo. In questo scenario, esiste già la maggior parte dei dati di backup, per cui il tempo di elaborazione del backup risulta inferiore.
- Un altro scenario in cui è consigliabile utilizzare la deduplicazione è quando la larghezza di banda di rete è limitata. Poiché solamente i blocchi di dati univoci viaggiano in rete, è possibile ridurre l'uso della rete.
- La deduplicazione è consigliata anche quando i dati di cui è stato eseguito il backup vengono spostati frequentemente da un nodo a un altro. In questo scenario, quando si prova a eseguire il backup del nuovo nodo (quello in cui i dati sono stati spostati dal nodo originale), la destinazione contiene già la copia e quindi viene eseguito il backup solamente delle informazioni di riferimento.

Configurazione degli archivi dati di deduplicazione in Arcserve UDP

I seguenti sono i parametri fondamentali che è necessario impostare per la configurazione di un archivio dati di deduplicazione:

Destinazione dati

La destinazione dati viene utilizzata per archiviare i dati protetti. È consigliabile utilizzare un disco di grandi dimensioni per la destinazione di dati poiché in esso verranno contenuti i blocchi di dati originali dell'origine.

Destinazione indice

La destinazione indice viene utilizzata per archiviare i file di indice. È consigliabile l'utilizzo di un disco differente per migliorare la velocità effettiva di elaborazione della deduplicazione.

Destinazione hash

La destinazione hash viene utilizzata per archiviare i file hash. È consigliabile l'utilizzo di una unità SSD ad alta velocità che consente di migliorare la capacità di deduplicazione richiedendo una bassa allocazione di memoria.

Se la destinazione hash viene configurata su una unità SSD ad alta velocità, è possibile utilizzarla per espandere la capacità di deduplicazione richiedendo una bassa allocazione di memoria.

Cartella di destinazione del backup

È la cartella di destinazione in cui risiedono i file .D2D e i file di catalogo.

Dimensioni dei blocchi

Le dimensioni dei blocchi di deduplicazione influiscono sulla capacità di deduplicazione stimata. Il valore predefinito delle dimensioni del blocco di deduplicazione è 16 KB. Se viene impostato su 32 KB, verrà raddoppiata la capacità di deduplicazione stimata. L'aumento delle dimensioni del blocco di deduplicazione può comportare la riduzione della percentuale di deduplicazione e, al tempo stesso, della quantità di memoria richiesta.

Allocazione memoria

Per calcolare la memoria richiesta, utilizzare lo strumento Stima dei requisiti di archiviazione e memorizzazione. Se la memoria allocata non è sufficiente, quando la memoria viene utilizzata completamente, i nuovi dati non riescono a inserire il nuovo hash nel database hash. Pertanto, non sarà possibile deduplicare gli eventuali dati sottoposti a backup in seguito, con una conseguente diminuzione del tasso di deduplicazione. Se non è possibile aumentare la

memoria per qualche motivo, tentare di aumentare le dimensioni del blocco di deduplicazione, in quanto comporterebbe una riduzione della memoria richiesta.

Nota: Non è possibile modificare le dimensioni del blocco per un archivio dati esistente.

Tenere presente che non si potrà avviare un nuovo processo di backup se la memoria hash è utilizzata completamente. Invece, è possibile continuare e terminare il processo di backup in corso, avviato prima che la memoria hash fosse utilizzata completamente. In tal caso, non verranno inserite nuove chiavi hash nel database hash, con delle conseguenze sulla percentuale di deduplicazione.

Ciò deriva dal fatto che tutti i blocchi di dati nel processo di backup in corso vengono ancora confrontati con le chiavi hash esistenti nel database hash.

• Se vengono raddoppiati con la chiave hash esistente, non vengono più scritti nel disco.

• In caso contrario, vengono scritti sul disco. Tuttavia, la nuova chiave hash non viene inserita nel database hash perché quest'ultimo è pieno. Pertanto, non sarà possibile confrontare i blocchi di dati successivi con le nuove chiavi hash.

Deduplicazione, crittografia e compressione

Oltre alla deduplicazione di dati, è possibile applicare anche la compressione e la crittografia a un archivio dati.

Se si abilita la crittografia, l'Agente Arcserve Unified Data Protection per Windows utilizza la risorsa CPU per crittografare i dati. Poiché la crittografia viene applicata solamente ai dati univoci, la risorsa CPU necessaria per la crittografia potrebbe essere minima dove la percentuale di deduplicazione è alta.

- Se non si applica la compressione né la deduplicazione, l'utilizzo della CPU è minore per l'attività di compressione e i dati archiviati non vengono compressi.
- Con la compressione standard e la deduplicazione, l'utilizzo della CPU è ottimale per l'attività di compressione e i dati archiviati vengono compressi, per cui lo spazio di archiviazione richiesto è minore.
- Con la compressione massima e la deduplicazione, l'utilizzo della CPU è massimo per l'attività di compressione e i dati archiviati sono superiori del 2-3%, per cui lo spazio di archiviazione richiesto è minore.

Limitazioni della deduplicazione

Non è possibile modificare il tipo di compressione, l'impostazione di crittografia e le dimensioni del blocco di deduplicazione una volta creato un archivio dati di deduplicazione.